ДВНЗ «УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
МІНІСТЕРСТВА ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

ТКАЧУК Тарас Юрійович

УДК 336.7:340.5:347.7

ДИСЕРТАЦІЯ
ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ЄВРОІНТЕГРАЦІЇ УКРАЇНИ

Подається на здобуття наукового ступеня **доктора юридичних наук**

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

_____ Т. Ткачук

Науковий консультант:
заслужений діяч науки і техніки України,
доктор юридичних наук,
старший науковий співробітник,
ДОВГАНЬ Олександр Дмитрович

Ужгород - 2019

АНОТАЦІЯ

Ткачук Т. Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України. — Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.07 — адміністративне право і процес; фінансове право; інформаційне право (081 — Право). – ДВНЗ «Ужгородський національний університет», Ужгород, 2019.

Дисертація присвячена дослідженню проблеми правового забезпечення інформаційної безпеки держави, порівняльним чином розглянуто відповідні практики у європейських країнах. На цьому теоретичному та емпіричному ґрунті у дисертації запропоновано розв'язання актуальної наукової проблеми – розроблення концептуальних правових засад забезпечення інформаційної безпеки держави та практичних рекомендацій щодо вдосконалення механізмів її реалізації в Україні.

Серед важливих теоретичних інновацій в роботі запропоновано та обґрунтовано включити до об'єктів правового забезпечення інформаційної безпеки України національні інтереси, цінності, цілі та надбання в інформаційній сфері. До інших важливих наукових досягнень відносяться розроблені в роботі критерії оцінки негативного впливу загроз на стан інформаційної безпеки України, якими запропоновано вважати деструктивні трансформації національних цінностей в інформаційній сфері, що дає змогу створити правове підґрунтя відповідної методологічної бази, а також класифіковано національних цінностей та національних цілей в інформаційній сфері та аргументовано доцільність їх законодавчого закріплення.

Введено в доктрину інформаційного права термін «національні

надбання в інформаційній сфері», під яким у роботі запропоновано розуміти сукупність унікальних інформаційних продуктів, що мають виняткове суспільне, економічне, військове та інше значення для реалізації національних цілей в інформаційній сфері.

У дисертаційному дослідженні виділено у системі інформаційно-психологічної складової інформаційної безпеки України такі елементи як духовна, воєнна, соціальна, економічна, екологічна та глобальна безпеки та змістовно охарактеризовано взаємозв'язки між ними, що дало змогу врахувати сучасні загрози та розробити пріоритетні напрями державної політики забезпечення інформаційної безпеки України;

Серед досягнень дисертації є розроблена авторська модель системи інформаційної безпеки держави на основі поєднання національних цінностей, інтересів, цілей та надбань у сфері інформаційних правовідносин, яку втілено в авторському проекті Закону України «Про інформаційну безпеку України».

У роботі акцентовано увагу на зростаючій ролі правових механізмів у забезпеченні інформаційної безпеки України, потребі ефективного законодавчого врегулювання суспільних відносин, що виникають у досліджуваній сфері, визначенні правових засад організації та координації дій суб'єктів забезпечення інформаційної безпеки України, розробці пріоритетних напрямів державної політики у сфері інформаційної безпеки. Дослідження інформаційної безпеки України з правничої точки зору пов'язане з формуванням якісної системи інформаційної безпеки, що відповідатиме сучасним вимогам та нагальним потребам України як повноправного члена й надійного партнера європейської спільноти.

Звернено увагу, що обравши євроінтеграційний курс та визначивши вступ до НАТО своїм стратегічним пріоритетом, Україна має орієнтуватися передусім на стратегію розвитку країн-учасниць ЄС та НАТО в інформаційній сфері. Для нашої держави імплементація європейських стандартів правового забезпечення інформаційної безпеки

держави є пріоритетним засобом інтеграції в європейський правовий простір.

У дисертації досліджено генезис теорій і концепцій правового забезпечення інформаційної безпеки держави, на даному теоретичному підґрунті обґрунтовано авторське бачення змісту «інформаційна безпека держави». Дослідження джерельної бази дало змогу виявити три концептуальні підходи до тлумачення інформаційної безпеки: 1) статичний (безпека як стан захищеності інформаційного середовища/інформації, система гарантій тощо), 2) діяльнісний (безпека як процес її забезпечення, здатність держави ефективно захистити національні інтереси і цінності); 3) комплексний (безпека як стан і процес).

Найбільш прийнятним із них є комплексний. За такого підходу інформаційну безпеку держави вперше визначено як:

1) стан, за якого в умовах дії реальних та потенційних загроз забезпечується самозбереження, сталий і прогресивний розвиток інформаційної сфери, зокрема захищеність інформаційної інфраструктури, інформаційного простору, інформаційних ресурсів, інформаційних процесів та їхніх суб'єктів, а також досягнення відповідних національних цілей та реалізація національних інтересів в інформаційній сфері;

2) постійний процес діяльності компетентних органів, спрямований на запобігання, протидію загрозам інформаційній сфері, застосування активних заходів інформаційного впливу, а також сукупність умов такої діяльності, які реалізуються й здатні контролюватися тривалий час.

За такого підходу інформаційну безпеку України вперше забезпечення інформаційної безпеки України визначено як постійний процес діяльності компетентних органів, спрямований на запобігання, протидію загрозам інформаційній сфері, застосування активних заходів інформаційного впливу, а також сукупність умов такої діяльності, які реалізуються й здатні контролюватися тривалий час.

Визначено об'єкт та предмет правового забезпечення інформаційної

безпеки держави. Запропоновано та обґрунтовано авторську концепцію щодо доктринального положення відносно об’єкту правового забезпечення інформаційної безпеки держави, включивши до сфери його впливу національні інтереси, цінності, цілі та надбання в інформаційній сфері. Реалізація національних інтересів в інформаційній сфері, визначених Доктриною інформаційної безпеки України, буде дієвою в разі законодавчого визначення національних цінностей і зумовлених ними національних інтересів. Національні інтереси, цінності та цілі в інформаційній сфері становлять предмет правового забезпечення інформаційної безпеки держави.

До національних цінностей в інформаційній сфері віднесено:

а) матеріальний добробут населення (у т. ч. на основі розвитку ІКТ);

б) інформаційна захищеність людини, суспільства, держави;

в) духовність, доступність віросповідання, попередження релігійного фанатизму та екстремізму;

г) мова;

ґ) культура інформаційних відносин;

д) свобода інформації, захищеність інформаційних прав людини, доступ до інформації, нейтралізація негативних інформаційних впливів та ін.

До національних цілей в інформаційній сфері віднесено:

а) покласти край спотворенням поглядів людей на навколишній світ і самих себе (духовна безпека);

б) забезпечити впровадження інформаційних технологій у військову сферу та забезпечити їх захист (військова безпека);

в) прискорити розробку та впровадження новітніх ІКТ у суспільно-економічну сферу (економічна безпека);

г) досягти належного рівня культури інформаційних відносин (соціальна безпека);

ґ) створити загальнодержавні інформаційні системи для постійного

моніторингу стану навколишнього середовища (екологічна безпека);

д) сприяти інтеграції національної інформаційної інфраструктури зі світовою інфраструктурою;

е) посилити захист інформаційних прав людини;

є) вжити термінових заходів для створення позитивного іміджу держави в умовах інформаційної глобалізації.

Виходячи із розробленої моделі взаємодії національних цінностей, інтересів цілей та надбань в інформаційній сфері, у дисертаційній роботі запропоновано основними критеріями оцінки негативного впливу на інформаційну безпеку держави вважати деструктивні трансформації національних цінностей в інформаційній сфері, які можливо встановлювати шляхом соціологічних опитувань та вивчення громадської думки. Такі критерії доцільно акумулювати в методологічній базі і на її підставі моніторити стан і динаміку вітчизняної інформаційної сфери, виявляти найбільш вразливі сфери.

З’ясовано місце правового забезпечення інформаційної безпеки держави у системі інформаційного права, а також класифіковано складові елементи та розроблено систему правового забезпечення інформаційної безпеки держави. Виявлено у вітчизняній системі інформаційного права нового елементу, котрий регулює відносини, пов'язані з правовим забезпеченням інформаційної безпеки, а також проаналізовано причини й передумови його виникнення. На цій теоретичній основі доведено об’єктивне існування нової підгалузі інформаційного права – правове забезпечення інформаційної безпеки держави.

Виходячи із розробленої схеми взаємодії національних цінностей, інтересів цілей та надбань в інформаційній сфері, запропоновано основними критеріями оцінки негативного впливу на інформаційну безпеку держави вважати деструктивні трансформації національних цінностей в інформаційній сфері, які можливо встановлювати шляхом соціологічних опитувань громадської думки. Такі критерії слід

акумулювати в методологічній базі і на її підставі моніторити стан і динаміку вітчизняної інформаційної сфери, виявляти найбільш вразливі сфери.

Значна увага приділена узагальненню теоретичних підходів до змісту загроз інформаційній безпеці держави, на цій основі запропоновані механізми протидії їм. Запропоновано інформаційно-психологічну складову інформаційної безпеки держави досліджувати у сукупності основних її складових: духовної, військової, соціальної, економічної, екологічної та глобальної безпеки, що дало змогу врахувати сучасні загрози та розробити пріоритетні напрями державної політики забезпечення інформаційної безпеки держави.

Досліджено практику діяльності суб'єктів забезпечення інформаційної безпеки України в умовах євроінтеграції та запропоновано напрями удосконалення їх функцій та завдань. Розроблена авторська модель системи інформаційної безпеки держави на основі поєднання національних цінностей, інтересів, цілей та надбань в інформаційній сфері.

Узагальнено міжнародний досвід правового забезпечення інформаційної безпеки держави, на цій основі розроблено концептуальні засади правового забезпечення інформаційної безпеки держави в умовах євроінтеграції та запропоновані пріоритети розвитку правових основ державної політики у сфері інформаційної безпеки. Аналіз чинного законодавства та практики європейських країн засвідчує: недоцільно закріплювати фіксований перелік загроз інформаційній безпеці України, оскільки він не має вичерпного характеру. Найбільш небезпечні з-поміж загроз — транскордонні і такі, що мають політичне забарвлення.

Підкреслено необхідність забезпечити одночасно безпеку інформації від знищення, перекручення, блокування, несанкціонованого витоку або порушення встановленого порядку її маршрутизації, по-друге, інформаційну безпеку громадянина та суспільства. Ця вимога продиктована значенням інформаційної картини світу, що формується на

індивідуальному та соцієтальному рівнях. Поширеним інструментом загроз є розповсюдження т. зв. патогенних текстів, спрямованих на деконструкцію ідеологічної, ціннісної, морально-етичної та інших ментальних систем.

У роботі доведено, що досвід зміни парадигми забезпечення національної безпеки України з реактивної на проактивну в контексті євроінтеграційних спрямувань є надзвичайно важливим, адже дає змогу правильно визначати стратегічні пріоритети, акумулювати зусилля щодо забезпечення інформаційної безпеки, а також сприятиме плідному співробітництву з усіма європейськими країнами у розбудові систем регіональної та міжнародної інформаційної безпеки.

З'ясовано, що цей досвід є також досить важливим для подальшої розбудови теорії національної безпеки та наукових засад забезпечення інформаційної безпеки.

Для України корисним є досвід країн Центральної Європи у забезпеченні інформаційної безпеки, зокрема Хорватії та Німеччини.

У роботі акцентовано увагу на актуальності приєднання України до інших європейських країн у розбудові системи міжнародної інформаційної безпеки, щоб протидіяти кібертероризму та кіберзлочинності, орієнтуючись при цьому на стандарти ЄС та НАТО. Для України важливим є досвід країн Східної Європи щодо приведення національного законодавства у відповідність до вимог міжнародних організацій, передусім, щодо забезпечення балансу між свободою та безпекою в інформаційній сфері на законодавчому рівні.

Сформовано рекомендації з удосконалення національного законодавства у сфері забезпечення інформаційної безпеки держави (розроблено проект ЗУ «Про інформаційну безпеку України») та відповідної практики правоохоронних органів (пам'ятка для посадових осіб органів державної влади та місцевого самоврядування «Як не стати жертвою шпигунських посягань»), що створює методологічну базу

здійснення гармонізації національного законодавства з міжнародним правом та європейським законодавством. Перспективно розвивати співробітництво України у розбудові систем регіональної та міжнародної інформаційної безпеки у рамках проекту «Міжмор'я» з метою протидії загрозам стратегічній стабільності, зокрема, кібертероризму та кіберзлочинності, орієнтуючись при цьому на стандарти ЄС та НАТО.

Доведено, що забезпечення інформаційної безпеки України є визначальним напрямом державної політики, від якого залежатиме існування держави, її національна безпека, соціально-економічний розвиток та відповідне місце у світовому співтоваристві.

Визначено основні цілі державної політики України у сфері забезпечення інформаційної безпеки: а) захист інформаційного суверенітету держави в сучасних умовах глобалізації та інтернаціоналізації процесів в інформаційній сфері; б) забезпечення інформаційної достатності для прийняття рішень державними органами, підприємствами та громадянами; в) реалізація конституційних прав і свобод громадян, суспільства і держави на інформацію.

Обґрунтовано, що основна мета державної політики у сфері забезпечення інформаційної безпеки України – це управління реальними та потенційними загрозами з метою створення необхідних умов для задоволення інформаційних потреб людини та громадянина, а також реалізації національних інтересів.

З огляду на сучасний стан загроз інформаційній безпеці, удосконалено пріоритетні напрями державної політики у сфері забезпечення інформаційної безпеки України: а) захист життєво важливих інтересів особистості, суспільства та держави від внутрішніх і зовнішніх загроз; б) захист суверенітету, підтримка політичної та соціальної стабільності, територіальної цілісності України; в) захист критичної інформаційної інфраструктури; г) забезпечення розвитку інформаційно-комунікаційних технологій; ґ) забезпечення участі України в міжнародній системі

інформаційної безпеки.

***Ключові слова*:** *безпека, інформаційна безпека, інформаційне право, інформаційні правовідносини, загрози, інформаційна політика, кібербезпека, кіберзагрози, інформаційне законодавство, євроінтеграція.*

SUMMARY

Tkachuk T. Yu. Legal providing of information security in conditions of European integration of Ukraine. - On the rights of the manuscript.

Dissertation for the degree of Doctor of Law in specialty 12.00.07 - administrative law and process; finance law; information law (081 - Law). - Uzhhorod National University, Uzhhorod, 2019.

The dissertation is devoted to the research of the problem of legal providing of information security of the state, the relevant practices in European countries are considered in the comparative way. On this theoretical and empirical ground in the dissertation the solution of the actual scientific problem is proposed - the development of conceptual legal principles for ensuring information security of the state and practical recommendations for improving the mechanisms of its implementation in Ukraine.

Among the important theoretical innovations in the work, it is proposed and substantiated to correspond to the objects of legal support of information security of Ukraine national interests, values, goals and achievements in the information sphere. Other important scientific achievements include the criteria for evaluating the negative impact of threats on the state of Ukraine's information security, which suggested to consider destructive transformations of national values in the information sphere, which enables to create the legal basis for the relevant methodological base, as well as classify national values and

national goals in the information sphere and the rationale for their legislative consolidation.

It is introduced into the doctrine of information law the term "national heritage in the information sphere", which is suggested in the work to understand as the totality of unique informational products that have an exceptional social, economic, military and other significance for the implementation of national goals in the information sphere.

In the dissertation research, the elements of spiritual, military, social, economic, ecological and global security are highlighted in the information and psychological component of the information security of Ukraine, and the interrelations between them are substantially characterized, which enabled to take into account modern threats and develop the priority directions of the state policy of providing information security of Ukraine.

Among the achievements of the dissertation is the author's model of the system of information security of the state based on the combination of national values, interests, goals and achievements in the field of information legal relations, which is embodied in the author's draft Law of Ukraine "On Information Security of Ukraine".

The paper focuses on the growing role of legal mechanisms in ensuring the information security of Ukraine, the need for effective legislative regulation of social relations arising in the field of study, the definition of legal principles for the organization and coordination of the activities of the subjects of providing information security of Ukraine, the development of priority areas of state policy in the field of information security. The study of information security of Ukraine from the legal point of view is associated with the formation of a high-quality information security system that meets the modern requirements and urgent needs of Ukraine as a full member and a reliable partner of the European community.

Attention is drawn to the fact that choosing the European integration course and defining NATO membership as their strategic priority, Ukraine

should focus first and foremost on the strategy of the development of the EU member states and NATO in the field of information. For our state, the implementation of European standards for legal security of information security of the state is a priority means of integration into the European legal space.

In the dissertation the genesis of theories and concepts of legal support of information security of the state is investigated, on the given theoretical basis the author's vision of the content "information security of the state" is substantiated. The source database research has revealed three conceptual approaches to the interpretation of information security: 1) static (security as a condition of the protection of the information environment / information, guarantee system, etc.), 2) activity (security as a process of its provision, the state's ability to protect effectively national interests and values); 3) complex (security as a state and process).

The most acceptable of them is the complex one. For such an approach, state information security was first defined as 1) a state in which, in the face of actual and potential threats, self-preservation, sustainable and progressive development of the information sphere, in particular the security of information infrastructure, information space, information resources, information processes and their subjects, is ensured, as well as the achievement of relevant national goals and the realization of national interests in the information sphere; 2) a permanent process of the activities of the competent authorities aimed at preventing, combating threats to the information sphere, the use of active measures of information influence, as well as a set of conditions for such activities that are implemented and can be monitored for a long time.

According to this approach, the information security of Ukraine for the first time was defined as 1) the state in which, under the conditions of actual and potential threats, self-preservation, sustainable and progressive development of the information sphere, in particular the security of information infrastructure, information space, information resources, information processes and their subjects, is ensured, as well as the achievement of relevant national goals and

the realization of national ainterests in the information sphere; 2) ensuring the information security of Ukraine is defined as a permanent process of the activities of the competent authorities aimed at preventing, countering threats to the information sphere, the use of active measures of information influence, as well as a set of conditions for such activities that are being implemented and can be monitored for a long time .

The object and subject of legal protection of information security of the state are determined. The author's conception about the doctrinal position regarding the object of legal support of information security of the state is proposed and substantiated, including national interests, values, goals and achievements in the information sphere in the sphere of its influence. Realization of national interests in the information sphere, determined by the Doctrine of Information Security of Ukraine, will be effective in the case of legislative definition of national values and their national interests. National interests, values and goals in the information sphere constitute the subject of legal protection of state information security.

The national values in the information sphere include: a) material well-being of the population (incl. On the basis of the development of ICT); b) information security of a person, a society, a state; c) spirituality, accessibility of religion, prevention of religious fanaticism and extremism; d) language; e) culture of information relations; e) freedom of information, protection of information rights, access to information, neutralization of negative informational influences, etc.

National goals in the information sphere include: a) to put the end to the distortion of the views of people in the surrounding world and themselves (spiritual security); b) to ensure implementation of information technologies in the military sphere and ensure their protection (military security); c) to accelerate the development and implementation of the latest ICTs in the socio-economic field (economic security); d) to achieve the appropriate level of culture of information relations (social security); e) to create national

information systems for the continuous monitoring of the state of the environment (environmental safety); e) to promote the integration of the national information infrastructure with the global infrastructure; e) to strengthen the protection of information rights; h) to take urgent measures to create a positive image of the state in the conditions of information globalization.

Proceeding from the developed model of interaction of national values, interests of goals and achievements in the information sphere, in the dissertation work the main criteria for assessing the negative impact on state information security are proposed to consider destructive transformations of national values in the information sphere that can be established through sociological surveys and the study of public opinion. It is expedient to accumulate such criteria in the methodological base and on its basis to monitor the state and dynamics of the domestic information sphere, to identify the most vulnerable spheres.

The place of legal security of state information security in the system of information law is determined, as well as the constituent elements are classified and the system of legal security of information security of the state is developed. The new element of the information system of the national system, which regulates the relations related to the legal security of information security, was also revealed, as well as the reasons and the background of its emergence were analyzed. On this theoretical basis the objective existence of a new sub-field of information law - the legal security of information security of the state has been proved.

Proceeding from the developed scheme of interaction of national values, interests of goals and achievements in the information sphere, the main criteria for assessing the negative impact on the state's information security are considered destructive transformations of national values in the information sphere, which may be established through sociological polls of public opinion. Such criteria should be accumulated in the methodological basis and on its basis monitor the state and dynamics of the domestic information sphere, to identify the most vulnerable spheres.

Considerable attention is paid to generalization of theoretical approaches to the content of threats to state information security, on this basis mechanisms of counteraction to them are proposed. The information-psychological component of information security of the state is proposed to be investigated in the aggregate of its main components: spiritual, military, social, economic, ecological and global security, which enabled to take into account modern threats and develop the priority directions of the state policy of ensuring information security of the state.

The practice of activity of subjects of providing information security of Ukraine in the conditions of European integration was investigated and directions of improvement of their functions and tasks were offered. The author's model of the system of information security of the state is developed on the basis of a combination of national values, interests, goals and achievements in the information sphere.

The international experience of legal security of information security of the state is generalized, on this basis, the conceptual framework of legal support of state information security in the conditions of European integration was developed and the priorities of the development of legal foundations of state policy in the field of information security were proposed. Analysis of current legislation and practice of European countries testifies: it is inappropriate to establish a fixed list of threats to Ukraine's information security, since it is not exhaustive. The most dangerous among threats are cross-border and politically colored.

It was emphasized the need to ensure simultaneous security of information from destruction, distortion, blocking, unauthorized leakage or violation of the established procedure for its routing, and secondly, the information security of the citizen and society. This requirement is dictated by the value of the information picture of the world, which is formed on the individual and societal levels. The common threat tool is to spread the so-called pathogenic texts aimed at deconstructing ideological, value, moral and ethical

and other mental systems.

It is proved that the experience of changing the paradigm of ensuring Ukraine's national security from reactive to proactive in the context of European integration is extremely important, since it enables to correctly identify strategic priorities, accumulate efforts to ensure information security, and will promote fruitful cooperation with all European countries in the development of systems of regional and international information security.

It has been argued that this experience is also very important for further development of the theory of national security and the scientific principles of information security.

For Ukraine, the experience of Central European countries in providing information security, in particular, Croatia and Germany, is useful.

The paper focuses on the relevance of Ukraine's accession to other European countries in the development of an international information security system to counter cyber-terrorism and cybercrime, while focusing on EU and NATO standards. For Ukraine, the experience of Eastern European countries is important in order to bring national legislation in line with the requirements of international organizations, first of all, to ensure a balance between freedom and security in the information sphere at the legislative level.

The recommendations on the improvement of the national legislation in the field of providing information security of the state have been formed (draft Law "On Information Security of Ukraine") and the relevant practice of law enforcement bodies (a memorial for officials of state authorities and local self-government "How not to become a victim of espionage attacks") , which creates a methodological basis for the harmonization of national legislation with international law and European legislation. Promote Ukraine's cooperation in developing regional and international information security systems within the framework of the "Inter-Sea Region" project in order to counteract threats to strategic stability, in particular cyber-terrorism and cybercrime, while focusing on EU and NATO standards.

It is proved that the provision of information security of Ukraine is a determining direction of state policy, on which the existence of the state, its national security, socio-economic development and the corresponding place in the world community will depend on.

The main objectives of the state policy of Ukraine in the field of ensuring information security are defined as the following: a) protection of information sovereignty of the state in the current conditions of globalization and internationalization of processes in the information sphere; b) ensuring information adequacy for decision-making by state bodies, enterprises and citizens; c) realization of constitutional rights and freedoms of citizens, society and state to information.

It is substantiated that the main objective of the state policy in the field of providing information security of Ukraine is management of real and potential threats in order to create the necessary conditions for meeting the information needs of man and citizen, as well as the realization of national interests.

Taking into account the current state of threats to information security, the priority directions of the state policy in the field of ensuring information security of Ukraine have been improved: a) protection of vital interests of the individual, society and the state from internal and external threats; b) protection of sovereignty, support of political and social stability, territorial integrity of Ukraine; c) protection of critical information infrastructure; d) ensuring the development of information and communication technologies; e) ensuring Ukraine's participation in the international information security system.

Key words: security, information security, information law, information legal relations, threats, information policy, cyber security, cyber threats, information law, eurointegration.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

В яких опубліковані основні наукові результати дисертації:

Монографія:

1. Ткачук Т. Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір: *моногр*. К. : ВД «АртЕк», 2018. 422 с.

Глави і розділи у підручниках:

2. Менеджмент інформаційної безпеки: підруч. : у 2 ч. / А. К. Гринь, О. Д. Довгань, В. І. Журавель, С. О. Князєв, Є. Д. Скулиш, О. М. Солодка, Т. Ю. Ткачук; за заг. ред. Є. Д. Скулиша. К. : НА СБУ, 2013. Ч. 2. 604 с. с. 43-132; с. 181-272

Глави і розділи у посібниках:

3. Ткачук Т. Ю. Конкурентна розвідка : *навч. посіб*. К. : НА СБУ, 2010. 240 с.

4. Довгань О. Д., Журавель В. І., Ткачук Т. Ю. Організаційно-правові основи охорони комерційної таємниці: *навч. посібн*. К. : НА СБУ, 2012. с. 137-277

5. Довгань О. Д., Журавель В. І., Ткачук Т. Ю. Протидія промисловому шпигунству: навч. посібн. К. : НА СБУ, 2015. с. 83-101, с. 121-198.

6. Організаційно-правові заходи захисту службової інформації : навч. посібник / І. П. Касперський, С. О. Князєв, О. І. Матяш, Т. Ю. Ткачук К. : НА СБУ, 2017. с. 14-36.

7. Кадрова політика у сфері інформаційної безпеки : *навч. посіб*. / Гуз А.М., Мамченко С.М., Ткачук Т.Ю. та ін. / Київ : Нац. акад. СБУ, 2017. с. 86-207.

8. Організація захисту інформації з обмеженим доступом : *навч. посібн.* / А. М. Гуз, І. П. Касперський, Т. Ю. Ткачук. К. : НА СБУ, 2018. с. 33-58.

Статті в наукових фахових виданнях України з юридичних наук, у т. ч. тих, які зареєстровані у міжнародних наукометричних базах:

9. Ткачук Т. Ю. Напрями імплементації міжнародних стандартів захисту персональних даних у законодавство України. *Митна справа.* 2010. № 5. Ч. 2. С. 3–9.

10. Ткачук Т. Ю. Інформація з обмеженим доступом на підприємстві: проблеми безпеки та захисту. *Право України*. 2011. № 3. С. 243–252.

11. Ткачук Т. Ю. Правові засади доступу громадян до публічної інформації у контексті законодавчих змін. *Інформаційна безпека людини, суспільства, держави.* 2011. № 2. С. 62–69.

12. Ткачук Т. Ю. Принципи забезпечення інформаційної безпеки держави: інформаційний аспект. *Митна справа*. 2012. № 1. Ч. 2. С. 399–405.

13. Ткачук Т. Ю. Принципи та провідні завдання взаємодії органів державної влади та суб’єктів господарювання у сфері забезпечення національної інформаційної безпеки. *Наше право*. 2012. № 1. Ч. 1. С. 141–148.

14. Ткачук Т. Ю. Місце і роль конкурентної розвідки в стратегічному плануванні інформаційної безпеки підприємства. *Інформаційна безпека людини, суспільства, держави*. 2013. № 2. С. 47–54.

15. Ткачук Т. Ю., Журавель В.І. Ризик-діяльність у сфері захисту інформації з обмеженим доступом. *Інформаційна безпека людини, суспільства, держави.* 2014. № 2. С. 86–95.

16. Ткачук Т. Ю. Правова охорона службової інформації як елемент системи забезпечення інформаційної безпеки держави: досвід

зарубіжних країн. *Юрид. наук. електр. журнал*. 2015. № 6 URL:http://www.lsej.org.ua/index.php/arkhiv-nomeriv?id=44

17. Ткачук Т. Ю., Журавель В. І. Соціальна складова менеджменту у системі захисту інформації з обмеженим доступом. *Інформ. безпека людини, суспільства, держави.* 2015. № 3 (19). С. 93–102.

18. Ткачук Т. Ю. Інформаційна безпека держави в онтологічному вимірі. *Порівняльно-аналітичне право.* 2015. №4. С. 284–287.

19. Ткачук Т. Ю., Яцко М.Г. Стан інформаційної безпеки України та основні завдання недержавних суб'єктів по її забезпеченню. *Інтернаука*. 2017. № 1(1). С. 41–43.

20. Ткачук Т. Ю. Інформаційна безпека: сучасні підходи до визначення категорії. *Актуальні питання публічного та приватного права*. 2017. № 2 (16). С. 45–54.

21. Ткачук Т. Ю. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. *Підприємництво, господарство і право.* 2017. № 10. С. 182–186.

22. Ткачук Т. Ю. Державна політика у сфері забезпечення інформаційної безпеки на сучасному етапі. *Наук. вісник УжНУ. Серія «Право».* 2017. № 46. Т. 2. С. 39–43.

23. Ткачук Т. Ю. Забезпечення інформаційної безпеки у країнах центральної Європи. *Юридичний науковий електронний журнал*. 2017 № 5. URL: http://lsej.org.ua/5_2017/30.pdf

24. Ткачук Т. Ю. Забезпечення інформаційної безпеки: досвід окремих країн східної Європи. *Інформація і право*. 2017. № 4. С. 62–73.

25. Ткачук Т. Ю. Забезпечення інформаційної безпеки у країнах позаблокового статусу. *Прикарпатський юрид. вісник*. 2017. № 4. С. 61–65.

26. Ткачук Т. Ю. Механізми протидії інформаційним загрозам зовнішніх джерел. *Вісник НТУ України «Київський політехнічний інститут». Політологія. Соціологія. Право.* 2017. № 1–2. С. 242–246.

27. Ткачук Т. Ю., Довгань О.Д. Система інформаційної безпеки України: онтологічні виміри. *Інформація і право.* 2018. № 1 (24). С. 89–104.

28. Ткачук Т. Ю., Довгань О.Д. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс. *Інформація і право.* 2018. № 2 (25). С. 73–85.

29. Ткачук Т. Ю. Пріоритетні напрями державної політики забезпечення інформаційної безпеки на сучасному етапі державотворення. *Науковий вісник ХДУ. Серія «Юридичні науки».* 2018. №4. С. 32-36

30. Ткачук Т. Ю., Довгань О.Д. Наукова рефлексія інформаційної безпеки України: від позитивізму до метафізики права. *Інформація і право*. 2018. № 4 (24). С. 79–89.

Статті в наукових періодичних виданнях із юридичних наук інших держав:

31. Ткачук Т. Ю. Складові інформаційної безпеки: аналіз критеріїв. *Visegrad Journal on Human Rights*. 2017. № 4. С. 153–158.

32. Ткачук Т. Ю. Суб'єкти забезпечення інформаційної безпеки держави: функціональний аналіз. *Jurnalul juridic national: teorie şi practică.* 2017. № 6. С. 42–46.

33. Ткачук Т. Ю. Інформаційна безпека держави у національному законодавстві європейських країн. *Visegrad Journal on Human Rights*. 2018. № 1. С. 145–150.

34. Ткачук Т. Ю. Теоретичний дискурс пошуку основних складових системи інформаційної безпеки держави. *Jurnalul juridic national: teorie şi practică.* 2018. № 2. С. 45–47.

35. Ткачук Т. Ю. Политика информационной безопасности НАТО. *Legea si Viata.* 2018. № 5. С. 187–191.

Які засвідчують апробацію матеріалів дисертації:

36. Ткачук Т. Ю. Інформаційна безпека суб'єктів господарювання як складова частина системи державного безпеко творення. *Актуальні проблеми забезпечення інформ. безпеки держави : мат. наук.-практ. конф. (Київ, 20.03.09).* : НА СБУ. С. 166–168.

37. Ткачук Т. Ю. Проблемні аспекти правового регулювання захисту персональних даних у процесі контррозвідувальної та оперативно-розшукової діяльності. *Актуальні проблеми управління інформ. безпекою держави : мат. наук.-практ. конф. (Київ, 17.03.10): НА СБУ*, 2010. С. 103–106.

38. Ткачук Т. Ю. Правові та організаційні засади взаємодії правоохоронних органів та приватних структур у сфері забезпечення інформаційної безпеки держави: досвід окремих країн. *Актуальні питання взаємодії інститутів громадянського суспільства та органів публічного адміністрування у напрямку розвитку правової системи України : мат. міжнарод. наук.-практ. конф. (Київ, 11–12.09.15)* : Центр правових наукових досліджень, 2015. С. 83–87.

39. Ткачук Т. Ю. Обґрунтування потреби наукової розробки теоретико-правових засад комплексного захисту інформації з обмеженим доступом. *Актуальні проблеми управління інформаційною безпекою держави: НА СБУ (Київ, 19.03.15).* С. 368–371.

40. Ткачук Т. Ю. Дозвільні засоби забезпечення інформаційної безпеки держави. *Політико-правові реформи та становлення громадянського суспільства в Україні : мат. всеукр. наук.-практ. конф. (Херсон, 09–10.10.2015).* 2015. С. 129–132.

41. Ткачук Т. Ю. Захист національних інформаційних ресурсів як пріоритетна складова інформаційної політики держави в умовах глобалізації. *Розвиток України в 21 ст. : економічні, соціальні, екологічні, гуманітарні та правові проблеми : мат. міжнарод. наук.-практ. конф. (Тернопіль, 30.03.12).* С. 209–212.

42. Ткачук Т. Ю. Охорона службової інформації в контексті

забезпечення інформаційної безпеки держави. *Актуальні проблеми управління інформ. безпекою держави: мат. (Київ, 20.03.14).* Ч.2. К. : НА СБУ, 2014. С. 69–74.

43. Ткачук Т. Ю. Україна як форпост європейської безпеки. *Zbornik prispevkov z medzinarodnej vedeckej konferencie "Pravna veda a prax: vyzvy modfrnych europskych integracnych procesov". (Bratislava, 27–28.11.15).* С. 242–245.

44. Ткачук Т. Ю. Витоки гібридної війни та сучасні її технології. Пріоритетні напрями наукових досліджень: *Мат. II Міжнарод. наук.-практ. конф. (Київ, 15–16.08.17):* МЦНД, 2017. С. 79–81.

45. Ткачук Т. Ю. Законодавчі підходи до кібербезпеки в окремих країнах світу. *Сучасні правові системи світу: тенденції та фактори розвитку : мат. міжнарод. наук.-практ. конф. (Запоріжжя, 25–26.08.17).* С. 84–86.

46. Ткачук Т. Ю. Кібербезпека: підходи до визначення в окремих країнах. *Актуальні проблеми управління інформ. безпекою держави : мат. наук.-практ. конф. (Київ, 24.05.17).* 2017. С. 142–144.

47. Ткачук Т. Ю. Інформаційна безпека держави як пріоритетна складова національної безпеки. *Верховенство права та правова держава : мат. міжн. наук.-практ. конф. (Ужгород, 15–16.09.17).* 2017. С. 142–145.

48. Ткачук Т. Ю. Тіньовий інтернет: співвідношення можливостей і загроз. *Інтернет речей: проблеми правового регулювання та впровадження : мат. першої наук.-практ. конф. (Київ, 24.10.17).* С. 100–103.

49. Ткачук Т. Ю. Кібербезпека: підходи до визначення в окремих країнах. *Кібербезпека в Україні: правові та організаційні питання : мат. всеукр. наук.-практ. конф. (Одеса, 17.11.17).* ОДУВС, 2017. С. 54–55.

50. Ткачук Т. Ю. Теоретико-правове осмислення інформаційної безпеки держави у контексті розвитку інформаційного суспільства. *Теоретико-правові основи формування та розвитку інформаційного*

суспільства : мат. наук.-практ. конф. (Київ, 29.11.17). 2017. С. 111–114.

54. Ткачук Т. Ю. Протидія кіберзагрозам у країнах позаблокового статусу. Освіта і наука у сфері нац. безпеки: проблеми та пріоритети розвитку : *мат. міжнарод. наук.-практ. конф. (Острог, 01.12.17)*. С. 66–70.

51. Ткачук Т. Ю. Інформаційна безпека держави як пріоритетна складова національної безпеки. *Science, research, development state and law. #2 (London, 27.02.18)*. С. 39–43.

52. Ткачук Т. Ю. Аксіологічні складові об'єкта правового забезпечення інформаційної безпеки України. *Сучасна юриспруденція Європейського Союзу: взаємодія права, нормотворчості та практики : мат. міжнарод. наук.-практ. конф. (Люблін, 17.04.18)*. 2018. С. 83–86.

53. Ткачук Т. Ю. Інформаційний чинник у гібридній війні. Кібербезпека у системі нац. безпеки України: пріоритетні напрями розвитку : *мат. наук. круглого столу (Маріуполь, 26.04.18)*. МДУ, 2018. С. 39–42.

55. Ткачук Т. Ю. Аксіологічні константи інформаційної без пеки держави. *Актуальні проблеми управління інформац. безпекою держави : мат. всеукр. наук.-практ. конф. (Київ, 30.03.18)*. НА СБУ, 2018. С. 167–169.

56. Ткачук Т. Ю. Україна як форпост європейської безпеки: аналіз інформаційної сфери. Україна та нац. інтереси в глобаліз. світі: візія націоналістів : *мат. п'ятих Бандерівських читань (Київ, 09.02.18)*. 2018. С. 394–404.

57. Ткачук Т. Ю. Взаємозв'язок національних цінностей, інтересів та цілей у концепції правового забезпечення інформаційної безпеки держави. *Права, свободи і безпека людини в інформаційній сфері : мат. наук.-практ. конф. (Київ, 10.05.18)*. 2018. С. 47–50.

58. Ткачук Т.Ю. Інформаційна безпеки у системі національної безпеки держави. *Освіта і наука у сфері національної безпеки: проблеми та*

пріоритети розвитку : збірник наукових праць за матеріалами Міжнародної науково-практичної конференції (8 червня 2018 р., м. Острог). Острог: Видавництво Національного університету «Острозька академія», 2018. С. 138-140.

Публікації, які додатково відображують результати дисертаційного дослідження:

59. Ткачук Т. Ю. Концептуальні засади функціонування конкурентної розвідки. *Проблеми правового забезпечення реалізації функцій державного управління і місцевого самоврядування. Серія «Право». Т. 3. Вип. 3.* Донецьк : ДонДУУ, 2010. С. 154–164.

60. Ткачук Т. Ю. Інформаційна функція грошей. Розвиток гуманітарних наук. *Проблеми і перспективи : мат. міжнарод. наук.-практ. конф. (Катовіце, 28.09-30.09.12).* С. 69–72.

61. Ткачук Т. Ю., Журавель В. І. Організаційне проектування у системі захисту конфіденційної інформації суб'єктів господарювання. *Інформаційна безпека людини, суспільства, держави.* 2014. № 1. С. 76–84.

62. Ткачук Т. Ю. Конкурентна розвідка: *моногр.* Коломия : ПАТ «Коломийська друкарня ім. Шухевича», 2015. 296 с.

63. Ткачук Т. Ю., Яцко М.Г. Суспільно-економічні передумови створення недержавної системи безпеки в Україні. *Молодий вчений.* 2017. № 1 (41), січень С. 157–159.

64. Ткачук Т. Ю., Кравченко О.О. Яким має бути Закон «Про комерційну таємницю»? *Вісник* АПСВТ. 2017. № 2. С. 10–19.

ЗМІСТ

АНОТАЦІЯ 2
ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ 28
ВСТУП 29
РОЗДІЛ І ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ ЯК ОБ'ЄКТ НАУКОВОГО ПІЗНАННЯ 41
1.1. Генезис правового забезпечення інформаційної безпеки людини, суспільства, держави 41
1.1.1. Першоджерела інформаційної безпеки 42
1.1.2. Інформаційна безпека на сучасному етапі державотворення 50
1.2. Понятійно-категоріальний синтез правового забезпечення інформаційної безпеки України 62
1.3. Теоретико-правові основи визначення об'єкта та предмета правового забезпечення інформаційної безпеки України 80
1.4. Методологічні засади правового забезпечення інформаційної безпеки України 110
Висновки до розділу 1 119
РОЗДІЛ ІІ ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ЄВРОІНТЕГРАЦІЇ УКРАЇНИ 122
2.1. Правове забезпечення інформаційної безпеки України як складова інформаційного права 122
2.2. Правова природа основних складових елементів інформаційної безпеки України 140
2.3. Правові засади організації системи інформаційної безпеки України 157
2.3.1. Співвідношення інформаційної та кібернетичної безпеки 174
Висновки до розділу 2 181

РОЗДІЛ ІІІ ТЕОЕРТИКО-ПРАВОВИЙ АНАЛІЗ СУЧАСНИХ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ В УМОВАХ ЄВРОІНТЕГРАЦІЇ 184
3.1. Класифікація загроз інформаційній безпеці України 184
3.2. Протидія загрозам інформаційній безпеці України: правові підходи 199
3.3. Функціональний аналіз суб'єктів забезпечення інформаційної безпеки України в умовах євроінтеграції 213
Висновки до розділу 3 235
РОЗДІЛ IV МІЖНАРОДНИЙ ДОСВІД ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ, СУСПІЛЬСТВА, ДЕРЖАВИ 240
4.1. Правові засади політики інформаційної безпеки Північноатлантичного альянсу 240
4.2. Забезпечення інформаційної безпеки у нейтральних країнах Європи 252
4.3. Досвід правового забезпечення інформаційної безпеки у країнах Європейського Союзу 266
Висновки до розділу 4 293
РОЗДІЛ 5 НАПРЯМИ РОЗВИТКУ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ЄВРОІНТЕГРАЦІЇ 301
5.1. Концептуальні засади правового забезпечення інформаційної безпеки України в умовах євроінтеграції 301
5.2. Пріоритети розвитку правових основ державної політики України у сфері інформаційної безпеки 351
Висновки до розділу 5 377
ВИСНОВКИ 384
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 395
ДОДАТКИ 453

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

Інформаційна безпека	ІБ
Інформаційно-комунікаційні технології	ІКТ
Інформаційна зброя	ІЗ
Інформаційно-психологічний вплив	ІПВ
Російська Федерація	РФ
Європейський Союз	ЄС
Служба безпеки України	СБУ
Міністерство оборони	МО
Засоби масової інформації	ЗМІ
Національна безпека	НБ

ВСТУП

Актуальність теми дослідження. В умовах євроінтеграції України, з урахуванням побудови інформаційного суспільства, все більшої актуальності набувають питання правового забезпечення інформаційної безпеки – запобігання й усунення різноманітними засобами і способами загроз людині, суспільству, державі в інформаційній сфері. Однак у сучасному багатогранному та динамічному світі проблеми інформаційної безпеки набувають принципово нових рис, тепер вони виходять далеко за межі запобігання війн і збройних конфліктів. Сьогодні вони стали їх підґрунтям, першоджерелом, основним ресурсом та головною зброєю.

В українських реаліях ці проблеми стали очевидними у 2014 році з подальшою ескалацією конфлікту. У таких умовах стає пріоритетним осмислення сукупності інформаційних процесів у контексті правового забезпечення безпеки України. З огляду на це цілком природним вбачається пошук основоположних цінностей, цілей, інтересів та надбань в інформаційній сфері, які слугуватимуть орієнтирами європейської перспективи України, майбутнього розвитку українського суспільства, заснованої на інформаційних технологіях, закладуть фундамент подальшого розвитку інформаційного права в Україні.

У цьому контексті закономірно зростає роль правових механізмів у забезпеченні інформаційної безпеки України, потреба ефективного законодавчого врегулювання суспільних відносин, що виникають у досліджуваній сфері, визначення правових засад організації та координації дій суб’єктів забезпечення інформаційної безпеки України, розробці пріоритетних напрямів державної політики у сфері інформаційної безпеки. Дослідження інформаційної безпеки України з правничої точки зору пов’язане з формуванням якісної системи інформаційної безпеки, що відповідатиме сучасним вимогам та нагальним потребам України як

повноправного члена й надійного партнера європейської спільноти.

Обравши євроінтеграційний курс та визначивши вступ до НАТО своїм стратегічним пріоритетом, Україна має орієнтуватися передусім на стратегію розвитку країн-учасниць ЄС та НАТО в інформаційній сфері. Для нашої держави імплементація європейських стандартів правового забезпечення інформаційної безпеки держави є пріоритетним засобом інтеграції в європейський правовий простір.

Актуальність теми дослідження зумовлюється передовсім гостротою самої проблеми забезпечення інформаційної безпеки України, особливо її правового складника, сфокусованого на забезпеченні безпеки людини, суспільства й держави.

Дослідження даної теми важливе для розуміння специфіки інформаційної безпеки та її потужного впливу на подальший розвиток суспільства.

Основним теоретичним підґрунтям дисертаційної роботи стали пов’язані з проблематикою даного дослідження праці в таких галузях та таких вчених:

філософії: А. Бергсон, Г. Гроцій, Р. Ієрінг, Н. Макіавеллі, Р. Оуен, Плутарх, Платон, Б. Рассел, Сенека, Сунь-цзи, А. Сен-Сімон;

інформаційного права: І. Арістова, О. Баранов, К. Бєляков, В. Брижко, І. Бондар, С. Бондаренко, О. Довгань, С. Домбровська, М. Згуровський, О. Золотар, І. Корж, Р. Калюжний, Б. Кормич, О. Костенко, В. Клочко, О. Логінов, В. Ліпкан, А. Марущак, Є. Мануйлов, О. Морозов, А. Нашинець-Наумова, В. Остроухов, І. Панова, В. Пилипчук, В. Петрик, В. Політанський, М. Присяжнюк, Ю.Размєтаєва, В. Рубан, Ю. Руденко, Г. Сащук, Я.Собків, О. Тихомиров, В. Фурашев, С. Феденько, Л. Харченко, О. Хілько, В. Шамрай, Р. Шаповал, В. Шатун, О. Ярема та ін.

інших галузей права: вітчизняні вчені – Ю. Бисага, Д. Бєлов, О. Береза, Ю. Білак, В. Білоус, В. Горбулін, В. Григор’єв, В. Гулай, О. Дзьобань, Т. Карабін, А. Качинський, Я. Лазур, А. Легеза, Ю. Лісовська, І. Лях, Я.

Малик, Й. Мастяниця, С. Мельник, Н. Нижник, Д. Прокоф'єва-Янчиленко, Г. Ситник, М. Савчин, О. Соснін, Л. Шиманський; зарубіжні вчені: С. Алексєєв, Дж. Барбер, Н. Вінер, В. Герхард, К. Геерс, Дж. Данн, К. Демпсі, Л. Козер, П. Корніш, А. Кемпф Р. Оуен, В. Піллітгері, Б. Рассел, А. Робертс, Ф. Сталдер, М. Лібіскі, О. Лукашов, А. Левін, Х. Міллінгтон, М. Нільес, К. Шенон, К. Шилде, Р. Ярґер та ін.

Накопичений теоретичний і практичний досвід формування системи забезпечення інформаційної безпеки України демонструє значні суперечності у правовому регулюванні відносин, що виникають у національному інформаційному просторі. Проаналізувавши джерельну базу та осмисливши реалії створення системи правового забезпечення інформаційної безпеки України, виявлено теоретичні та практичні проблеми – від браку достатніх теоретичних основ правового забезпечення інформаційної безпеки України до відсутності системності й недостатньої ефективності відповідних практик.

Зв'язок роботи з науковими програмами, планами, темами. Дисертацію виконано відповідно до Пріоритетних напрямів розвитку правової науки на 2016–2020 рр., затверджених Постановою Загальних зборів Національної академії правових наук України від 03.03.16., Плану законодавчого забезпечення реформ в Україні, схваленого Постановою Верховної Ради України від 04.06.15 № 509-VIII, а також в рамках планових дослідницьких тем Науково-дослідного інституту інформатики і права Національної академії правових наук України "Теоретичні та організаційно-правові основи забезпечення кібербезпеки в Україні" (№ державної реєстрації 0116U007745) та «Теоретико-правові основи захисту прав, свобод і безпеки людини в інформаційній сфері» (№ державної реєстрації 0117U007745).

Результати дослідження було розглянуто та обговорено на науково-практичному семінарі в Науково-дослідному інституті інформатики і права Національної академії правових наук України, протокол від 14 вересня

2018 р.

Мета і завдання дослідження. *Мета* – формування теоретико-методологічних основ правового забезпечення інформаційної безпеки України в умовах євроінтеграції шляхом розвитку теоретичних засад інформаційного права та формування пропозицій щодо вдосконалення інформаційного законодавства.

Накреслена дослідницька мета асоційована з розв'язанням вагомої теоретико-практичної проблеми – розроблення концептуальних правових засад забезпечення інформаційної безпеки держави та практичних рекомендацій щодо вдосконалення механізмів її реалізації у контексті євроінтеграції України.

Досягнення поставленої мети передбачає розв'язання таких *завдань*:

- дослідити генезис наукових поглядів у сфері правового забезпечення інформаційної безпеки України;
- на основі понятійно-категоріального синтезу з'ясувати змістовну сутність основних понять дослідження;
- визначити об'єкт та предмет правового забезпечення інформаційної безпеки держави;
- охарактеризувати методологічні засади правового забезпечення інформаційної безпеки держави
- з'ясувати місце правового забезпечення інформаційної безпеки України у системі інформаційного права;
- класифікувати складові елементи та розробити систему інформаційної безпеки держави;
- узагальнити теоретичні підходи до змісту загроз інформаційній безпеці України та запропонувати механізми протидії їм в умовах євроінтеграції;
- дослідити практику діяльності суб'єктів забезпечення інформаційної безпеки України в умовах євроінтеграції;

- узагальнити досвід правового забезпечення політики інформаційної безпеки Північноатлантичного альянсу;
- з'ясувати особливості правового забезпечення інформаційної безпеки у нейтральних країнах Європи;
- дослідити досвід правового забезпечення інформаційної безпеки у країнах Європейського Союзу;
- запропонувати та обґрунтувати конкретні напрями вдосконалення правового забезпечення інформаційної безпеки в умовах євроінтеграції України;
- виокремити та обґрунтувати конкретні напрями державної політики у сфері інформаційної безпеки України.

Об'єкт дослідження – суспільні відносини у сфері інформаційної безпеки України.

Предмет дослідження – правове забезпечення інформаційної безпеки в умовах євроінтеграції України.

Гіпотеза дослідження ґрунтується на припущенні, що забезпечення інформаційної безпеки в умовах євроінтеграції України буде ефективною за умов її належного правового забезпечення та наукового обґрунтування відповідних рекомендацій удосконалення інформаційного законодавства.

Методи дослідження. Як методологічна основа дослідження використані філософські (діалектичний, метафізичний), загальнотеоретичні, (гносеологічний, структурно-функціональний), спеціальні (порівняльно-правовий, індуктивний) та міжгалузеві методи наукового пізнання (історичний, аналітичний), застосування яких зумовлюється системним підходом.

За допомогою *філософських методів*, які стали онтологічною основою дослідження, зокрема *діалектики*, досліджено інформаційну безпеку України як важливу складову національної безпеки держави, з'ясовано взаємозв'язки основних складових інформаційної безпеки держави, обґрунтовано взаємозалежність стану інформаційного

законодавства та правового забезпечення інформаційної безпеки України (підрозд. 1.1–1.4). У рамках *метафізичного методу* пізнання «інформаційна безпека України» розглядається крізь призму категорії істини, досліджена еволюція правового забезпечення інформаційної безпеки, досліджується її правова природа, зроблені прогнози розвитку інформаційного суспільства в Україні, визначені та охарактеризовані національні цілі та цінності в інформаційній сфері (підрозд. 2.1–2.3).

За допомогою *гносеологічного методу* дослідження з'ясовано поняття «інформаційна безпека держав», визначено його особливості, а також його інформаційно-правову природу (підрозд. 1.1–1.3, 2.1–2.3). *Історичний метод* дав змогу дослідити генезис теорій та концепції правового забезпечення інформаційної безпеки держави (підрозд.1.1). Використання *аналітичного методу* сприяло класифікації загроз інформаційній безпеці держав та розробці механізмів протидії їм (підрозд. 3.1., 3.2.), а також аналізу функціонування суб'єктів забезпечення інформаційної безпеки держави (підрозд. 3.3.). *Порівняльно-правовий метод* покладено в основу дослідження міжнародного досвіду правового забезпечення інформаційної безпеки держави (підрозд. 4.1.–4.3.). *Формально-юридичний метод* дав змогу дослідити компетенцію суб'єктів забезпечення інформаційної безпеки України (підрозд. 3.3.), а також застосовувався при тлумаченні норм права для з'ясування їх суті, змісту та вираженої в них волі законодавця (підрозд. 2.1.-2.2.). *Структурно-функціональний аналіз* дав можливість визначити відповідність нормативно-правових актів, з якими асоційована сучасна система правового забезпечення інформаційної безпеки держави, реальним суспільним відносинам у цій сфері та міжнародним стандартам (підрозд. 5.1., 5.2.). Використання *індуктивного методу*, *методів правового моделювання та прогнозування* дало змогу підтвердити висновок про необхідність удосконалення правового забезпечення інформаційної безпеки України, шляхом розробки та прийняття ЗУ «Про інформаційну

безпеку України» (підрозд. 5.1).

Наукова новизна. Робота є однією з перших у вітчизняній правничій науці досліджень правового забезпечення інформаційної безпеки в умовах євроінтеграції України. На цьому теоретичному та емпіричному ґрунті запропоновано розв'язання актуальної наукової проблеми – напрацювання концептуальних та правових засад забезпечення інформаційної безпеки України, а також практичних рекомендацій щодо вдосконалення механізмів її забезпечення в умовах євроінтеграції.

Основними науковими добутками даної праці стали:

Уперше:

- запропоновано та обґрунтовано включити до об'єктів правового забезпечення інформаційної безпеки України національні інтереси, цінності, цілі та надбання в інформаційній сфері;
- розроблено критерії оцінки негативного впливу загроз на стан інформаційної безпеки України, якими запропоновано вважати деструктивні трансформації національних цінностей в інформаційній сфері, що дає змогу створити правове підґрунтя відповідної методологічної бази;
- виділено у вітчизняній системі інформаційного права нову складову – забезпечення інформаційної безпеки України, а також проаналізовано причини й передумови її виникнення;
- класифіковано національні цінності та національні цілі в інформаційній сфері та аргументовано доцільність їх законодавчого закріплення;
- введено в доктрину інформаційного права термін «*національні надбання в інформаційній сфері*», під яким запропоновано розуміти сукупність унікальних інформаційних продуктів, що мають виняткове суспільне, економічне, військове та інше значення для реалізації національних цілей в інформаційній сфері;

- виділено у системі інформаційно-психологічної складової інформаційної безпеки України такі елементи як духовна, воєнна, соціальна, економічна, екологічна та глобальна безпеки та змістовно охарактеризовано взаємозв'язки між ними, що дало змогу врахувати сучасні загрози та розробити пріоритетні напрями державної політики забезпечення інформаційної безпеки України;

- на основі теоретичного доробку та практичних даних розроблено авторську модель системи інформаційної безпеки держави на основі поєднання національних цінностей, інтересів, цілей та надбань у сфері інформаційних правовідносин, яку втілено в авторському проекті Закону України «Про інформаційну безпеку України».

Удосконалено:

- базові поняття дослідження: «інформаційна безпека України», «забезпечення інформаційної безпеки України», «правове забезпечення інформаційної безпеки України», що дозволить упорядкувати понятійно-категоріальний апарат інформаційного права;

- методологічні засади правового забезпечення інформаційної безпеки України у частині доцільності поєднання методів примусу і переконання;

- змістовну складову предмету правового забезпечення інформаційної безпеки України – його доповнено новими характеристиками: пов'язаність суспільних відносин з інформацією, інформаційною інфраструктурою і правовим статусом суб'єктів інформаційної сфери чи зумовленість нею; зв'язаність з об'єктами національних інтересів, цілей, цінностей в інформаційній сфері; зумовленість проявів відповідних загроз безпеці в інформаційній сфері;

- підхід до системно-функціонального аналізу суб'єктів правового забезпечення інформаційної безпеки України, що дало змогу обґрунтувати доцільність розширення координуючої функції

уповноваженого органу у сфері забезпечення інформаційної безпеки держави;

- пріоритетні напрями розвитку правових основ державної політики у сфері інформаційної безпеки з урахуванням досвіду європейських країн та сучасної обстановки у нашій державі.

Набули подальшого розвитку:

- теорія інформаційного права та забезпечення інформаційної безпеки України в частині утвердження інформаційного права як самостійної галузі права та розширення меж його правового впливу;

- теоретичні положення щодо еволюції інформаційно-правових досліджень правового забезпечення інформаційної безпеки України та інформаційного права як галузі права;

- теоретичні підходи про зміст, динаміку розвитку сучасних загроз інформаційній безпеці України та оптимальні правові механізми протидії їм;

- узагальнення зарубіжного досвіду правового забезпечення інформаційної безпеки держави, що створює правову базу побудови системи інформаційної безпеки в Україні, здійснення гармонізації національного законодавства з міжнародним правом та європейським законодавством, а також розроблено пам'ятку для посадових осіб органів державної влади та місцевого самоврядування «*Як не стати жертвою шпигунських посягань*».

Практичне значення одержаних результатів. Висновки й пропозиції були впроваджені та можуть бути використані:

у правотворчій діяльності – при підготовці змін і доповнень до законодавчих та відомчих нормативно-правових актів, що стосуються питань забезпечення національної та інформаційної безпеки. Зокрема, при підготовці проекту Закону України «Про національну безпеку України» (*довідка підкомітету з питань державної безпеки Комітету Верховної Ради України з питань національної безпеки і оборони № Д-023/385 від*

14.06.18);

у правозастосовній практиці – при вдосконаленні практики забезпечення інформаційної безпеки людини, суспільства і держави в частині попередження протиправної діяльності спеціальних служб іноземних держав *(акти впровадження від 31.05.18 та від 20.06.18)*;

у науково-дослідній діяльності – як основа для подальших теоретичних і практичних розробок ефективної системи забезпечення інформаційної безпеки, а також опрацювання проблемних питань інформаційного права. Окремі положення дослідження враховано в науково-дослідній роботі Науково-дослідного інституту інформатики і права НАПрН України *(акт впровадження від 21.06.2018 р.)*;

у навчальному процесі – під час розробки та оновлення навчально-методичного забезпечення навчальних дисциплін «Інформаційне право».

Особистий внесок здобувача. Висновки та пропозиції, що становлять наукову новизну дисертації, розроблені автором самостійно. Для обґрунтування деяких висновків використано праці інших учених, на які обов'язково зроблено посилання. Із наукових праць, опублікованих у співавторстві, використано лише ті ідеї та положення, які одержано особисто здобувачем. Особистий внесок автора в наукові праці, виконані у співавторстві, становлять: ризик-діяльність у сфері захисту інформації з обмеженим доступом (60 %); соціальна складова менеджменту у системі захисту інформації з обмеженим доступом (60 %); стан інформаційної безпеки України та основні завдання недержавних суб'єктів по її забезпеченню (30 %); система інформаційної безпеки України: онтологічні виміри (70 %); правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс (70 %), наукова рефлексія інформаційної безпеки України: від позитивізму до метафізики права (80 %).

Апробація результатів дисертації. Результати досліджень, викладені в дисертації, були представлені у вигляді доповідей та виступів на

наукових заходах:

міжнародні науково-практичні конференції: «Актуальні питання взаємодії інститутів громадянського суспільства та органів публічного адміністрування у напрямку розвитку правової системи України» (Київ, Центр правових наукових досліджень, 11–12.09.15); «Розвиток України в 21 ст. : економічні, соціальні, екологічні, гуманітарні та правові проблеми» (Тернопіль, 30.03.12); «Розвиток гуманітарних наук. Проблеми і перспективи» (Катовіце, 28–30.09.12); «Pravna veda a prax: vyzvy modfrnych europskych integracnych procesov» (Гданськ, 27–28.11.17); «Пріоритетні напрями наукових досліджень (Київ : МЦНД, 15-16 серпня 2017 року 2017); «Сучасні правові системи світу: тенденції та фактори розвитку» (Запоріжжя, 25–26.09.17); «Верховенство права та правова держава» (Ужгород, 15–16.09.17); «Science, research, development state and law» (Лондон, 27.02.18); «Сучасна юриспруденція Європейського Союзу: взаємодія права, нормотворчості та практики» (Люблін, 17.04.18); «Освіта і наука у сфері національної безпеки: проблеми та пріоритети розвитку (Острог, 01.12.17);

всеукраїнські науково-практичні конференції: «Актуальні проблеми забезпечення інформаційної безпеки держави» (Київ, НА СБУ, 20.03.09); «Актуальні проблеми управління інформаційною безпекою держави» (Київ, НА СБУ, 17.03.10; 20.03.14; 19.03.15; 24.05.17; 30.03.18); «Політико-правові реформи та становлення громадянського суспільства в Україні» (Херсон, 9–10.10.15); «Інтернет речей: проблеми правового регулювання та впровадження» (Київ, 24.10.17); «Кібербезпека в Україні: правові та організаційні питання» (Одеса, 17.11.17); «Теоретико-правові основи формування та розвитку інформаційного суспільства» (Київ, 29.11.17); «Безпекотворення: питання теорії, практики та правові аспекти. Тема року: Формування безпекового середовища України як передумова розвитку бізнесу (Київ, 13.12.17); «Кібербезпека у системі національної безпеки України: пріоритетні напрями розвитку» (Маріуполь, 26.04.18); «Україна

та національні інтереси в глобалізованому світі: візія націоналістів» (Київ, 09.02.18); «Права, свободи і безпека людини в інформаційній сфері» (Київ, 10.05.18); «Освіта і наука у сфері національної безпеки: проблеми та пріоритети розвитку» (Острог, 08.06.2018).

Публікації. Основні положення та висновки дисертації викладено в 64 наукових працях, зокрема в 1 індивідуальній монографії, розділи в 1 підручнику, глави у 6 навчальних посібниках, у 26 статтях, що опубліковані у фахових виданнях України, наукових періодичних виданнях інших держав і наукових періодичних вітчизняних виданнях, що включені до міжнародних наукометричних баз даних (у тому числі 5 – у наукових періодичних виданнях інших держав), у 23 тезах доповідей на конференціях, у 6 наукових працях, які додатково відображують результати дисертаційного дослідження.

Структура дисертації зумовлена метою й завданнями дослідження та складається із вступу, п’яти розділів, що містять 15 підрозділів, висновків до кожного розділу та загальних висновків, списку використаних джерел і додатків. Загальний обсяг дисертації становить 486 сторінок, з яких основного тексту – 394 сторінок. Список використаних джерел налічує 533 найменувань і становить 59 сторінок, додатки – 33 сторінок.

РОЗДІЛ 1.
ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ ЯК ОБ'ЄКТ НАУКОВОГО ПІЗНАННЯ

1.1. Генезис правового забезпечення інформаційної безпеки людини, суспільства, держави

За останні роки парадигма інформаційної безпеки нашої держави суттєво змінилася. Насамперед трансформовано саму природу, а відповідно і стратегічний вимір концепції забезпечення інформаційної безпеки держави. При цьому інформаційна безпека України постає не як щось віртуальне, абстрактний об'єкт наукового пізнання, а як абсолютно реальна субстанція, в межах якої точаться запеклі бої, існують очевидні загрози з явними наслідками. Можемо упевнено стверджувати, що в Україні створюється своя модель інформаційної безпеки, яка ґрунтується виключно на власному досвіді як правового, так і оперативного її забезпечення. Ця модель почала будуватися в надзвичайно складний період державотворчих процесів, під час практично неоголошеної війни з Росією. Отже, серед зовнішніх чинників, що спонукають до розробки та впровадження власної концепції забезпечення інформаційної безпеки України, найбільш суттєвим убачається процес підриву за допомогою інформації традиційних цінностей країн та народів і нав'язування чужого світосприйняття.

Сучасні наукові підходи до концепції інформаційної безпеки ґрунтуються на багатій філософській базі, розвиток якої починається ще з давніх часів. Мислителі різних епох завжди шукали причини і джерела

небезпек, прагнули домогтися стійкого миру, безпеки та процвітання, в ході чого й змінювалися погляди на інформацію. Питання безпеки особи, суспільства, держави та отримання достовірної інформації про це хвилювала філософів Стародавнього світу. Щоправда, вказана проблема розглядалася переважно в контексті війни й миру [1, с. 40]. Водночас слід підкреслити, що для філософської культури Стародавнього світу був характерний синкретизм, тобто для тогочасної наукової думки не існувало розподілу між сферами духовної діяльності людини.

1.1.1. Першоджерела інформаційної безпеки

Коли йдеться про інформаційно-комунікаційні технології, передовсім маються на увазі засоби зв’язку чи, швидше, канали зв’язку. З найдавніших часів зв'язок асоціювався з магією. Одним з різновидів магії був звук. Людський голос (звук, який видається людиною) вважався магічним за своєю природою. У книзі Буття Адам виконував магічну за своєю суттю дію, даючи найменння рослинам і тваринам. Таким чином він підтверджував дану йому Богом могутність, а проголошення назв стало справжньою демонстрацією магічних можливостей. Самі імена теж наділялися магічною силою. Так, у древньому іудаїзмі ім’я Бога само по собі було ототожненням могутності, а промовляти його міг лише первосвященик раз на рік, перебуваючи наодинці у найсвятішій частині Храму. У багатьох культурах особи, які проходили певні ритуали посвячення, отримували нові й часто втаємничені імена. За давньою ірландською легендою поет, котрий мав магічну здатність управляти мовою, міг прокляти будь-яку людину, давши їй ім’я із «вплетеним» у нього прокляттям.

Якщо зв'язок вважався за своєю природою магічним, то аналогічним було ставлення й до процесу підтримки цього зв’язку. До прикладу,

давньоєгипетський бог Тот «опікувався» як магію й мудрістю, так і писемністю, причому різниці між цими поняттями практично не існувало. У древньоєврейському алфавіті, а пізніше й у Кабалі літери і слова самі по собі вважалися носіями магічної сили. Так, слова «*вимовляти*» та «*читати заклинання*» були синонімами. У багатьох стародавніх культурах ті, хто мав доступ до цієї особливої магії - до загадкових таємниць знаків і звуків, які забезпечували й оберігали зв'язок, – вважалися хранителями магії.

Чим менш доступними були засоби зв'язку, перетворюючись на прерогативу посвячених, тим більше вони асоціювалися з таємницею та магією. Відомо, що німецький гуманіст, лікар, алхімік, натурфілософ, окультист, астролог і знаний адвокат Агріппа Неттесгаймський листувався з ученими інших країн, а пізніше зміцнював свій імідж мага, видаючи отриману від них інформацію за повідомлення духів.

Абсолютно не принципово, що наш розум сьогодні звик сприймати ці речі як продукти технології, а не магії. До того як картезіанське мислення призвело до фрагментації знання, магія і технології були єдині. Нині вони залишаються нероздільними лишень у метафоричному сенсі. Проте, незалежно від термінології, багато хто й донині продовжує говорити про «мистецтво створювати події». Від Агріппи до нас пройшло дуже багато часу. Змінися й технології. Ми живемо в епоху цифрових технологій і вже не уявляємо нашого буття без Інтернету, електронної пошти та інших плодів технологічного прогресу. Проте і сьогодні, як сказав колись Уїнстон Черчілль, «*хто володіє інформацією, той володіє світом*». Тобто володіння інформацією залишається певним магічним дійством, здатним впливати на маси, результати парламентських чи президентських виборів, ставати збудником революцій, війн і т.д. І якщо цей світ являє собою найбільш яскраву на сьогодні демонстрацію магічної сили, то він також є потужною потенційною силою для маніпуляцій свідомістю, а це і є своєрідною магією. Якщо ж відбуваються якісь впливи на поведінку людини чи груп

людей, логічно постає й категорія «безпеки», котра в цьому разі матиме дуалістичну характеристику: безпека інформації як інструменту впливу та безпека від інформації, яка може вплинути. В обох випадках суб'єктний склад різний.

Історія інформаційної безпеки (хоча раніше її так не називали) сягає корінням сивої давнини. Приміром, ще цар Давид у своїй молитві промовляв: *«Ти погубиш тих, хто говорить брехню; кровожерним і підступним гребує Господь»* [2, с. 370]. Брехня в даному разі, як би ми сказали сьогодні, це – «дезінформація» чи «недостовірна інформація». Суб'єктів розповсюдження такої інформації Давид характеризує вельми суворо, що, вочевидь, означає тяжкість подібних діянь. Давньогрецький письменник, історик і філософ-мораліст Плутарх згадує звичай, коли кожного, хто входив до сессітії, старший, показуючи на двері, попереджав: «Жодне слово з них не виходить» [2, с. 181]. Це свідчить про розуміння неабиякої важливості вміння зберігати секрети в таємниці, а також про те, що вже тоді існували прототипи сучасних секретоносіїв. Своєю чергою, давньоримський філософ, поет та державний діяч Сенека у праці «Едип-цар» застерігає від використання недостовірної інформації, говорячи устами свого героя, що виявлення довіри віроломному - надати йому можливість шкодити [3, с. 142]. А сентенцією «безпека є запобіганням шкоді» Платон фактично говорить про інформаційну розвідку [4, с. 415].

Ведучи мову про інформаційну безпеку держави, неможливо обійти увагою духовного натхненника інформаційних війн китайського військового стратега й філософа Сунь-Цзи (313-239 рр. до н. е.), який написав першу у цій сфері фундаментальну працю під назвою «Мистецтво війни», де, зокрема, говориться: *«Якщо прогресивний володар або мудрий генерал отримує перемогу над противниками кожного разу, коли вони переходять до дії, то це досягається завдяки попередній інформації. Так звана попередня інформація не може бути отриманою ні від духів, ані від божеств, ні за аналогією з попередніми подіями, ані шляхом розрахунків. Її*

необхідно отримати від людини, знайомою із ситуацією супротивника» [5, с. 93]. В основі концепції Сунь-Цзи лежить теорія управління ворогом: «*його заманюють в пастки вигодою, позбавляють хоробрості, послаблюючи й виснажуючи перед атакою*» [5, с. 10].

Якісно новий етап формування елементів науково-філософських концепцій безпеки пов'язаний з епохою Відродження. У центрі уваги передових мислителів цього періоду стояла людина, її духовне життя (інформаційна сфера), її звільнення з-під церковного гніту й соціальної несправедливості. Осмислення умов безпечного гармонійного розвитку особистості привела гуманістів до постановки питання про усунення з життя людей найбільшого зла - війни. Народженню ідеї вічного миру сприяло, безперечно, перетворення війни у все більшу загрозу для народів Європи. Удосконалення зброї, створення численних армій і воєнних коаліцій, багаторічні війни, що продовжували роздирати європейські країни у ще ширших масштабах, аніж раніше, змусили мислителів епохи Відродження задуматися над проблемою безпечних міждержавних стосунків і шукати шляхи їх нормалізації, зокрема, шляхом обміну інформацією стосовно безпекових питань.

У XVI столітті італійський мислитель Нікколо Макіавеллі сформулював інформаційно-психологічну концепцію державної влади, де виклав основні принципи інформаційного протиборства в політичній сфері [6]. Крім того, історія багата прикладами проведення потужних інформаційно-пропагандистських акцій, класичних варіантів глобальної дезінформації народу, які відіграли свою фатальну роль.

На початку XVII ст. здійснюються спроби юридичного впорядкування міждержавних відносин. Одним із засновників теорії природного права й міжнародно-правової науки став голландський мислитель Гроцій Гуго де Гроот. Його трактат «Про право війни і миру», присвячений передусім проблемам міжнародного права, містить основні положення цієї галузі: договори між державами, які дотримуватимуться

через природний закон, мають замінити владу Папи Римського; слід заборонити несправедливі війни, що порушують будь-чиє право; воюючі сторони зобов'язані утримуватися від винищення ворожої власності й жорстокості щодо цивільною населення. Г. Гроцій пропонував також заснувати орган для розв'язування суперечок між державами, який би мав ефективні (у тому числі інформаційні) засоби примусу [7, с. 145-147]. Заслуга основоположника науки міжнародного права полягала й у тому, що він, розуміючи складність усунення збройного насильства, розвивав ідеї його гуманізації, обміну інформацією та регулювання відносин між державами на користь миру й безпеки.

У XVII ст., коли завершувалося становлення більшості національних держав Європи, окреслився етап обґрунтування ідеї «вічного миру». На відміну від «християнського миру», що містить у собі релігійну нетерпимість і апологетику, а то й заклик до боротьби з невірними, більшість проектів «вічного миру» відображали успіхи емпіричної філософії й раціоналістичний підхід. У таких проектах часто фігурував «державний інтерес» у створенні міцного миру й забезпеченні стійкої безпеки як реальної передумови процвітання молодих держав. Ідеться про «Політичний заповіт» А.-Ж. Рішельє, «Досліди» Ф. Бекона та ін.

Наукове ж обґрунтування проблеми національної безпеки взагалі, й інформаційних її аспектів зокрема, в сучасному розумінні й певні напрямки її вирішення містяться у працях Томаса Гоббса та Іммануїла Канта. Як слушно зазначає український дослідник проблем безпеки О.Дзьобань, погляди Гоббса й Канта на сутність досліджуваної проблеми є найбільш характерними в даному контексті [8, с. 41]. Розуміючи як природний стан беззаконня й наявності у кожного права на все, Кант та Гоббс приходять до необхідності встановлення громадянського устрою, за якого забезпечувалася би безпека індивіда. Попри принципові розбіжності у поглядах філософів на процесуальні аспекти досягнення безпечного стану, їхні теорії збігаються у тому, що споконвічно притаманна індивідам

повна свобода обмежується ними (теоріями) заради безпеки в усіх аспектах її розуміння, але безпека дає змогу цю свободу реалізувати.

Фундаментальні ідеї гоббсівського й кантівського вчень про безпечне існування особи, суспільства й держави, способи забезпечення миру й безпеки набувають особливої актуальності в сучасних умовах інтенсивного розвитку загальноєвропейського й світового процесу в напрямку визнання й поступового ствердження ідей панування права, принципів свободи й рівності. Міркування цих мислителів стосовно проблем безпеки продовжують відігравати величезну роль в усвідомленні того, де ми знаходимося й куди маємо рухатися, аби вийти на правильний шлях до майбутнього безпечного існування. В сучасних умовах пошуку оптимальних варіантів розв'язання проблеми забезпечення безпеки індивідів, суспільств, держав та їх союзів органічне поєднання раціональних зерен обох наведених теорій, безумовно, сприятиме віднайденню того оптимального стану й способу забезпечення інформаційної безпеки, який буде прийнятним для різних суспільних утворень у багатополюсному сучасному світі.

Ідеї безпеки у період раннього Просвітництва знайшли своє відображення у філософській і політичній творчості Джона Локка. Розробкою філософських питань безпеки через релігійно-етичне розуміння проблеми миру займалися в епоху Просвітництва Ф. Вольтер, Д. Дідро, гоббсівську позицію підтримував Ж.-Ж. Руссо; в період німецької класичної філософії - Й. Фіхте та Й. Гердер, котрі під різними кутами зору розглядали ідею забезпечення безпеки через обґрунтування державного суверенітету.

Багато цікавих ідей щодо вирішення безпекових проблем висунули соціалісти-утопісти Клод Анрі де Рувруа Сен-Сімон, Шарль Фур'є і Роберт Оуен. Так, Сен-Сімон - французький мислитель, соціолог, один із засновників утопічного соціалізму - запропонував ідею своєрідної колективної безпеки народів. Він уважав, що його філософська система,

котру він назвав «новим християнством», «оновленою релігією», є інформаційним підґрунтям, покликаним «створити для всіх народів стан вічного миру й безпеки, об'єднуючи їх проти тієї нації, яка побажала би досягти свого власного блага за рахунок загального блага всього людства. Таке досягнення здійснюється шляхом об'єднання їх (народів) проти всякого уряду, який пройнятий антихристиянським духом до такої міри, щоб загальнонаціональні інтереси принести в жертву приватним інтересам правителів» [9, с. 411]. Очевидно, що така ідея, як на той час, так і сьогодні, не є обґрунтованою і для наукового аналізу серйозно сприйматися не може.

Валлійський філософ, педагог та соціаліст-утопіст Роберт Оуен уважав, що початок якісно нового безпечного стану - вселюдської гармонії - може покласти лише належним чином організоване виховання людей на підставі доцільного застосування інформаційних аспектів виховного процесу Він підкреслював, що тільки звільнення народів від приватновласницького ярма й об'єднання їх в один союз покладе край насильству й уможливить забезпечення безпеки [10, с. 375]. Окремі елементи теорії Р. Оуена (які стосуються союзницьких лозунгів) спостерігаються сьогодні в умовах глобалізаційних тенденцій, однак поєднати в єдиний науковий підхід його розуміння принципів виховання і принципів об'єднання людей вельми проблематично, а тому можливості застосування даної точки зору для сучасного розуміння проблем інформаційної безпеки достатньо обмежені.

Французький філософ Анрі Бергсон, поєднуючи інформаційну безпеку з розумінням закритого й відкритого суспільств, зазначав, що насильство й війни є неминучим наслідком закритих суспільств і, отже, сумною необхідністю епохи. Єдину можливість подолання проявів насильства, несправедливості, роз'єднаності людей і досягнення безпечного стану існування людства він убачав у пропаганді «духу простоти», сповіщеного християнськими містиками, принципів аскетизму, у відмові від «штучних

потреб», спричинених переважанням розвитку в останні століття «тіла» людства, а не його «душі» [11, с. 269].

Англійський філософ, логік і мораліст Бертран Рассел у своїх численних творах попереджав людство, що настав вирішальний момент історії, коли воно мусить зробити вибір: або загинути внаслідок війни (оскільки сучасна зброя вражає обидві сторони), або цю небезпеку перемогти. Розум повинен узяти гору над безглуздям, і особливе місце у даному процесі має належати формуванню та спрямуванню необхідних інформаційних потоків (впливів) [12, с. 77].

Мислителі різних епох засуджували насильство, пристрасно мріяли про вічний мир і безпеку, пропонували різні моделі здійснення своїх задумів. Одні з них звертали увагу насамперед на інформаційно-етичний бік проблеми (Августин Блаженний, І. Кант, Р. Оуен, А. Бергсон, А. Швейцер). Вони вважали, що агресія, війна є породженням аморальності, що безпечного стану можливо досягти тільки шляхом морального перевиховання людей у дусі взаєморозуміння, терпимості до різних віросповідань, усунення націоналістичних пережитків, виховання людей за принципом «усі люди - брати». Інші вбачали головну перешкоду для досягнення безпечного суспільного стану в господарській руїні, в порушенні нормального функціонування всієї економічної та інформаційної структур (Ціцерон), у колізії природного й громадянського станів особистості (Т. Гоббс, Дж. Локк). У зв’язку з цим вони намагалися схилити людство до миру й безпеки, малюючи картини загального процвітання в суспільстві без воєн, у якому пріоритет надаватиметься розвитку науки, техніки, мистецтва, літератури, інформації, а не вдосконаленню засобів знищення. Вони вважали, що міждержавну безпеку можна встановити завдяки розумній політиці освіченого правителя. Треті розробляли правові аспекти безпеки, досягти якої вони пропонували шляхом угоди між урядами, створенням регіональних або всесвітніх федерацій держав (Г. Гроцій, Сен-Сімон, К. Ясперс, А. Тойнбі). Четверті

переконували, що коріння небезпек має соціальний характер, що усунути їх можна, лише змінивши структуру суспільства (Еразм Роттердамський, С. Франк).

1.1.2. Інформаційна безпека на сучасному етапі державотворення

Цілком очевидно, що й сьогоднішні, й перспективні, адекватні соціальній дійсності наукові розвідки у сфері інформаційної безпеки без опори на класичну спадщину будуть досить сумнівними. Водночас, не менш очевидно, що творчість найвидатніших представників світової філософської думки, незважаючи на її беззаперечну цінність і неминущу актуальність, далеко не вичерпує усіх аспектів філософського осягнення проблеми інформаційної безпеки.

А преціньь, їх погляди є найбільш показовими як у своїй протилежності, так і в єдності, що може стати тим перспективним аспектом осмислення сутності інформаційної безпеки, навколо якого й будуватиметься майбутня система забезпечення інформаційної безпеки як на національному, так і на глобальному рівнях. Принаймні сучасні методологічні підходи до соціально-філософського аналізу феномена інформаційної безпеки мають увібрати в себе якомога більше позитивних елементів проаналізованої історичної спадщини. Ретроспективний аналіз даної проблеми потрібен для вибору перспективної методології дослідження питань інформаційної безпеки.

Нині у глобальному медіапросторі, в публіцистичних і наукових працях, а також у політичних і державних документах багатьох країн широкого вжитку набули терміни «інформаційна війна», «інформаційне протиборство», «інформаційний вплив», «інформаційна зброя» тощо. Інформаційно-комунікаційні технології (ІКТ) відіграють ключову роль у світовій політиці, економіці та системах безпеки. До інформаційних

диверсій у кіберпросторі сьогодні вдаються як організовані групи, так і окремі особи. Дедалі важливішою складовою військового потенціалу держав стає інформаційна зброя (ІЗ) як доповнення до власне військового арсеналу. При цьому за своїми наслідками інформаційні війни між державами можуть бути не менш руйнівними і жорстокими, ніж традиційні. Утім, і в давні часи психологічна перевага над ворогом подеколи була важливішою за його фізичне знищення. Так, ще понад дві тисячі років тому згадуваний вище китайський воєначальник, стратег і мислитель Сунь-Цзи наголошував, що «*війна – це шлях обману*», а отже: «…якщо ти й можеш щось, показуй противнику, начебто не можеш; якщо ти й користуєшся чимось, показуй йому, начебто ти цим не користуєшся; хоча б ти і був близько, показуй, начебто ти далеко; хоча б ти і був далеко, показуй, що ти близько» [5, с. 88].

Доба глобальної інформаційної революції значно розширила можливості для подібної діяльності. Мабуть, першим прикладом використання ІКТ у ході бойових дій стала операція «Буря в пустелі», проведена Сполученими Штатами Америки в Іраку в 1991 році. Новітній формат протистояння передбачав тривалий інформаційно-психологічний тиск і комплексне застосування засобів розвідки, управління, зв’язку, навігації та радіоелектронної боротьби. З кінця 1990-х років спостерігається послідовне зростання потужності інформаційних впливів у рамках операцій у Югославії (1999), Афганістані (2001), Іраку (2003), Лівії (2011); 2008 року під час збройного конфлікту в Грузії дієвий деструктивний інформаційно-психологічний вплив забезпечили західні держави. Наразі у протистояннях в Україні та Сирії реалізуються майже всі наявні методи інформаційного впливу.

При цьому на міжнародному рівні дотепер відсутні загальноприйняті визначення терміна «інформаційно-комунікаційні технології» і пов’язаних з ним понять. Процес юридичного оформлення понятійного апарату сфери ІКТ у глобальному правовому просторі триває, і, оскільки метою спільних

зусиль у зазначеному напрямі є узгодження численних термінологічних суперечностей, важливо простежити розвиток відповідної термінології в національних державних документах. З-поміж широкого спектра понять, прямо й опосередковано пов'язаних з проблематикою інформаційної безпеки, у цій роботі зосередимося лише на тих, що є найбільш значущими для її теми.

Дослідники питань інформаційної безпеки особливу увагу приділяють такому поняттю, як «інформаційна війна». Уперше цей термін використав науковий радник Міністерства оборони (МО) Сполучених Штатів Америки Томас Рона у звіті «Системи зброї та інформаційної війни», який він підготував у 1976 році для компанії «Боїнг» [13]. У цьому документі Т. Рона висловлює думку, що інформаційна інфраструктура як ключова складова економіки США стає вразливою ціллю як у воєнний, так і в мирний час. В офіційний обіг термін «інформаційна війна» ввів міністр оборони США в директиві від 21.12.1992 «Інформаційне протиборство» («Information Warfare») [14]. Отже, збройні сили Сполучених Штатів першими використали новітні інформаційні технології у війні в Перській затоці (1991), а після її завершення ключові персони військової сфери США, знову ж таки першими на світовій арені, на офіційному рівні сформулювали стратегічні засади інформаційного протиборства.

Подальший розвиток досліджуваних нами питань пов'язаний з іменем професора Мартіна Лібіцкі, фахівця з корпорації RAND (американський аналітичний центр, заснований 14 травня 1948 року в Санта-Моніка (Каліфорнія), вважається першим аналітичним центром у світі)[1]. У серпні 1995 року була оприлюднена його стаття «Що таке інформаційна війна?». Вже понад 20 років тому М. Лібіцкі писав, що психологічний вплив на противника під час військових дій використовується з давніх часів, проте у війнах нашої доби технічні методи і психологічні інформаційні операції мають однаково важливе

[1] https://www.rand.org/

значення й застосовуються в комплексі. Професор Лібіцкі запропонував одну з перших класифікацій інформаційних воєн. Він виокремлює сім різних аспектів цього феномена:

1) війна у сфері контролю та управління;
2) розвідувальна війна;
3) електронна війна;
4) психологічна війна;
5) хакерська війна;
6) економічна інформаційна війна;
7) кібервійна [15].

На реальному полі бою ведеться *війна у сфері контролю та управління*, спрямована на переривання каналів зв'язку між командуванням і виконавцями. Цей вид активності нападника має на меті порушення систем управління військами, ліній комунікацій і системи управління противника в цілому на стратегічному, оперативному й тактичному рівнях. У кінцевому підсумку сторона, що атакує, прагне домогтися цілковитої ізоляції командування від виконавців. Війна у сфері контролю та управління, за М. Лібіцкі, не є новим форматом для збройних сил Сполучених Штатів.

Розвідувальна війна надає можливість за допомогою інформаційних технологій отримати важливу військову інформацію та додаткові дані про противника. З іншого боку, захист власної інформації з використанням відповідних інструментів також є частиною розвідувальної війни.

Засоби електронних комунікацій, як-от радіозв'язок, радари, комп'ютерні мережі тощо, є цілями атак з боку противника в *електронній війні*. Одним із важливих її елементів вважають криптографію.

Психологічна війна сфокусована на впливі на свідомість людей. На думку М. Лібіцкі, ЗМІ є важливим засобом її ведення. Використання інформаційних можливостей і ресурсів у ході психологічної війни може набувати таких форм: культурний конфлікт, операції проти національної

ідеї, військового керівництва і збройних сил противника.

Натомість у *хакерській війні* об'єктом впливу є комп'ютерні мережі (КМ), а засобами впливу – шкідливе програмне забезпечення, у тому числі комп'ютерні віруси. Залежно від цілей та об'єктів такі операції можуть бути оборонного або ж наступального характеру. Атаки на КМ можуть як супроводжувати воєнні дії, так і провадитися в мирний час. Об'єктами хакерського впливу є комп'ютерні мережі військових, державних і приватних структур та інформаційних ресурсів.

Метою *економічної інформаційної війни* Мартін Лібіцкі вважає комерційну інформацію, припускаючи, що замість залежності держав від матеріального забезпечення й обміну прийде дедалі більша залежність від інформаційних потоків. Двома основними формами такої війни є інформаційна блокада та інформаційний імперіалізм [15].

На момент написання статті (1995 рік) розглядати *кібервійну* як реалії сучасного життя М. Лібіцкі вважав передчасним, а визначав її як інформаційну війну майбутнього. Відтоді ситуація змінилася, і нині експерти, аналізуючи деякі комп'ютерні атаки, зокрема застосування шкідливого програмного забезпечення на ядерних об'єктах Ірану у 2010–2012 роках, послуговувалися вже саме терміном «кібервійна».

Успішне ведення інформаційної війни неможливе без масиву надійних специфічних даних про супротивника, зауважує професор Лібіцкі. Накопичення цих знань включає аналіз ЗМІ противника, оцінку впливу мас-медіа на прийняття рішень на державному рівні, детальне вивчення бюрократичного апарату країни, національної комунікаційної інфраструктури, особливостей програмного забезпечення систем управління і т. ін. У цих умовах ґрунтовна підготовка фахівців для кваліфікованого провадження інформаційних операцій на всіх їхніх етапах набуває винятково важливого значення. Придушення противника не є пріоритетом діяльності таких фахівців – їхня головна мета полягає в забезпеченні інтересів *своєї* держави.

Праці М. Лібіцкі, одного з найвпливовіших американських дослідників і теоретиків в інформаційній сфері, стали базисом для концепцій і стратегій збройних сил Сполучених Штатів, а також відповідних документів Міністерства юстиції США. Його наукові інтереси дотепер охоплюють специфіку застосування ІКТ у системі національної безпеки. Зокрема, цю проблематику Мартін Лібіцкі висвітлює у статті «Криза й ескалація в кіберпросторі», оприлюдненій 2012 року Корпорацією RAND [16].

Дослідження М. Лібіцкі сприяли розробленню нових військових доктрин Сполучених Штатів Америки, як-от:

1) Директива міністра оборони США TS.3600.1, прийнята в 1992 році [14], де визначається поняття інформаційної війни, поставлені завдання перед міністерством оборони і комітетом начальників штабів (КНШ), окреслені питання розвитку форм і способів ведення інформаційної війни, порядок розробки статутних документів та проведення наукових досліджень;

2) «Доктрина боротьби із системами управління», уведена в дію Об'єднаним комітетом начальників штабів у лютому 1996 року [17];

3) «Об'єднана доктрина інформаційних операцій» міністерства оборони США, в якій наведено два базових поняття – інформаційна війна (information warfare) та інформаційна операція (information operation). Перше з них визначене як комплексний вплив (сукупність інформаційних операцій) на певного противника або кількох противників під час кризи чи конфлікту для вирішення поставлених завдань. Друге поняття стосується дій, до яких вдаються з метою ускладнення збору, обробки, передачі та зберігання інформації системами противника при захисті власної інформації та інформаційних систем [18].

Подальшого вдосконалення визначення поняття «інформаційна операція» набуло в керівних документах НАТО, ухвалених 1999 року. У них зазначений термін трактується як дії з метою *здійснення впливу на*

прийняття рішень шляхом впливу на інформацію, інформаційні процеси і системи управління противника при одночасному захисті своєї інформації та інформаційних систем для досягнення власних політичних і військових цілей. Згодом, у 2010 році, у словнику військових термінів Міністерства оборони США наведено розширене тлумачення цього терміна: «Інформаційна операція – інтегроване використання основних можливостей електронних методів протиборства, комп'ютерних мереж, інформаційної підтримки військових операцій, радіоелектронного придушення, дезінформації, забезпечення безпеки транзакцій спільно з технічною підтримкою й іншими можливостями для руйнування, спотворення, захоплення і впливу на процес прийняття рішень людиною та автоматизованою системою протиборчої сторони [19].

За декілька років у доктрині «Інформаційні операції» («Information Operations», 2014) Об'єднаного комітету начальників штабів США зміст терміна знову уточнюється; йдеться про планування, підготовку, виконання, а також оцінку інформаційних операцій як частини військових операцій. З огляду на перманентну мінливість стратегічної обстановки й інформаційного середовища обстоюється інтегроване використання в ході військових операцій усіх пов'язаних з інформацією можливостей поряд з іншими діями для руйнування, спотворення, захоплення і впливу на процес прийняття рішень противниками або потенційними противниками в ході захисту своїх інтересів [18]. Подібна ревізія понятійних рамок свідчить про невпинне зростання ролі інформаційної сфери в сучасному житті. Ефективне інтегрування всіх пов'язаних з інформацією можливостей в об'єднані операції, як відзначив голова Об'єднаного комітету начальників штабів США, створює умови для досягнення цілей командування.

У згадуваному раніше словнику військових термінів МО США під інформаційною підтримкою військових операцій розуміють операції, що плануються для передачі відібраної інформації та індикаторів зарубіжній аудиторії з метою впливу на її емоції, мотиви, міркування і врешті-решт -

на поведінку урядів іноземних держав, організацій, груп, окремих індивідів. Інформаційна підтримка військових операцій має на меті стимулювати або посилити наміри й поведінку цієї аудиторії, виходячи з цілей організатора операції [19].

Привертає увагу, що обговорювані поняття в сучасному термінологічному арсеналі американських військових експертів тлумачаться з акцентом на взаємозв'язок технічних і психологічних інформаційних методів. Це вказує на нагальну потребу в закріпленні відповідної термінології в міжнародних правових документах, а також є свідченням важливості офіційного визнання того факту, що в наш час ці методи знаходять широке застосування у кризах і конфліктах. Відтак, протидія різним формам інформаційного впливу поряд із забезпеченням надійного, безпечного і безперебійного функціонування інформаційних систем перетворюється на критично важливий чинник. Усвідомлення цього спонукало економічно розвинені країни до створення спеціальних державних структур, на які покладено відповідальність за забезпечення інформаційно-технічної та інформаційно-психологічної безпеки. До компетенції цих органів і структур належить також проведення інформаційних операцій.

Особливість сучасного розвитку суспільних відносин в Україні, як слушно зауважив І. Сопілко, полягає в тому, що становлення української державності відбувається паралельно, в умовах проголошення курсу на інтеграцію до Європейського Союзу, що сприяє системному реформуванню всіх галузей права відповідно до законодавства ЄС. Проте, при реалізації європейських планів виникає низка питань щодо вдосконалення правового регулювання інформаційних відносин. З-поміж цих питань, наприклад: розвиток масивів відкритих даних органів державної влади, адже відкриття даних змінює підходи до державного управління та стратегічного розвитку України; системи відкритих даних органів місцевого самоврядування; колізії щодо захисту даних від

протиправних посягань; електронне врядування та ін. [20, с. 61].

Щоб отримати перевагу над противником в економічній, політичній, військовій та/або іншій сфері, суб'єкт (суб'єкти) світової спільноти чи політичної системи вдаються до активного впливу на інформаційну сферу суб'єктів, яким протистоять. Такого роду взаємини називають *інформаційним протиборством*. Інформаційно-психологічне протиборство як певна методологія зміни картини світу в заданому напрямі стало нині однією з форм боротьби передових держав, що демонструє стрімкий розвиток. Об'єктом впливу можуть бути як окремі особи або групи осіб, котрі приймають рішення на різних рівнях (кожен на своєму), так і масова свідомість нації в цілому. У політичній сфері в інформаційно-психологічному протиборстві для впливу на думки, настрої і зрештою на поведінку протилежної сторони використовують інформаційні, дипломатичні, військово-демонстраційні, економічні та інші важелі.

З-поміж особливостей інформаційно-психологічного впливу принциповими вбачаються такі:

– *відсутність територіальних обмежень*, що дозволяє долати кордони між державами, уражаючи свідомість противника;

– *здійснення без видимих слідів*: об'єкт впливу вважає, що він самостійно ухвалює те чи інше рішення, насправді ж його скеровують до прийняття саме цього рішення;

– *відносна економічність* для ініціаторів, оскільки невелика за обсягом вхідна інформація може забезпечити максимально значущий результат, наприклад, формування потрібної громадської думки;

– *можливість різних* (аж до діаметрально протилежних) *інтерпретацій* одного й того ж факту;

– *неможливість блокування* дій противника в інформаційній боротьбі, навіть за умови наявності найсучасніших ІКТ (на відміну від симетричної відповіді в разі використання традиційних видів зброї).

Інформаційно-психологічна війна є найгострішою формою

протиборства в інформаційно-психологічній сфері, здійснюваного шляхом впливу на цю сферу противника з метою вирішення стратегічних завдань. Серед іншого це передбачає цілеспрямоване і планомірне використання інформаційно-психологічних інструментів та інших засобів (дипломатичних, військових, економічних та ін.) для впливу на думки, настрої і в кінцевому підсумку на поведінку противника з метою змусити його діяти в бажаному напрямі. Таким чином, *інформаційно-психологічний вплив (ІПВ) – це застосування інформаційно-психологічних засобів для впливу на психіку людини з метою коригування в потрібному для суб'єкта впливу напрямі і внесення змін до поведінки та/або світогляду*. Головним критерієм успішності ІПВ виступає результат цього процесу, що може виражатися у вигляді зміни настанов, поведінки, намірів та оцінок конкретного індивіда або групи осіб.

Основною формою ведення і головним елементом змісту інформаційно-психологічної війни є *інформаційно-психологічна операція – сукупність видів, форм і способів інформаційного впливу, узгоджених, скоординованих і взаємопов'язаних за цілями, завданнями, місцем, часом, об'єктами і процедурами.* Інформаційно-психологічні операції розрізняються за масштабами, цілями й завданнями, об'єктами впливу, використовуваними технологіями та умовами проведення. За термінами здійснення інформаційно-психологічні операції поділяють на:

- стратегічні (довгострокові);
- оперативні (середньострокові);
- тактичні (короткострокові).

За часом здійснення:

- на операції, що проводяться до переходу конфлікту в силову фазу;
- такі, що реалізуються в умовах активного зіткнення.

За спрямованістю виокремлюють операції:

- спрямовані безпосередньо проти реципієнта;

- такі, що проводяться в інтересах комунікатора, або операції проти третіх осіб з метою схилити їх на свій бік.

Своєю чергою, інформаційно-психологічні методи й засоби психотехнологій класифікують на відкриті й приховані (таємні), позитивні й негативні, такі, що переслідують явні та приховані цілі.

Таємні інформаційно-психологічні операції однієї держави або ж групи держав проти іншої (інших) реалізуються через здійснення спрямованого інформаційного впливу на індивідуальну, групову, масову свідомість, почуття, волю громадян, а також шляхом дезінформування суб'єктів прийняття політичних, економічних та іншого роду рішень і підриву інформаційної інфраструктури супротивної сторони.

Мета подібних операцій – створити умови, за яких у військовій, політичній, економічній та інших сферах країн – об'єктів інформаційно-психологічного впливу ухвалюватимуться управлінські рішення, вигідні для держав – організаторів цього впливу. Щоби сформувати такі умови, спеціально підготовлена інформація доводиться до об'єктів впливу за допомогою електронних, друкованих та інших засобів масових комунікацій, електронного й поштового зв'язку, аудіо-, відео- та кінопродукції, відкритих телекомунікаційних мереж, наочно-демонстраційних засобів і т. ін.

На сучасному етапі боротьби держав за сфери впливу акцент із явного застосування сили усе помітніше зміщується на використання більш гнучких засобів, основним із яких є контроль і керування інформаційними ресурсами. Для досягнення цих цілей в умовах зростаючої насиченості інформаційними й керуючими засобами, у тому числі й іноземного виробництва, може бути використане високоефективне таємне проникнення у програмне забезпечення державних інформаційних ресурсів. Українські правоохоронці постійно нагадують, що злочинці намагаються зламати інформаційні мережі й поштові сервери державних установ. Під виглядом офіційних листів над-

силаються електронні повідомлення із вкладеним шкідливим програмним забезпеченням, яке рекомендується встановити. Зокрема, СБ України неодноразово звертала увагу керівників державних органів влади та установ, а також співробітників ІТ-департаментів на необхідність посилення заходів з недопущення несанкціонованого встановлення програмного забезпечення чи його оновлення, аби не допустити хакерського проникнення на державні інформаційні ресурси.

Крім того, висока результативність використання інформаційно-телекомунікаційних систем і технологій, широкий спектр їх застосування і прихований характер дії зумовили те, що багато країн ведуть розробки в галузі теорії та практики їх застосування як інформаційної зброї і, як наслідок, - теорії ведення інформаційних війн.

Стрімкий розвиток технологій роботи з інформацією в розвинених країнах зумовлює формування стратегій «інформаційної війни», головною метою якої є інформація, оволодіння нею чи трансформація у своїх інтересах. Очевидним стає той факт, що в сучасних умовах інформаційні технології відіграють надзвичайно важливу роль не тільки в забезпеченні національної безпеки, а й у розвитку особистості, суспільства й держави.

Підсумовуючи аналіз теорій правового забезпечення інформаційної безпеки держави, зазначимо, що перші спроби людини зберегти таємність будь-якої інформації поклали початок формуванню теоретичних основ інформаційної безпеки. З розвитком технологій і обсягів передачі даних змінювалися методи захисту інформації. Як бачимо, на сучасному етапі розвитку суспільства ефективне забезпечення інформаційної безпеки дозволяє вирішувати ключові питання практично всіх видів національної безпеки. Інформаційна безпека є важливою складовою системи національної безпеки, і від успішного вирішення питань даної сфери залежить забезпечення глобальної загальносвітової безпеки.

1.2. Категоріально-понятійний синтез правового забезпечення інформаційної безпеки України

Сьогодення постає перед Україною з новими викликами та надскладними завданнями. Під час опору різноплановим проявам гібридної війни, розгорнутої Російською Федерацією, стало очевидним, що наразі наша держава стикнулася з життєвою необхідністю захисту фундаментальних національних цінностей – незалежності, територіальної цілісності й суверенітету держави, свободи, прав людини й верховенства права, добробуту, миру й безпеки, – а також у стислі терміни має забезпечити ефективне функціонування сектору безпеки й оборони в умовах обмежених ресурсів. Запорукою успішної протидії широкомасштабній зовнішній агресії та сталого розвитку інформаційного суспільства в Україні є сьогодні не лише нарощування технологічних можливостей здійснення інформаційного обміну, а й глибоке усвідомлення усіма суб'єктами інформаційних відносин необхідності здійснення усіх заходів захисту інформаційних ресурсів та забезпечення інформаційної безпеки держави [21, с. 45-46], що неможливо без чіткого усвідомлення сутності останньої. Цікавим є й той факт, що самі російські дослідники відзначають, що інформаційна безпека від другої половині XX сторіччя стає одним із найважливіших елементів національної безпеки [22, с. 21].

Ст. 17 Конституції України визначає, що «захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» [23], що свідчить про набуття категорією «інформаційна безпека» в нормативно-правовому аспекті конституційного статусу [24, с. 30].

Незважаючи на те, що напрямок наукових досліджень, предметом якого є питання інформаційної безпеки, почав формуватись у період

інтенсивної інформатизації, самé це явище існує стільки ж, скільки існує людство, дістаючи прояву в усіх сферах життєдіяльності суспільства. В повсякденному житті під інформаційною безпекою розуміють зазвичай необхідність протидії витоку інформації з обмеженим доступом, а також поширенню недостовірної інформації, однак застосування системного підходу дозволяє побачити відмінність наукового розуміння цієї проблеми від побутового [25, с. 174]. Серед головних напрямів досліджень проблем інформаційної безпеки в юридичній науці А. Марущак називає «визначення основних понять та категорій, які застосовуватимуться для унормування відповідних суспільних процесів» [26, с. 18].

Доктринальних визначень інформаційної безпеки існує сьогодні дуже багато, однак досі немає єдиної думки щодо її сутності [27-31]. За класифікацією В. Ліпкана, можна виокремити декілька підходів до визначення сутності феномену інформаційної безпеки, за якими під останнім розуміють: стан захищеності інформаційного простору; процес управління загрозами та небезпеками, що забезпечує інформаційний суверенітет України; стан захищеності національних інтересів країни в інформаційному середовищі або в інформаційній сфері; захищеність установлених законом правил, за якими відбуваються інформаційні процеси в державі; важливу функцію держави; суспільні відносини, пов’язані із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі; невід’ємну частину політичної, економічної, оборонної та інших складових національної безпеки [32, с. 25-30].

У свою чергу, О. Данільян, О. Дзьобань та М. Панов визначають це поняття як безпеку об’єкта від інформаційних загроз або негативних впливів, пов’язаних з інформацією, та нерозголошення даних про той чи інший об’єкт, що є державною таємницею [33, с. 165].

За визначенням В. Гурковського, інформаційна безпека України - це суспільні відносини, пов’язані із захистом життєво важливих інтересів

людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі, що є необхідною умовою збереження та примноження духовних і матеріальних цінностей державоутворювальної нації, її існування, самозбереження і прогресивного розвитку України як суверенної держави, що залежить від цілеспрямованої інформаційної політики гарантій, охорони, оборони, захисту її національних інтересів [34, с. 74].

Використовує категорію національних інтересів і О. Баранов, визначаючи інформаційну безпеку як стан захищеності національних інтересів України в інформаційному середовищі, за якого не допускається (або зводиться до мінімуму) завдання шкоди особі, суспільству, державі через неповноту, несвоєчасність, недостовірність інформації й несанкціоноване її поширення та використання, а також через негативний інформаційний вплив і негативні наслідки функціонування інформаційних технологій [35, с. 60-62]. Інформаційну безпеку як стан захищеності національних інтересів України в інформаційній сфері від загроз особі, суспільству, державі через неповноту, несвоєчасність інформації, несанкціоноване поширення та використання інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій визначають також В. Шатун та О. Гладун [36, с. 175].

Так само Р. Калюжний вважає, що інформаційна безпека – це вид суспільних інформаційних правовідносин стосовно створення, підтримки, охорони та захисту бажаних для людини, суспільства й держави безпечних умов життєдіяльності, спеціальних правовідносин, які пов’язані зі створенням, зберіганням, поширенням і використанням інформації [37, с. 18-19].

Н.Нижник, Г.Ситник та В.Білоус під інформаційною безпекою розуміють стан правових норм і відповідних їм інститутів безпеки, які гарантують постійну наявність даних для прийняття стратегічних рішень та захист інформаційних ресурсів країни [38, с. 21].

В.Ярочкін та Т.Шевцова вважають, що інформаційна безпека - це проведення правових, організаційних та інженерно-технічних заходів при формуванні та використанні інформаційних технологій, інфраструктури та інформаційних ресурсів, захисті інформації високого значення і прав суб'єктів, що беруть участь в інформаційній діяльності [39, с. 24].

В.Ліпкан, Л.Харченко та О.Логінов розглядають інформаційну безпеку як процес управління загрозами та небезпеками державними й недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України [40, с. 75].

А.Лукашов пропонує визначати інформаційну безпеку як функціонування системи засобів, що забезпечують захищеність інформаційних систем, котрі являють собою впорядковану сукупність як інформаційних ресурсів (не лише держави, а й фізичних та юридичних осіб), так і інформаційних технологій та комплексу програмно-технічних засобів, якими здійснюються інформаційні процеси в людино-машинному або автоматичному режимі. Встановлення та функціонування вказаної системи засобів спрямоване на забезпечення прав людини, інтересів суспільства та держави в інформаційній сфері [41].

К.Бєляков також зазначає, що під інформаційною безпекою слід розуміти не лише технологічну, але й правову захищеність інформаційної сфери суспільства, що забезпечує її формування та розвиток в інтересах громадян, організацій та держави в цілому [42, с. 255].

Близької точки зору дотримується Б.Кормич, котрий вважає, що інформаційна безпека - це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування й розвитку людини, всього суспільства та держави [43, с.].

Ю.Фісун характеризує інформаційну безпеку як «стан захищеності інформаційного середовища, що відповідає інтересам держави, який забезпечує формування, використання і можливості розвитку незалежно

від впливу внутрішніх і зовнішніх інформаційний загроз» [44, с. 90].

На думку І.Панаріна, інформаційна безпека – це стан інформаційного середовища суспільства і політичної еліти, що забезпечує його формування і розвиток в інтересах керівництва країни, громадян і суспільства [45, с. 128].

А.Тер-Акопов під інформаційною безпекою розуміє стан захищеності інформації, яка забезпечує життєво важливі інтереси людини [46, с. 33].

В.Шульга пропонує інформаційну безпеку розглядати через єдність таких ознак, як стан, властивість управління загрозами й небезпеками. Ці чинники забезпечують обрання оптимального шляху усунення загроз та мінімізації впливу негативних наслідків, зокрема у сфері інформаційної діяльності держави [47].

Останнє визначення в цілому відповідає й поглядам В.Лопатіна [48, с. 19], Г.Почепцова [49, с. 193], С.Расторгуєва [50, с. 14], Р.Хаби [51, с. 220], В.Рубана [25, с. 174], М.Згуровського [30, с. 12], Г.Ємельянова, С.Стрельцова [52, с. 17], М.Потрубача [53, с. 34] та багатьох інших дослідників, котрі розглядають інформаційну безпеку як стан, що характеризується відсутністю небезпеки, тобто чинників та умов, котрі загрожують безпосередньо індивідові, державі, спільноті з боку інформаційно-комунікаційного середовища. Такий підхід сьогодні найбільш поширений, і його можна вважати традиційним, що, втім, не означає відсутність у ньому істотних вад, що є слушним приводом для наукової полеміки.

Проте ми підтримуємо позицію І. Коржа, котрий вважає подібну постановку питання утопічною: оскільки соціум у процесі свого розвитку піддавався, піддається і піддаватиметься різним деструктивним впливам (загрози, небезпеки, виклики), які стають все складнішими для протидії та деструктивними за наслідками, стверджувати про «захищеність» соціуму буде надміру сміливо. Тут можна говорити про ступінь захищеності, але це

ускладнить розуміння вказаного феномена. На погляд ученого, більш реалістичним і адекватним є підхід, згідно з яким «інформаційна безпека держави являє собою збалансований стан функціонування інститутів держави і суспільства, за якого забезпечується мінімальний вплив негативних факторів на національні інтереси держави та її громадян в інформаційному просторі і тим самим забезпечується формування та розвиток цього простору в інтересах особистості, суспільства і держави». Як випливає з наведеного, негативний вплив завжди буде і він завдаватиме певної шкоди соціуму. Однак, за умови мінімізації цього негативного впливу, можна досягти належного функціонування вітчизняного інформаційного простору і його подальшого розвитку [54, с. 38].

Якщо звернутися до нормативного визначення інформаційної безпеки, то слід зазначити, що чинне законодавство України не містить відповідного розгорнутого тлумачення цього поняття, проте нормативні акти, які торкаються питань інформаційної безпеки, закономірно розглядають її в контексті більш загального поняття національної безпеки. Справді, в умовах сьогодення наявність та доступність достовірної інформації про стан та динаміку розвитку економічних, політичних, соціальних та інших процесів у суспільстві вирішальною мірою визначають можливості владних структур та суспільства в цілому щодо вироблення та реалізації ефективних рішень в геополітичній, військово-стратегічній, науковій, освітній, культурній, історичній та екологічній сферах, а за умов інтелектуалізації та інформатизації суспільства інформація та інформаційні комунікації стають факторами, здатними або забезпечити стратегічну стабільність та розвиток суспільства й держави в цілому, або роз’єднати та дестабілізувати суспільство [55-56]. То ж чим активніше розвивається інформаційна сфера, яка стала системоутворювальним чинником життєдіяльності суспільства, тим більше політична, економічна, оборонна та інші складові національної безпеки будь-якої держави залежатимуть від інформаційної безпеки, причому

надалі, в ході розвитку технічного прогресу, ця залежність зростатиме [57-58].

Відтак, інформаційна безпека є не лише самостійною складовою національної безпеки, а й невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки (зокрема, І.Бондар пропонує розглядати національну безпеку України в інформаційній сфері як інтегральну цілісність чотирьох складових – персональної, публічної (суспільної), комерційної (корпоративної) й державної безпеки [59, с. 72]), адже всі типи взаємовідносин між суб'єктами інформаційного суспільства ґрунтуються на споживанні й обміні інформацією. Як слушно зазначає з цього приводу В.Ліпкан, «національні інтереси, загрози їм, управління цими загрозами в усіх галузях національної безпеки знаходять свій вираз, реалізуються через інформацію та інформаційну сферу» [32, с. 25]. Відповідно, конструктивним шляхом визначення поняття «інформаційна безпека» дослідник уважає виокремлення його сутнісних ознак, які є похідними від поняття «національна безпека» [60, с. 210]. Таким чином, з'ясовуючи сутність інформаційної безпеки, передусім слід визначитися зі змістом категорії «національна безпека».

Термін «національна безпека» вперше був використаний президентом США Т. Рузвельтом у 1904 році як синонім поняття «оборона». Надалі цей термін використовувався у дослідженнях американських учених Г. Моргентау, Т. Моргана, Е. Мея, Б. Рассела, А.Уолферса та інших. Системне його застосування розпочалося в США відразу після Другої світової війни при розробці концепції національної безпеки та доктрини державної безпеки країни. Дещо пізніше був прийнятий закон про національну безпеку, який зобов'язав усі державні структури вести чітко визначену політику, а також була запроваджена нова державна посада - спеціальний помічник президента США з питань національної безпеки [61, с. 36]. Якщо спочатку поняття «національна безпека» стосувалося переважно питань забезпечення військової безпеки,

то згодом її почали розглядати як здатність держави захистити національні інтереси у певних зовнішніх та внутрішніх умовах, а також забезпечити збереження основних ідеалів людського суспільства, недоторканності, свободи та своєрідності. Зокрема, у США національна безпека трактується як такий стан суспільства, за якого «…Сполучені Штати зберігаються як вільна нація і дотримується недоторканність основних її інститутів і цінностей» [62].

Як зазначає Г. Новицький, у СРСР термін «національна безпека» не набув поширення насамперед через розуміння терміна «національна» як такого, що пов’язаний з певним етносом. Тому запровадження в політичний та науковий обіг в Україні запозиченого із західної політології поняття «національна безпека» спиралося на американську і французьку політологічні школи, які розглядають націю як співгромадянство, тобто, «політичну націю» [63, с. 116]. Перший офіційний підхід до проблем національної безпеки в Україні був представлений у Концепції (основах державної політики) національної безпеки України, схваленій Постановою Верховної Ради України в січні 1997 року [64]. Наступним важливим кроком в цьому напрямку було прийняття у 2003 році закону «Про основи національної безпеки України», відповідно до якого національна безпека України – це захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам [65]. Утім, таке визначення, як і інші базові визначення національної безпеки, квінтесенцією яких є «захищеність» або «стан захищеності», не є досконалим, адже під захищеністю зазвичай розуміють стан, за якого певний об'єкт «огороджується» від несприятливих впливів ззовні, перебуває у незмінному середовищі, зберігає свої властивості й характеристики, що досягається за допомогою захисту як системи заходів, спрямованих на нейтралізацію таких впливів [66; 67, с. 24]. Відповідно,

захищеність є статичною ознакою, котра звужує поняття безпеки, адже забезпечення безпеки припускає не тільки збереження існуючого стану, а і створення можливостей для виходу на новий, якісно вищий рівень розвитку. Зосередження ж уваги і сил на захищеності не мобілізує адаптаційні механізми суспільства, відмовляє йому у необхідності інновацій та орієнтує на консервацію статус-кво, на виживання, а не на розвиток та зростання [67, с. 20].

Погоджуючись з думкою А. Уолферса, який зазначив, що «безпека в об'єктивному сенсі передбачає відсутність загроз наявним цінностям, а в суб'єктивному – відсутність остраху з приводу того, що вказаним цінностям може бути заподіяно шкоду» [69], вважаємо принципово важливим, аби в ході реалізації стратегій безпеки наголос робився не на захисті та стані захищеності, а на збереженні цінностей та реалізації інтересів у обстановці різнопланових загроз.

Отже, національна безпека являє собою складне за своєю структурою явище, що включає як систему умов і факторів захисту національних інтересів, так і процес використання ресурсів і можливостей суспільства для збереження, підтримання і вдосконалення цих умов і факторів, що свідчить про можливість розглядати національну безпеку з позицій організаційно-структурного і функціонально-діяльнісного підходів.

За організаційно-структурного підходу національна безпека розглядається як певне утворення, система, що характеризується подільністю, відкритістю, адаптивністю та наявністю структури, мети й пріоритетів оптимальної взаємодії елементів [70, с. 86], для пізнання сутності котрої необхідно дослідити компоненти, з яких вона утворена. Такими складовими, зокрема, можуть вважатись об'єкти, рушійні сили, сфери національної безпеки тощо.

Основними рушіями системи національної безпеки є національні цінності, інтереси й цілі. Зазначені елементи визначають зміст, характер,

конфігурацію та спрямованість системи.

Під національними цілями слід розуміти пріоритети суб'єктивної діяльності, спрямованої на реалізацію національних інтересів за допомогою інструментальних державних механізмів [71, с. 127].

Інтереси зазвичай визначаються як усвідомлені потреби. Відтак, під національними інтересами традиційно розумілася сукупність життєво важливих інтересів особи, суспільства та держави, що виражаються у спрямуванні нації на збереження та сталий розвиток, а також становлять першопричину політичних дій та звершень, переломлюючись у вигляді економічних, політичних та інших доктрин, концепцій та програм [72, с. 140]. Слід звернути увагу на те, що інтереси, попри усталені визначення національної безпеки через поняття «захищеності інтересів», захищати не потрібно, натомість слід забезпечувати умови для їхньої реалізації, адже інтерес – це лише усвідомлена потреба, тоді як захисту потребують передусім відповідні цінності [73, с. 148; 74].

То ж головним елементом у тріаді рушійних сил є національні цінності, під якими в загальному вигляді розуміють ідеальні, матеріальні, соціальні й духовні блага, що задовольняють потреби й інтереси людей і сприяють прогресивному розвитку особи й соціальних утворень [75, с. 304]. Саме у цінностях виявляються інтереси суб'єктів суспільних відносин, зіткнення яких породжують загрози [76, с. 34].

Необхідність протидії загрозам зумовлює доцільність дослідження національної безпеки як процесу, тобто, з точки зору функціонально-діяльнісного підходу, відповідно до якого національна безпека розглядається як динамічне явище, котре постійно змінюється та еволюціонує. Цей підхід орієнтує на аналіз національної безпеки як процесу збереження й підтримання її сталого стану як єдиного утворення, оптимального розвитку всіх рівнів і сфер безпеки як цілого, що забезпечує захист національних цінностей в умовах можливого розгортання загроз, а також дозволяє оцінювати можливості суспільства й держави щодо

протидії загрозам, і також щодо вміння і здатності створювати інформаційні загрози противнику.

Зауважимо, що розуміння національної безпеки як процесу не ототожнює поняття «національна безпека» та «забезпечення національної безпеки», адже вони співвідносяться як об'єкт діяльності – позитивна цінність та власне діяльність, що провадиться за допомогою певних сил і засобів. Крім того, таке розуміння національної безпеки вказує на динамічний характер національної безпеки й на те, що вона є відкритою системою, яка перебуває у тісному зв'язку із середовищем та потребами людини, суспільства й держави. З точки зору функціонально-діяльнісного підходу забезпечення національної безпеки орієнтується не лише на боротьбу із загрозами як зовнішніми та сторонніми явищами, але й власне на безпеку як важливу соціальну цінність.

З урахуванням того, що пріоритетність того або іншого виду національної безпеки визначається об'єктивними факторами – ступенем потреби людей, соціальних груп, суспільства, держав, світового співтовариства у безпеці для збереження й розвитку себе, а також життєво важливих об'єктів і цінностей (природних і соціальних); зростаючою уразливістю людей і життєво важливих об'єктів і цінностей (природних і соціальних) без зосередження зусиль на зміцненні безпеки; наявністю широкого кола надзвичайних небезпек, яким повинна протистояти система безпеки [77, с. 42-43], – інформаційна безпека закономірно виходить на перший план у системі національної безпеки. Як зазначає з цього приводу М.Присяжнюк, лише та держава може розраховувати на лідерство в економічній, військово-політичній та інших сферах, мати стратегічну й тактичну перевагу, гнучкіше регулювати економічні витрати на розвиток озброєнь і військової техніки, підтримувати перевагу з ряду передових технологій, яка має перевагу в засобах інформації та інформаційної боротьби [21, с. 43]. Таким чином, *зміст категорії «інформаційна безпека», як і «національна безпека» в цілому, доцільно розглядати з точки*

зору функціонально-діяльнісного підходу, визначаючи її передусім як процес, а не «стан захищеності».

Зокрема, В. Ліпкан акцентує увагу на тому, що поняття процес означає послідовність станів, пов'язаність стадій їх зміни і розвитку, тобто, на відміну від «стану», «процес» акцентує увагу на моменті спрямованості у зміні об'єкта, цілепокладанні. Тоді як «стан» відображає лише один момент, певну мить безпеки, а отже не вичерпує її повністю [32, с. 33]. З цією точкою зору погоджується також О. Рижук, зазначаючи, що розглядати безпеку лише як стан недоречно, оскільки втрачається динамізм як самої безпеки, так і тієї системи, для якої безпека виступає функцію її подальшого розвитку й існування [78].

На основі аналізу різних підходів до визначення категорії інформаційної безпеки О. Золотар робить слушний висновок про недоцільність суворого дотримання однієї позиції. Найбільш відповідним, на думку дослідниці, є комплексний підхід, за яким інформаційна безпека визначається через її істотні риси, найбільш важливі основні функції, з урахуванням постійної динаміки інформаційних і соціальних систем [79, с. 145].

На наш погляд, інформаційна безпека - це унікальний феномен сучасного суспільства, формування якого має глобальне значення для всього людства, внаслідок чого життєво необхідно сформулювати його об'єктивне, практичне визначення.

Дійсно, інформаційна безпека - досить складний феномен, крім того, існують деякі умови, що створюють труднощі у визначенні даного поняття. Виділимо основні:

1. Інформаційна безпека - об'єктивний феномен, викликаний об'єктивними умовами розвитку соціуму. Його формування відбувається на тлі процесу інформатизації суспільства, який, в свою чергу, сам перебуває на стадії становлення і потребує подальшого уважного вивчення. Крім того, особливості інформаційної безпеки в Україні

пов'язані, перш за все, з реформуванням самої системи національної безпеки країни. В результаті існування перерахованих факторів виникають труднощі, що не дозволяють сформулювати досить повне визначення досліджуваного поняття.

2. Труднощі у визначенні поняття «інформаційна безпека», на наш погляд, обумовлені ще тим фактом, що феномен інформаційної безпеки досліджується в різних аспектах: технічному, правовому, психологічному, соціальному і ін. Учені, які розглядають цей феномен з точки зору своєї наукової галузі, наповнюють поняття «інформаційна безпека» власним змістом, тим самим ще раз підкреслюючи її багатогранну природу, що накладає деякі труднощі в процесі вироблення єдиного визначення. В результаті чого дослідження носять спеціалізований характер і розглядають інформаційну безпеку з певних наукових позицій. Філософський аналіз, проведений в рамках нашого дослідження, повинен узагальнити існуючі уявлення про інформаційну безпеку, з метою вироблення засобів і методів, що підвищують ефективність рішень поставлених перед нею завдань. Необхідність філософського осмислення інформаційної безпеки безперечна, тому що, тільки філософське вивчення на базі синтезу існуючих досліджень спроможне сформулювати єдине розуміння феномену.

Основні підходи до визначення інформаційної безпеки:

- гуманітарний: розглядає інформаційну безпеку з точки зору проблем, пов'язаних із забезпеченням духовного оновлення суспільства, дотриманням конституційних прав і свобод громадян у галузі інформаційної діяльності. Основні питання зазначеного підходу складають такі проблеми, як формування методологічних основ забезпечення інформаційної безпеки; становлення інформаційної безпеки як міждисциплінарної галузі наукового знання; розвиток правового регулювання; забезпечення безпеки масового, групового та індивідуального свідомості; дослідження місця і ролі інформаційної

безпеки в соціальних процесах сучасного суспільства;

- нормативний: характеризує ступінь правового, у першу чергу, законодавчому визначенні інформаційної безпеки;

- психологічний підхід розставляє акценти на психологічній складовій інформаційної безпеки. Психологічний підхід кардинально відрізняється від усіх існуючих, оскільки висуває на передній план суб'єкт інформаційної взаємодії людину, особистість, він абсолютно справедливо зазначає одну з сутнісних сторін інформаційної безпеки, якій властивий психологічний аспект. Однак трактування інформаційної безпеки, найбільш яскраво відображають точку зору даного підходу, на нашу думку, також є обмеженими, оскільки захист психологічного стану людини на тлі впливів інформаційних процесів - обов'язковий, іманентний, але не єдиний елемент інформаційної безпеки.

Важливо відзначити, що психологічний підхід останнім часом отримав активний розвиток, в результаті чого сформувався новий напрямок соціальної практики і наукових досліджень - інформаційно-психологічна безпека;

На наш погляд, практично для всіх дослідників при розробці визначення загальним було прагнення внести не тільки термінологічну, але й методологічну ясність у смислове значення поняття «інформаційна безпека». Так, виходячи з того, що сутність безпеки системи полягає в здатності зберігати свою цілісність і здатність розвиватися, реалізовуючи зазначені здібності в реальних умовах, в тому числі і в несприятливих (конфлікти, ризик, невизначеність та т. ін.), приходимо до головного методологічного висновку: система забезпечення безпеки, в нашому випадку - інформаційна, спрямована на реалізацію перерахованих адаптивних здібностей. Тому інформаційну безпеку варто розглядати як безпеку об'єкта в інформаційному середовищі і як безпеку інформаційної сфери.

У цьому процесі також має велике значення вже накопичений

позитивний досвід попередніх поколінь, як правило, закріплений в міфах, переказах, моральних нормах і принципах, інакше - культурі соціуму. Так, в сутнісному плані інформаційна безпека - це стан об'єкта (суб'єкта), при якому інформаційне середовище, в якому він функціонує, дозволяє зберігати можливість і здатність реалізовувати свої рішення, відповідно до цілей, спрямованих на прогресивний розвиток. Подібний стан рівноваги всієї системи визначається нами як стійкий.

Зазначене вище означає, що інформаційна безпека досягається не тільки за рахунок засобів, методів і заходів, спрямованих на захист інформаційного середовища і захист об'єкта (суб'єкта) від деструктивного впливу, але й через розбудову спроможності у об'єкта (суб'єкта) ухилятися від деструктивного інформаційного впливу. Таким чином, завдання забезпечення інформаційної безпеки полягає в тому, щоб створити оптимальні умови для функціонування інформаційної інфраструктури, головний елемент якої, не комп'ютер, але людина, міг прогресивно розвиватися і діяти, згідно зі своїми цінностями та цілями. Підкреслимо зазначену думку як вузлову в нашому дослідженні.

У кінцевому підсумку цінності, відображені в свідомості людини, формують її життєві цілі, світоглядні орієнтири, визначають потреби. Саме цінності задають основні критерії, що відповідають за вибір і обґрунтування дій соціального суб'єкта в процесі функціонування в інформаційній сфері. Ми висуваємо цінності в якості одного з ключових компонентів визначення «інформаційна безпека», що є характерною ознакою власного трактування поняття.

Виділений основний системоутворюючий зміст інформаційної безпеки, на нашу думку, визначає її як цілісний феномен. Підводячи підсумок нашим розробкам, виведемо власну дефініцію інформаційної безпеки.

Інформаційна безпека - стійкий стан інформаційної сфери, що забезпечує свою цілісність і захист об'єктів при наявності несприятливих

внутрішніх і зовнішніх впливів на основі усвідомлення людиною своїх цінностей, потреб (життєво важливих інтересів) і цілей розвитку.

Дане визначення в концентрованому вигляді виражає сутність поняття «інформаційна безпека». Аксіологічний, гносеологічний і онтологічний аспекти розкривають філософський зміст розглянутого визначення. Онтологічний аспект інформаційної безпеки фіксує ситуацію покликану боротися з ризиком, метою якої є забезпечення цілісності об'єкта і стійкого стану інформаційного середовища. Антропологічний аспект поняття виявляє забезпечення безпеки суб'єкта інформаційної взаємодії. Аксіологічна складова поняття «інформаційна безпека» відображає цінності і цілі, що визначають інформаційні потреби людини.

Дійсно, інформаційна безпека - складний феномен об'єктивного розвитку сучасної цивілізації, спрямований на сприяння гармонійному розвитку інформаційного суспільства. Забезпечення інформаційної безпеки, перш за все, потребує вивчення негативних результатів процесу застосування інформаційних технологій, дослідження причин їхнього прояву, що в кінцевому підсумку допоможе виявити способи їхнього подолання, тим самим формуючи безпечний стан інформаційного середовища.

Не вдаючись до поглибленого аналізу сучасних підходів до розуміння суті інформаційної безпеки держави, відзначимо, що з-поміж існуючих концептуальних підходів до трактування інформаційної безпеки, а саме: статичного (безпека як стан захищеності інформаційного середовища/інформації, система гарантій тощо), діяльнісного (безпека як процес її забезпечення, здатність держави ефективно захистити національні інтереси та цінності) та комплексного (безпека як стан і процес) найбільш прийнятним, зважаючи на практику забезпечення інформаційної безпеки держави в теперішній час, є останній. З позицій цього підходу інформаційну безпеку України доцільно розглядати як *стан, за якого в умовах дії реальних та потенційних загроз забезпечується*

самозбереження, сталий і прогресивний розвиток інформаційної сфери, зокрема захищеність інформаційної інфраструктури, інформаційного простору, інформаційних ресурсів, інформаційних процесів та їх суб'єктів, а також досягнення відповідних національних цілей та реалізація національних інтересів в інформаційній сфері. При цьому забезпечення інформаційної безпеки держави, на нашу думку, це *постійний процес діяльності компетентних органів, спрямований на запобігання, протидію загрозам інформаційній сфері, застосування активних заходів інформаційного впливу, а також сукупність умов такої діяльності, які реалізуються і здатні контролюватися тривалий час.* В основу даного підходу покладено принцип, відповідно до якого основною метою забезпечення інформаційної безпеки є створення безпечного інформаційного середовища. А для цього захищати національні інтереси й цінності, виходячи з виявлення загроз і намірів противника, замало. Даний підхід передбачає також протидію та активні контрзаходи у процесі забезпечення інформаційної безпеки держави.

Оскільки під дією інформаційних впливів можуть цілеспрямовано змінюватися світогляд та мораль як окремих осіб, так і суспільства в цілому, нав'язуватися чужі інтереси, мотиви, спосіб життя, на перший план виходить аналіз сутності та форм проявів сучасних методів прихованого агресивного впливу, виявлення дій, що мають цілеспрямований агресивний характер і які суперечать інтересам національної безпеки, вироблення механізмів протидії їм у всіх напрямах [80]. Запропоноване визначення базується на комплексному функціональному визначенні національної безпеки та врахуванні особливостей інформаційної сфери, а також акцентує увагу не лише на пасивній (протидія інформаційним загрозам) [81, с. 15-16], але й на активній складовій (створення інформаційних загроз) інформаційної безпеки. Останнє є особливо актуальним у світлі завдань, визначених Стратегією національної безпеки, щодо протидії інформаційній війні, яка

ведеться проти України [82].

Слід погодитися з О. Левіним, який вважає, що визначати інформаційну безпеку через захищеність не зовсім коректно. Вчений переконаний, що, дотримуючись загальновідомої тези «краща оборона - це напад», треба діяти активно, знищувати джерела інформаційної небезпеки. При цьому щодо змісту інформаційної безпеки варто використовувати не поняття «інтереси», а набагато більш фундаментальне поняття «цінності». На думку О.Левіна, в цінностях виявляються інтереси суб'єктів суспільних відносин, зіткнення яких породжують загрози [76, с. 34].

Інформаційна безпека держави це завжди сутнісно діалектичне поняття, оскільки безпека може існувати лише в контексті небезпеки, постійних загроз, постійного процесу виявлення цих загроз, їх локалізації, зменшення негативного впливу, прогнозу на майбутнє. А тому, правильним убачається твердження А. Нашинець-Наумової, що інформаційна безпека здатна до розвитку і саморозвитку, тому будь-яке наукове знання про неї набуває актуального значення. Інформаційну безпеку України можна інтерпретувати як сукупність життєво важливих умов функціонування суб'єктів (особи, суспільства, держави) в інформаційній сфері та суб'єктивних (правових, політичних, інформаційних, наукових, оперативно-розшукових) можливостей їх усвідомлення й контролю [83, с. 4, 10].

Попри таке її основне й найбільш поширене розуміння, «інформаційна безпека» (зокрема, і як об'єкт права) є поняттям неоднозначним. На це є дві основні причини. По-перше, фундаментальні закономірності розвитку матерії залишаються досі недостатньо дослідженими, що спонукає фахівців послуговуватися терміном «інформація» для опису маловивчених і часто непорівнянних явищ, пов'язаних з об'єктами матеріального світу, зокрема, із системами живої та неживої природи. По-друге, величезні потенційні можливості кібернетики, яка створила передумови для виникнення уявлень про самоорганізовані

системи як єдину форму існування матерії, наразі увійшли в суперечність з обмеженими операційними можливостями поняття «інформація» К. Шеннона [84], за допомогою якого досі намагаються розкрити гносеологію, генезис та онтологію цих систем. По суті, ця суперечність насправді була закладена ще Н. Вінером [85], котрий у своїх працях терміном «інформація» позначав «робоче тіло», за допомогою якого забезпечується управління. Одначе цей термін позначає дещо інші явища. Ми чітко бачимо, що головні підходи та концепції до розуміння основних сутностей інформаційної безпеки держави проходять етап від діалектичного пізнання до синергетичного їх розуміння.

Концепція інформаційної безпеки України, яка офіційно представлена на рівні законодавчих актів, наголошує на ключовій її функції у забезпеченні першорядних інтересів нашої держави, позаяк виключно інформаційне середовище слугує каналом реалізації загроз національній безпеці в усіх сферах діяльності держави. Розв’язання проблем інформаційної безпеки є актуальним завданням для сучасного суспільства в контексті забезпечення національної безпеки держави. Визначення місця інформаційної безпеки в системі чинників національної безпеки держави, дослідження її основних завдань і напрямів функціонування є важливим етапом вироблення ефективної стратегії у цій сфері.

1.3. Теоретико-правові основи визначення об’єкта та предмета правового забезпечення інформаційної безпеки України

У життєдіяльності будь-якого суспільства виокремлюють зазвичай чотири основні сфери. Кожну з них утворює сукупність суспільних відносин, об’єднаних за певною ознакою та об’єктом правового

регулювання:

1) Сфера матеріального виробництва - суспільні відносини, які утворюють матеріальну сферу. Об'єднані на тій підставі, що охоплюють виробничу діяльність, пов'язану зі створенням матеріальних благ, а також результати цієї діяльності, виробничу інфраструктуру.

2) Сфера політики - утворюється сукупністю суспільних відносин, що склалися у зв'язку з боротьбою за владу, можливість управляти справами суспільства, визначати напрями розвитку соціуму й використовувати для їх реалізації фінансові та інші ресурси держави. Ця сфера також охоплює політичні документи різних партій, ідеологію.

3) Сфера духовного життя - утворюється сукупністю суспільних відносин, що виникають у зв'язку з інтелектуальною діяльністю людей, а також результатами цієї діяльності - досягненнями науки й мистецтва, літератури, культурними цінностями.

4) Сфера соціального життя - утворюється сукупністю суспільних відносин, що виникають у ході забезпечення життєдіяльності людини, її відтворення.

В останні десятиліття відгалузилася ще одна сфера життєдіяльності суспільства - *інформаційна*, що зумовлює необхідність ревізії відповідного науково-теоретичного дискурсу, особливо в контексті безпекотворчої парадигми.

Історично належність до певних спільнот сприяла впровадженню засобів інформаційних комунікацій між людьми. Усвідомлення того, що вплив на засоби інформаційних комунікацій може зашкодити інтересам цих спільнот, зумовило виникнення такої категорії, як інформаційна безпека (ІБ). Своєю чергою, для правового забезпечення ІБ необхідно виробити узгоджене юридичне визначення цього терміна.

На сучасному етапі однією з найважливіших умов підтримання стратегічної стабільності на глобальному рівні є забезпечення інформаційної безпеки в усіх сферах життєдіяльності суспільства. Захист

інформації можна розглядати як сукупність тісно пов’язаних між собою завдань у галузях міжнародного права, організації управління, розроблення й розвитку технічних засобів, програмування, прикладної математики тощо.

В американському і європейському законодавстві поняття «інформаційна безпека» розкривається через низку принципів, що дає змогу визначати зміст законодавства в цій сфері й основні напрями його розвитку. Так, принципами інформаційної безпеки є:

1) *доступність* – доступ до інформації й функціонування системи, попри можливі перебої в електропостачанні, стихійні лиха, нещасні випадки або атаки;

2) *автентичність* – підтвердження особи користувача (включно з можливістю анонімності);

3) *цілісність* – відправлення, отримання чи зберігання інформації в повному обсязі й незмінному вигляді;

4) *конфіденційність* – захист комунікацій і розміщеної в них інформації від перехоплення й ознайомлення особами, які не мають на це права.

Зазначені поняття предметно тлумачаться в декількох законодавчих актах. Наприклад, конфіденційність – у законах про персональні дані, про телекомунікації, про електронний документообіг, про права споживачів в окремих сферах (фінансовій, медичній та ін.). Такий підхід дозволяє уніфікувати категорію інформаційної безпеки в сучасному законодавстві.

Нині мета інформаційної безпеки розглядається в широкому й вузькому сенсі. У першому випадку йдеться про інформаційну безпеку особистості, суспільства й держави, у другому – про безпеку самої інформації та каналів її прийому/передачі, а також про організаційні заходи щодо захисту від застосування противником інформаційної зброї (ІЗ) у ході бойових дій.

У широкому сенсі метою інформаційної безпеки є забезпечення

надійного і всебічного захисту особистості, суспільства в цілому, держави від загроз у вигляді організованих інформаційних потоків, спрямованих на деформацію громадської й індивідуальної свідомості. Отже, інформаційна безпека держави включає в себе збереження інформаційних ресурсів держави і захищеність особи та суспільства в цілому в інформаційному просторі.

Інформаційна сфера утворюється сукупністю суспільних відносин, пов'язаних з інформацією та інформаційною інфраструктурою як об'єктами інтересів індивіда, суспільства й держави.

Інформація є специфічним явищем у житті людини і суспільства. Комунікація становить основу виховання, освіти, формування особистості, впливу на неї. Через комунікаційні канали людина пізнає зміст соціальних і технічних норм, водночас отримує попередження про можливі негативні наслідки нехтування ними. То ж, з одного боку, інформація - це засіб адаптації людини і суспільства до умов існування, засіб накопичення знань про навколишній світ, на основі яких людина і суспільство обирають лінію поведінки задля задоволення своїх потреб, реалізації інтересів. З другого боку, інформація є засобом управління людиною, її поведінкою, діяльністю громадських організацій, органів державної влади, функціонуванням технічних систем тощо.

Інтенсивне впровадження засобів інформатизації, телекомунікації та зв'язку в людське життя, іманентна та повсюдна глобалізація суттєво узалежнили суспільство, окремі сфери його життєдіяльності від процесів виробництва, розповсюдження та використання інформації. Унаслідок цього інформація стала об'єктом різноманітних суспільних правовідносин.

Так, у сфері матеріального виробництва виділяється сектор, пов'язаний зі створенням і впровадженням сучасних інформаційних технологій, засобів інформатизації, телекомунікації та зв'язку, програмних продуктів, баз даних і знань. Обсяг фінансів, що обертаються на інформаційному ринку, вже перевищує сукупний обсяг відповідних

ресурсів на автомобільному і нафтовому ринках.

У сфері політичного життя сучасні інформаційні технології дали змогу істотно змінити способи ведення політичної боротьби. Інформаційне забезпечення стало важливою частиною державної політики з підтримання громадського діалогу, встановлення належної взаємодії між владою та суспільством. Набула поширення «війна компроматів»: за допомогою неправдивої/напівправдивої інформації протиборчі сили намагаються створити в населення потрібні образи (імідж) підтримуваних ними політичних діячів, забезпечують відданість певним політичним ідеям, формують вигідний для них світогляд тих чи тих соціальних груп.

У сфері духовного життя сучасні інформаційні технології суттєво змінили зміст інтелектуальної праці, підвищили її продуктивність, зробили її результати доступнішими суспільству. З розвитком новітніх засобів інформатизації сформувався попит на наукомісткі технології, які уречевлюють досягнення духовного життя людини, зріс також попит на розважальну продукцію, розширилися можливості просувати релігійні погляди, доносити й пропагувати їх великим групам людей.

У соціальній сфері сучасні інформаційні технології змінили способи реалізації соціальних функцій: нарахування й виплати пенсій, матеріальної допомоги, медичної діагностики, статистичного обліку тощо. Одночасно посилилася залежність добробуту й безпеки людини від достовірності інформації, що накопичується і зберігається у громадських і державних інформаційних системах, від здатності державних і громадських організацій забезпечити дотримання необхідного режиму використання інформації.

Національні інтереси в інформаційній сфері визначаються тією роллю, яку відіграє інформація, а також інформаційна інфраструктура в забезпеченні сталого розвитку нації в конкретних історичних умовах.

Національні інтереси в інформаційній сфері утворюються шляхом збалансування соціальних інтересів індивіда як особистості, інтересів

суспільства й держави, що реалізуються в інформаційній сфері, включно з їхніми інтересами у використанні інформаційної сфери для збереження національної ідентичності.

При цьому слід усвідомлювати, що соціальні *інтереси особистості* в демократичному суспільстві спрямовані насамперед на свободу поширення своїх переконань, інтелектуальної творчості, збереження недоторканності свого внутрішнього світу, свободу самовираження і самовдосконалення, свободу спілкування з іншими людьми, захист своєї свободи від її обмеження іншими людьми, громадськими організаціями та державою.

Інтереси суспільства спрямовані на використання інформації та інформаційної інфраструктури для забезпечення сталого розвитку соціуму.

Інтереси держави - на підвищення ефективності використання інформаційної сфери для виконання функцій управління справами суспільства.

Інтереси особистості, суспільства і держави полягають у збереженні етнічної ідентичності. Ці інтереси забезпечуються підтримкою певного правового статусу особистості, інституційних утворень суспільства і державних органів.

Забезпечення інформаційної безпеки - сукупність діяльності щодо недопущення шкоди властивостям об’єкта безпеки, зумовленої інформацією та інформаційною інфраструктурою, а також засобів і суб’єктів цієї діяльності. Структура цього поняття охоплює: предмет та об’єкт безпеки, загрози об’єкту безпеки, діяльність із захисту об’єкта безпеки від загроз, засоби і суб’єкти забезпечення безпеки.

Основними об’єктами інформаційної безпеки є пов’язані з національними інтересами інформація, інформаційна інфраструктура та правовий статус суб’єктів інформаційної сфери.

Суб’єктами забезпечення інформаційної безпеки є органи, організації та особи, уповноважені законом на здійснення відповідної діяльності.

Діяльність держави щодо забезпечення інформаційної безпеки, яка провадиться у правовій формі, становить суть правового забезпечення інформаційної безпеки.

У широкому розумінні *об'єктами правового забезпечення інформаційної безпеки України* передовсім виступають:

1. **Особа** (людина і громадянин), її права і свободи.

1.1. Право соби на збирання, зберігання, використання та поширення інформації.

1.2. Правова заборона незаконного втручання у зміст, процеси обробки, передачі та використання персональних даних.

1.3. Захищеність від негативного інформаційно-психологічного впливу.

2. **Суспільство** – матеріальні й духовні цінності.

2.1. Збереження і примноження у суспільстві духовних, культурних і моральних цінностей.

2.2. Забезпечення суспільно-політичної стабільності, міжетнічної та міжконфесійної злагоди.

2.3. Формування і розвиток демократичних інститутів громадянського суспільства.

3. **Конституційний лад, суверенітет і територіальна цілісність держави.**

3.1. Правові обмеження щодо інформаційної залежності, інформаційної блокади нашої держави, а також інформаційної експансії з боку інших держав та міжнародних структур.

3.2. Забезпечення ефективної взаємодії органів державної влади та інститутів громадянського суспільства у ході формування, реалізації та коригування державної інформаційної політики.

3.3. Побудова та розвиток інформаційного суспільства.

3.4. Забезпечення економічного та науково-технологічного розвитку України.

3.5. Формування позитивного іміджу України.

3.6. Інтеграція України у світовий інформаційний простір.

Зважаючи на той факт, що об'єктами інформаційної безпеки можуть бути свідомість та психіка людей, інформаційні системи різного масштабу й різного призначення, пропонуємо об’єктом правового забезпечення інформаційної безпеки держави розглядати:

- національні цінності в інформаційній сфері;
- національні інтереси в інформаційній сфері;
- національні цілі в інформаційній сфері.

Американські військові дослідники Ярґер Річард та Джордж Барбер, розглядаючи дану тріаду в системі забезпечення національної безпеки держави, визначають національні *цінності* як найменш рухомий і найстабільніший елемент системи. Цінності формуються під час історичного процесу, розвитку матеріальної та духовної культури суспільства, відповідають геополітичному спрямуванню країни. Національні *інтереси* - елемент порівняно динамічний, що формується на основі національних цінностей під впливом довгострокових тенденцій суспільного розвитку. Національні *цілі* - найрухливіший елемент [86].

Доктрина інформаційної безпеки України визначає та змістовно наповнює тільки **національні інтереси** в інформаційній сфері. Це, зокрема:

1) життєво важливі інтереси особи:

- забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації;
- забезпечення конституційних прав людини на захист приватного життя;
- захищеність від руйнівних інформаційно-психологічних впливів;

2) життєво важливі інтереси суспільства і держави:

- захист українського суспільства від агресивного впливу деструктивної пропаганди, передусім з боку Російської Федерації;
- захист українського суспільства від агресивного інформаційного впливу Російської Федерації, спрямованого на пропаганду війни, розпалювання національної та релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету й територіальної цілісності України;
- усебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності в доступі до достовірної та об'єктивної інформації;
- забезпечення вільного обігу інформації, крім випадків, передбачених законом;
- розвиток та захист національної інформаційної інфраструктури;
- збереження і примноження духовних, культурних і моральних цінностей українського народу;
- забезпечення всебічного розвитку і функціонування української мови в усіх сферах суспільного життя на всій території України;
- вільний розвиток, використання і захист мов національних меншин та сприяння вивченню мов міжнародного спілкування;
- зміцнення інформаційних зв'язків з українською діаспорою, сприяння збереженню її етнокультурної ідентичності;
- розвиток медіа-культури суспільства та соціально відповідального медіа-середовища;
- формування ефективної правової системи захисту особи, суспільства та держави від деструктивних пропагандистських впливів;

- створення з урахуванням норм міжнародного права системи та механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів, насамперед пропаганди;
- розвиток інформаційного суспільства, зокрема його технологічної інфраструктури;
- безпечне функціонування і розвиток національного інформаційного простору та його інтеграція у європейський і світовий інформаційний простір;
- розвиток системи стратегічних комунікацій України;
- ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування та реалізації державної політики в інформаційній сфері;
- забезпечення розвитку інформаційно-комунікаційних технологій та інформаційних ресурсів України;
- захищеність державної таємниці та іншої інформації, вимоги щодо захисту якої встановлені законом;
- формування позитивного іміджу України у світі, донесення оперативної, достовірної та об'єктивної інформації про події в Україні до міжнародної спільноти;
- розбудова системи іномовлення України та забезпечення наявності іншомовного українського каналу в кабельних мережах та у супутниковому мовленні за межами України.

Відповідно до аналізу Доктрини інформаційної безпеки України можна виділити чотири основні складові національних інтересів України в інформаційній сфері.

Перша складова – дотримання конституційних прав і свобод людини і громадянина щодо отримання інформації та користування нею, забезпечення духовного оновлення України, збереження та зміцнення моральних цінностей суспільства, традицій патріотизму, гуманізму, культурного й наукового потенціалу країни.

Друга складова – інформаційне забезпечення державної політики України, доведення до власних громадян і міжнародної спільноти достовірної інформації про державну політику України, її офіційної позиції щодо соціально значущих подій внутрішньодержавного й міжнародного життя, забезпечення доступу громадян до відкритих державних інформаційних ресурсів.

Третя складова – розвиток сучасних інформаційних технологій, вітчизняної індустрії інформації, в тому числі засобів інформатизації, телекомунікації та зв'язку, забезпечення потреб внутрішнього ринку відповідною продукцією і вихід цієї продукції на світовий ринок, а також створення належних умов для накопичення, зберігання й використання вітчизняних інформаційних ресурсів. Сьогодні тільки на цьому ґрунті можна вирішувати проблеми створення наукомістких технологій, технологічного переозброєння промисловості, збільшення досягнень вітчизняної науки і техніки. Наша країна може й повинна посісти гідне місце серед світових лідерів мікроелектронної та комп'ютерної галузі.

Зміст *четвертої складової* національних інтересів України в інформаційній сфері передбачає правовий захист інформаційних ресурсів від розвідувально-підривної діяльності спеціальних лужб іноземних держав, а таож від несанкціонованого доступу до секретної інформації. Крім того, важливим аспектом у сучасних умовах є забезпечення безпеки національних інформаційних і телекомунікаційних систем.

Змістовне наповнення національних інтересів в інформаційній сфері визначається передовсім наявністю загроз, а зміст загроз національним інтересам в інформаційній сфері - чинниками негативного впливу на об’єкти безпеки.

До об’єктів національних інтересів в інформаційній сфері належать:

1) інформація;

2) інформаційна інфраструктура;

3) правовий статус суб’єкта в інформаційній сфері.

Можна стверджувати, що національні інтереси в інформаційній сфері є природною потребою людини, суспільства та держави такого стану, який забезпечує їх стабільне функціонування та існування, а також забезпечує сталий розвиток.

Досить слушною вбачається думка американського дослідника Ч.Ларче, котрий доводить, що за своєю спрямованістю національні інтереси зорієнтовані на забезпечення виживання та прогресивний розвиток і певною мірою лідерства особи, суспільства, держави. Тільки крізь призму їх реалізації та захисту можуть і повинні розглядатися проблеми створення системи національної безпеки, її головна мета, цілі, завдання, принципи функціонування, усі внутрішні параметри [87].

Ряд теоретиків пропонують інтереси держави розташовувати у певній ієрархічній послідовності, визначаючи найбільш пріоритетні. Зокрема, американські дослідники Р.Яргер та Г.Барбер обґрунтовують думку, що пріоритети національних інтересів держави можна класифікувати за чотирма категоріями та трьома рівнями важливості [86].

1. Захист батьківщини.
2. Економічне процвітання.
3. Гармонійний розвиток суспільства.
4. Створення сприятливих умов для ефективної участі країни у світовому розподілі праці.

Категорії використовуються для забезпечення систематизації інтересів. Важливість інтересів - це засіб визначення їх пріоритетності.

- *Життєво важливі* - у разі їх недотримання негайно виникає загроза найвагомішим національним інтересам.
- *Важливі* - у разі їх недотримання буде завдано такої шкоди, яка істотно зачіпатиме найважливіші національні інтереси.
- *Периферійні* - їх недотримання спричинить значні матеріальні та інші втрати, але вони не зачіпатимуть найвагоміших національних інтересів.

Існує також думка, що стратегія національної безпеки потребує ієрархії пріоритетів національних інтересів держави. Без її чіткого визначення може виникнути невідповідність між задекларованими цілями та засобами їх реалізації [88, с. 77].

Уважаємо формування, а тим паче законодавче закріплення такої ієрархії досить умовними, адже визначення тих чи інших пріоритетних національних інтересів в інформаційній сфері має часові обмеження, оскільки залежить від оперативної обстановки, є завданням вибору прийнятних для кожного окремого випадку засобів їх досягнення та вироблення тактичних завдань. Тому формування національних інтересів в інформаційній сфері має носити системний характер. Вони, як слушно зазначає С.Андрущенко, є найважливішими завданнями внутрішньої та зовнішньої політики [89, с .54].

Єдину ієрархію пріоритетів, яка може слугувати орієнтиром, пропонують американські дослідники Ч.Лерч і А.Саїд, котрі вважають, що ціннісне наповнення будь-яких національних інтересів має ґрунтуватися на п'яти видах «добра»:

1) окремих громадян;

2) суспільства у цілому;

3) держави;

4) соціально зацікавлених груп у державі;

5) уряду та його членів [90, с. 11].

Відомий учений у галузях філософії та національної безпеки Б.Пархонський ще на початку 1990-х років констатував, що стратегічні інтереси визначаються згідно з обраним курсом життя та розвитку нації на довготривалий період, однак вони можуть трансформуватись у контексті нових історичних умов. Ситуація в XXI ст. змінюється досить радикально – економічний і технологічний прогрес дедалі більше визначатиметься духовно-інтелектуальним розвитком. Цей вельми вагомий чинник може кардинально вплинути на геополітичну ситуацію. Вчений також

прогнозував, що в майбутньому важелі головних економічних, політичних, технологічних інтересів перебуватимуть у руках не володарів фінансової потуги та природних ресурсів, а насамперед носіїв найрозвинутіших форм духу та інтелекту [91, с. 6].

Таким чином, реалізація визначених в Доктрині інформаційної безпеки України національних інтересів в інформаційній сфері буде ефективною і дієвою за умови законодавчого визначення **національних цінностей**, які зумовлюють потребу в розробці національних (державних) інтересів. Разом вони формують *національні цілі* (схематично це зображено на рис. 2.1.).

Отже, першочергового законодавчого визначення потребують саме національні цінності в інформаційній сфері. Дана тріада має стати чітким орієнтиром формування та розвитку державної політики.

Ми цілком підтримуємо думку Є.Мануйлова, що у стратегічному сенсі державі варто зміцнювати аксіосферу суспільства шляхом відтворення цінностей через освіту та виховання, дбати про інформаційну безпеку та захищеність культурно-інформаційного простору країни від зовнішніх впливів. Інформаційна стабільність та втілення чітких ціннісних пріоритетів демократичного розвитку держави забезпечуватиме їй конкурентоспроможність у глобальних процесах сучасності [92, с. 16].

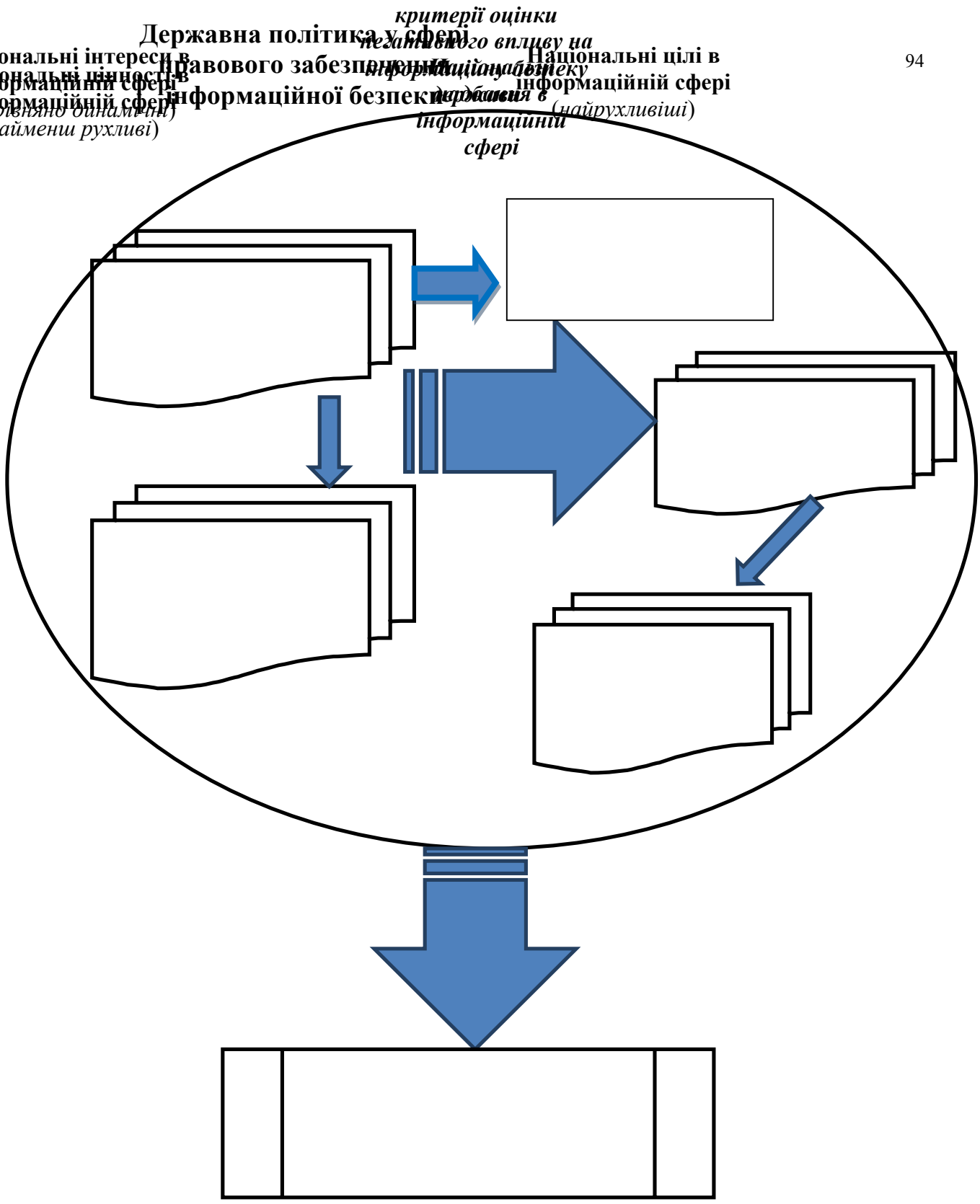

Рис. 2.1. Взаємодія національних цінностей, інтересів цілей та надбань в інформаційній сфері

Джерело: розроблено автором.

Б.Гогвуд та Л.Ган національні цінності розглядають як переконання,

мораль, стандарти та більш специфічні норми, котрі впливають на процес вироблення політики на всіх рівнях (індивідуальному, груповому, організаційному та суспільному) через спрямування та стримування поведінки та дій учасників процесу творення політики, впливаючи на їхнє сприйняття бажаного кінцевого стану (кінцевих цінностей) та прийнятних засобів (інструментальних цінностей) для його досягнення [93, с. 160].

До цього твердження слід додати важливу засторогу відомого соціолога М.Вебера стосовно того, що кожна історична епоха має свою систему цінностей, тобто це категорія принципово історична [94, с. 64]. Варто погодитися з думкою С.Ларіна, що національні цінності є певними концептуальними, ідеологічними основами, консолідуючими чинниками, важливими життєвими орієнтирами на шляху ефективного суспільного розвитку [9, с. 47].

Вельми ґрунтовно цю проблему досліджували вітчизняні фахівці В.Горбулін та А.Качинський. Вони структурували систему національних цінностей, поділяючи їх на цінності індивіда, цінності суспільства та цінності держави [71, с. 107]. З погляду дослідників, подальше існування держави й нації має розглядатися крізь призму її ціннісного ядра, що консолідує суспільство, а саме: національна безпека, духовні надбання, добробут, система міжнародних зв’язків, патріотизм і соціальна справедливість. На нашу думку, до наведеної вище системи національних цінностей варто також долучити такі індивідуальні цінності, як: моральність; релігійність; толерантність; миролюбність; доброзичливість; працелюбство; сім’я (сімейні цінності) тощо, які завжди були притаманними українцям і відображають сутнісні засади українського національного характеру. В.Горбулін особливо наголошував на важливості національних цінностей, зазначаючи, що стратегія національної безпеки України формується на основі оцінок національних цінностей у контексті міжнародної обстановки [96, с. 4]. Таке застереження особливо актуалізувалося з початком збройної агресії Росії проти нашої країни.

Національні цінності в інформаційній сфері - це сукупність духовних та матеріальних цінностей людини, суспільства і держави, яким властиві чітко окреслені світоглядні, соціокультурні, соціально-економічні, географічні та демографічні ознаки. Вони формують правову, філософську та етичну основу для забезпечення подальшого існування суспільства і держави, дають змогу усвідомити національну мету держави в інформаційній сфері. Національні цінності в інформаційній сфері, виходячи із сутнісного їх тлумачення, являють собою найбільш специфічний сегмент, той, що потребує особливого захисту. До *національних цінностей в інформаційній сфері,* з огляду на сучасний стан державотворення в Україні, слід віднести:

1. **Матеріальний добробут** населення, зокрема й на основі розвитку ІКТ.
2. **Інформаційна захищеність** людини, суспільства, держави.
3. **Духовність**. Доступність віросповідання, запобігання релігійному фанатизму та екстремізму, неприпустимість використання релігії як психологічного чинника тероризму, розвиток традиційних українських релігійних напрямів.
4. **Мова** як основний ідентифікатор нації, як засіб передачі інформації та знань, як пам'ять поколінь.
5. **Культура** інформаційних відносин.
6. **Свобода інформації.** Захищеність інформаційних прав людини, доступ до інформації, нейтралізація негативних інформаційних впливів.

Первинним у структурі національних цінностей в інформаційній сфері має стати соціально-економічна складова інформаційної безпеки. Відтак, на наше глибоке переконання, добробут населення як базова категорія економічної політики держави має стати субстанціональним компонентом й інформаційної безпеки держави, а особливо - національної безпеки України.

На думку Г.Ситника, об’єктивне існування і вплив на безпеку особи, суспільства, держави та людської цивілізації природних і суспільних явищ зумовлюють можливість розподілу цінностей на природні й соціальні [97, с. 123], що загалом й відображено у запропонованому вище переліку національних цінностей в інформаційній сфері.

Згадуваний раніше Б.Парахонський свого часу зазначав, що у сучасному світі захист національних інтересів уже не може спиратися лишень на стратегію силового протистояння. Ефективнішою стає реалізація власних національних інтересів за допомогою економічної, духовно-інтелектуальної експансії [98, с. 3]. Ця теза підтвердилася вітчизняною історією останнього десятиріччя зі своєю кульмінацією у 2014 році.

Ще у 2008 році А. Марущак піднімав питання доцільності розробки та законодавчого закріплення критеріїв негативного впливу на інформаційну безпеку [99]. Проте, такі критерії до сьогодні не визначені ні в рамках наукового дискурсу, ні законодавчо. Вважаємо, що дане питання актуалізувалося сьогодні, першочергово зв’язку із вразливістю національної безпеки. При цьому вважаємо за доцільне уточнити дане поняття, додавши до нього оціночний підхід. Таким чином ми будемо говорити про *критерії оцінки негативного впливу на інформаційну безпеку держави*. У даному контексті досить слушним є твердження міністра оборони США (2015–2017) Ештона Картера: «Говорити про питання безпеки – це найкраща річ, яку можна зробити, бо безпека, вона як повітря. Якщо вона є – ви не думаєте про це, але як тільки ви її позбавляєтесь, то це єдине, про що ви можете думати» [100].

На рівні міжнародного права розроблені критерії інформаційної безпеки, які можуть слугувати відповідними орієнтирами для розробки критеріїв оцінки негативного впливу на інформаційну безпеку. Так звана «Помаранчева книга» Міністерства оборони США (Критерії оцінки надійності комп'ютерних систем –Trusted Computer System Evaluation

Criteria, TCSEC) початково таким критерієм визначила надійність, тобто певний ступінь довіри до інформаційної системи [101]. У 1986 р. країни Європи спільно розробили загальні «Європейські критерії безпеки інформаційних технологій» [102], якими, зокрема, визначені завдання засобів інформаційної безпеки. Для визначення ефективності та надійності засобів захисту в єврокритеріях було вперше введено поняття «**адекватності засобів захисту**» [103].

З зазначеного можемо припустити, що критерієм ефективності забезпечення інформаційної безпеки має бути високий рівень безпеки при мінімумі відповідних затрат.

Дещо пізніше були розроблені «Єдині критерії безпеки інформаційних технологій» (англ.: Common Criteria for Information Technology Security Evaluation), які проголошені невід'ємним компонентом інформаційних технологій [104], відповідно до яких були визначені загальновідомі сьогодні такі основні характеристики інформаційної безпеки як конфіденційність, цілісність та доступність – так звана тріада CIA [2].

Виходячи із розробленої нами схеми взаємодії національних цінностей, інтересів цілей та надбань в інформаційній сфері, вважаємо, що основними критеріями оцінки негативного впливу на інформаційну безпеку держави є національні цінності. Адже їх порушення, недотримання, спотворення тощо призводять до суттєвого негативного впливу на інформаційну безпеку людини, суспільства, держави, нації. Таким чином, *критерії оцінки негативного впливу на інформаційну безпеку держави – це методологічна база, у рамках якої визначається такий стан розвитку національних цінностей в інформаційній сфері, за якого дія зовнішніх та внутрішніх факторів на них не призводить до утруднення чи унеможливлення її функціонування та розвитку.* На основі такої методологічної бази можливим є визначення найбільш вразливих сфер

[2] конфіденційність (англ. ***C****onfidentiality, privacy*), цілісність (англ. ***I****ntegrity*), доступність (англ. ***A****vailability*)

інформаційної безпеки держави, відповідна акумуляція сил і засобів їх нейтралізації, а також розробка напрямів їх розвитку та вдосконалення.

До *національних цілей в інформаційній сфері* відносимо:

1. *Покінчити* з порушенням та спотворенням поглядів людей на навколишній світ і самих себе, здійснюваних шляхом культивування уявних цінностей, насадження деструктивних пріоритетів, завдань і цілей перед суспільством і окремою особистістю (духовна безпека).

2. *Забезпечити* впровадження інформаційних технологій у військову сферу та їх захист (військова безпека).

3. *Прискорити* розробку та впровадження новітніх конкурентоспроможних ІКТ у суспільно-економічну сферу (економічна безпека).

4. *Досягти* належного рівня культури інформаційних відносин (соціальна безпека).

5. *Створити* загальнодержавні інформаційні системи для постійного моніторингу стану навколишнього середовища (екологічна безпека).

6. *Сприяти* інтеграції національної інформаційної інфраструктури зі світовою інфраструктурою.

7. *Посилити* захист інформаційних прав людини;

8. *Вжити термінових заходів* для створення позитивного іміджу держави в умовах інформаційної глобалізації.

Категорія «національні надбання» більш характерна для сфери культури й мистецтва. Проте, з огляду на потужний розвиток інформаційних технологій, їх визначальний вплив як на військову сферу, так і на інші суспільні відносини, насамперед у медицину, економіку, низку добутків інформаційної сфери по праву можна віднести до національних надбань в інформаційній сфері. При цьому вони відграватимуть тут роль певного індикатора та критерію ефективності реалізації національних цілей в означеній сфері.

Автори законопроекту «Про інформаційну безпеку України» [105] так визначили національні надбання в інформаційній сфері: найбільш вагома, вартісна частина інформаційних ресурсів, особливо кінцеві результати інтелектуальної, творчої діяльності, кращі зразки вітчизняного (національного) інформаційного продукту без позбавлення права власності на них можуть оголошуватися національним надбанням України і незалежно від форм власності охоронятися державою як пам'ятки історії та культури. Не зовсім зрозуміло, чому законотворці обмежилися лишень пам’ятками історії та культури, адже ці надбання мають набагато ширший ціннісний спектр.

На нашу думку, *національні надбання в інформаційній сфері* – це сукупність унікальних інформаційних продуктів, що мають виняткове військове, суспільне, економічне та інше значення для реалізації національних цілей в інформаційній сфері.

Створити вичерпний перелік національних надбань в інформаційній сфері неможливо, адже з кожним днем такий список може поповнюватися відповідними розробками чи, навпаки, зазнавати вилучень у зв’язку із застарілістю чи втратою цінності. Визначальним критерієм віднесення до такого переліку є особливе, стратегічне значення інформаційного продукту як для забезпечення інформаційної безпеки держави безпосередньо, так і для розвитку інших сфер, а також унікальність за своєю природою.

Наприклад, *до національних надбань в інформаційній сфері, які мають особливе значення для розвитку військової її складової,* сьогодні є всі підстави віднести:

- створений ДП Спецтехноекспорт 29 серпня 2016 року дистанційно керований тактичний багатоцільовий транспортний засіб «Фантом»[3];

[3] «Фантом» – це мінібронетранспортер-безпілотник. Він оснащений денним та нічним комплексами прицілювання, що дозволяє вести вогонь у будь-який час доби на відстані понад 1 км. Запас ходу наземного безпілотника становить до 20 км, а управління здійснюється захищеним радіоканалом або через волоконний кабель завдовжки 5 км.

- реактивну систему залпового вогню «Верба»[4];
- радіолокаційну станцію для виявлення літаків-невидимок МР-18, розроблену запорізьким Науково-виробничим комплексом «Іскра»[5];
- радіолокаційну станцію «Пелікан»[6];
- шолом доповненої реальності для танкістів[7];
- безпілотник «Горлиця»[8].

До національних надбань в інформаційній сфері, які мають особливе значення для розвитку соціальної її складової та медицини, можемо

«Фантом» розрахований на транспортування боєкомплекту, евакуацію поранених з поля бою і виконання бойових завдань (https://nv.ua/ukr/ukraine/events/top-13-novih-ukrajinskih-vijskovih-rozrobok-vid-sholoma-dopovnenoji-realnosti-do-mini-avtomata-1086249.html).

[4] Ця зброя – нове покоління відомих «Градів». Керування вогнем, прицілювання та навіть перезаряджання «Верби» здійснюється в автоматичному режимі з кабіни, без безпосереднього втручання бійців у її роботу (https://www.ukrinform.ua/rubric-technology/2297366-ukroboronprom-pokazav-novu-ukrainsku-zbrou.html).

[5] Дана станція здатна виявляти навіть стелс-техніку (літаки-невидимки).

[6] Науково-виробничий комплекс «Іскра» розробив також рухому трикоординатну радіолокаційну станцію кругового огляду 80К6К1 «Пелікан», котра виконує два основних завдання: протиповітряна оборона – визначення ворожих повітряних цілей та передача їхніх координат вітчизняним винищувачам для негайної реакції та знищення супротивника; у складі зенітно-ракетних комплексів – визначення координат техніки ворога, а також позицій, з яких ведуться ворожі обстріли (https://iskra.zp.ua/index.php?lang=ua).

[7] 26 жовтня 2016 року стало відомо, що український проект LimpidArmor працює над пристроєм доповненої реальності, призначеним для військових, у першу чергу – екіпажів бронетанкової техніки. Стартап LimpidArmor, що спочатку розробляв такий пристрій для картингу, на зустрічі учасників АТО у Дніпрі поспілкувався з танкістами, які обговорювали недоліки систем огляду вітчизняної військової техніки. Дещо пізніше учасникам проекту потрапив до рук шолом Microsoft HoloLens, і вони вирішили зайнятися розробкою девайса для війська, який вирішив би проблему з недоліками систем огляду (http://milnavigator.com.ua/%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%81%D1%8C%D0%BA%D0%B0-%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D1%96%D1%8F-%D0%BF%D1%80%D0%BE%D0%BF%D0%BE%D0%BD%D1%83%D1%94-%D0%B2%D0%BE%D0%B4%D1%96%D1%8F%D0%BC/).

[8] Держпідприємство «Антонов» у кооперації з провідними підприємствами України активно розробляють безпілотний літальний комплекс під назвою «Горлиця». Окрім багатофункціональної розвідувальної апаратури, «Горлиця» має можливості оснащення високоточними засобами ураження. Причому практична відстань польоту ударного безпілотника становитиме понад тисячу кілометрів. Такі характеристики дозволяють використовувати «Горлицю» як надсучасний засіб, за допомогою якого можна вести спостереження за противником або цілими потенційно небезпечними напрямами, а в разі потреби – вражати цілі високоточною зброєю (http://uprom.info/news/vpk/dp-antonov-prodemonstruvalo-proekti-troh-ukrayinskih-bpla/).

віднести:

- TechnoEyes – рукавичка для людей з вадами зору[9];
- комп'ютерний фонендоскоп[10].

До національних надбань в інформаційній сфері, які мають особливе значення для розвитку економіки, можемо віднести:

- розвиток ІТ-сфери.

Стосовно останнього слід особливо підкреслити, що українська ІТ індустрія стала однією із трьох галузей вітчизняної економіки з найбільшим внеском у ВВП країни. Загальний дохід ІТ галузі за 2017 рік становив 3,6 мільярда доларів США, поступаючись за обсягом тільки доходу українських сільського господарства та металургії. У теперішній час продукти та послуги ІТ сектору формують 3% ВВП України [106].

Це – лиш незначна частка того, що можна вважати національним надбанням в інформаційній сфері. Подальші здобутки та їх позитивний вплив як на забезпечення інформаційної безпеки держави, так і на інші дотичні сфери значною мірою залежатиме від продуманої державної політики у цій сфері та ефективних правових механізмів її реалізації.

Вартує підтримки позиція відомого українського дослідника державного управління національною безпекою Г.Ситника, котрий дійшов висновку, що національні цінності визначають сутність (зміст), цілісність і стійкість, національні інтереси – структуру і характер, а національні цілі – конфігурацію та спрямованість формування й функціонування даної

---

[9] Це – інфрачервоний датчик відстані, який допомагає людям з проблемами зору ліпше орієнтуватися на вулицях міста. У 2013 році цей прилад, створений молодим українцем, потрапив до трійки кращих винаходів світу.

[10] У 2006 році група вчених-акустиків з Національної академії наук України створила комп'ютерний фонендоскоп. Унікальний комплекс для реєстрації та обробки звуків дихання дозволяє не лише за лічені хвилини встановити точний діагноз, а й контролювати клінічний перебіг захворювань дихальних органів. В основі дії комплексу – багатоканальна реєстрація звуків за допомогою чотирьох сенсорів з подальшим аналізом отриманої інформації. Відзначається, що традиційна система обробки звуків дихальної системи, усталена в медичній практиці, дає при діагностиці до 20 відсотків помилок, а український винахід дозволяє взагалі відмовитися від традиційного "прослуховування" (http://www.nas.gov.ua/UA/Messages/news/Pages/View.aspx?MessageID=2794).

системи [97, с. 46]. Це стосується в цілому й інформаційної безпеки держави.

Вітчизняна юриспруденція зазначає, що предметом правового регулювання є такі суспільні відносини, упорядкування яких можливе і водночас доречне саме за допомогою юридичних засобів і способів, адже право є універсальним соціальним регулятором, проте не єдиним і не всеохоплюючим. Предметом регулювання інформаційного права може бути: суспільні відносини, які виникають у зв'язку з пошуком, створенням, зберіганням, обробкою, відчуженням, аналізом, синтезом, реалізацією тощо інформації, тобто, суспільні відносини, пов'язані із обігом інформації [107, с. 23-24] .

Предмет правового забезпечення інформаційної безпеки - сфера правового впливу на поведінку людей, що має на меті недопущення прояву загроз об'єктам інформаційної безпеки або мінімізацію негативних наслідків прояву цих загроз. Цю сферу утворюють сукупно суспільні відносини, що мають такі основні ознаки:

- належність до інформаційних відносин або зумовленість ними;
- зв'язаність з об'єктами національних інтересів в інформаційній сфері;
- зумовленість проявів загроз безпеці об'єктам національних інтересів в інформаційній сфері.

Предметна спрямованість діяльності щодо забезпечення інформаційної безпеки визначається сукупністю суспільних відносин, пов'язаних з інформацією та інформаційною інфраструктурою в різних сферах життєдіяльності суспільства й державного управління, реалізацією правового статусу суб'єктів інформаційної сфери, проявами загроз, здатних зашкодити національним інтересам.

Можна виділити два основних типи цілей протидії:

1) ліквідація загроз безпеці;

2) мінімізація шкоди від прояву загроз.

Мета забезпечення інформаційної безпеки держави - досягнення стану захищеності суспільних відносин від прояву зовнішніх і внутрішніх загроз, пов'язаних з інформацією та інформаційною інфраструктурою у процесі захисту національний цінностей, реалізації національних інтересів, досягненні національних цілей.

Доцільним убачається виділити такі основні групи інформаційних відносин (див. *табл. 2.1.*):

Таблиця 2.1.

Групи інформаційних відносин

Група відносин	**Форма представлення інформації**	**Функція інформації**
Товарно-грошові відносини	Повідомлення	Товар, послуга або об'єкт прав інтелектуальної власності
Духовні відносини	Відомості	Засіб впливу на психічний стан суб'єктів
Відносини у сфері соціального та державного управління	Відомості та повідомлення	Засіб ідентифікації суб'єктів, регулювання їх діяльності
Відносини в галузі управління технічними й технологічними системами	Повідомлення	Засіб забезпечення узгодженого функціонування окремих складових систем
Відносини, пов'язані з повсякденним міжособистісним спілкуванням	Відомості	Засіб самовдосконалення суб'єктів, їхнього інформаційного збагачення

Перелічені інформаційні відносини породжуються інтересами суб'єктів, реалізованими в інформаційній сфері.

На нашу думку, варто виокремити такі три основні групи вказаних інтересів:

1) вільно володіти інформацією;

2) передавати окремі масиви інформації певним суб'єктам;

3) приховувати окремі масиви інформації від інших суб'єктів.

Реалізуючи ті чи інші інтереси в інформаційній сфері, суб'єкт взаємодіє з іншими суб'єктами, певним чином оформлюючи ці відносини, тобто, дотримуючись визначеного порядку їх здійснення. Цей правопорядок залежить від рівня розвитку інформаційної інфраструктури, а також засобів, якими може оперувати суб'єкт для реалізації його інтересів. У цивільно-правових відносинах відповідна взаємодія зазвичай набуває форми угоди, об'єктом якої є послуга, а в публічних відносинах - вимоги або звернення. Розглянемо детальніше можливі форми такої взаємодії.

Взаємодія, пов'язана з пошуком інформації. Така взаємодія може відбуватися або у формі угоди, змістом якої є надання посередницької послуги в пошуку повідомлень, що мають необхідні ознаки (оформлення, зміст матеріальної чи духовної сфери життя суспільства, рівень теоретичного узагальнення відомостей, мова, якою представлені дані, тощо), або шляхом надання можливості суб'єкту взаємодії самостійно добирати необхідні йому повідомлення. Соціальним результатом такої взаємодії може бути як визначення місця зберігання повідомлень, котрі відповідають пошуковим ознакам конкретного суб'єкта, який володіє цими повідомленнями, отримання дозволу на доступ до цих повідомлень, так і відмова суб'єктові в наданні такого доступу або неможливість встановити місце зберігання шуканих повідомлень.

Взаємодія, що має на меті отримання повідомлень, здійснюється у формі угоди, зміст якої - надавання послуг з передавання необхідних повідомлень, а *взаємодія, що має на меті зберігання повідомлень* - це послуги щодо забезпечення збереження наявних повідомлень. Соціальним результатом цих взаємодій буде отримання необхідних повідомлень, збереження фізичних властивостей матеріального носія, на якому вони закріплені, й, відповідно, можливість ознайомлюватися зі змістом

повідомлень.

Взаємодія, що має на меті використання повідомлень для отримання відомостей, здійснюється у формі угоди, зміст якої - надавання можливості ознайомлюватися з важливими для суб'єкта повідомленнями. Соціальний результат цієї взаємодії полягає в перетворенні повідомлення у відомості, які відображаються в «інформаційній моделі» суб'єкта.

Взаємодія, що має на меті передавання (поширення) відомостей, здійснюється у формі угоди, зміст якої - надавання послуги із закріплення повідомлення, що містить трансльовані відомості, на матеріальному носії, а також передавання (доведення) повідомлення до певних суб'єктів або невизначено великої кількості суб'єктів у певний спосіб (розсилка поштою, агітація і пропаганда, розміщення на рекламних щитах, поширення повідомлень у радіо- і телепрограмах, в інших ЗМІ, розміщення на веб-сайтах тощо). Соціальний результат цієї взаємодії - доставляння повідомлення адресатам або ознайомлення адресатів із повідомленням, що за певних обставин може зумовити зміну їхньої поведінки.

Взаємодія, що має на меті оброблення інформації. Іноді фахівці виокремлюють ще один вид інформаційних відносин, - що виникають у процесі взаємодії, котра має на меті оброблення інформації. Під обробленням інформації зазвичай розуміють перетворення певної сукупності повідомлень у нове повідомлення (безліч повідомлень), яке здійснює суб'єкт безпосередньо чи за допомогою технічних засобів, послуговуючись заздалегідь заданими алгоритмами або без них. Така взаємодія може здійснюватися у формі угоди, що полягає в наданні інформаційної (наукової, творчої) послуги, а її соціальний результат - нове повідомлення чи відомість. Взаємодію, що має на меті оброблення інформації, можна розглядати як різновид взаємодії, що має меті володіння відомостями, за якої частина операцій із підготовки повідомлень до сприйняття суб'єктами здійснюється за допомогою обчислювальної

техніки.

У публічних правовідносинах взаємодія відбувається для задоволення інтересів особи й суспільства, пов’язаних з інформацією, якою володіє держава, а також інтересів держави, що стосуються інформації, котрою володіють особи та організації, органи місцевого самоврядування, які становлять основу громадянського суспільства.

Інтереси особистості й суспільства, пов’язані з наявною у держави інформацією, спрямовані на володіння відомостями, необхідними для контролю за діяльністю держави, здійснення правомірної поведінки, оцінювання обстановки у найважливіших сферах суспільного життя. Ці інтереси також спрямовані на передавання державі, зокрема її органам, інформації, необхідної для виконання покладених на них функцій.

Взаємодія особистості та організацій з державними органами, *що має на меті володіння необхідною інформацією або передавання інформації,* здійснюється здебільшого у формі звернень. Взаємодія державних органів з особою та організаціями, що має на меті оволодіння наявною в них інформацією, може відбуватися у формі вимоги, коли надання відомостей передбачено правовими нормами, або у формі повідомлення, коли норми права приписують оприлюднення державними органами відповідної інформації. У передбачених законом випадках ця взаємодія може набувати також форми відмови в наданні інформації.

Взаємодія, що має на меті отримання послуг зв’язку. Інтереси суб’єктів, пов’язані з використанням інформаційної інфраструктури, реалізуються за допомогою встановлення взаємодії з іншими суб’єктами, що має на меті отримання послуг зв’язку, змоги використання повідомлень, накопичених в інформаційних системах, а також використання можливостей автоматизованих систем управління та обробки даних, комп'ютерних систем для здійснення обробки інформації. Соціальним результатом цих взаємодій є підвищення якості провадження основної інформаційної діяльності.

Забезпечення реалізації розглянутих взаємодій становить основу змісту поняття «*інформаційні правовідносини*».

Інформаційні правовідносини - це регульовані правом суспільні відносини, що виникають у процесі взаємодії суб'єктів, що має на меті задоволення їхніх інтересів у володінні необхідною інформацією, в передаванні частини наявної інформації іншим суб'єктам, а також у збереженні інформації.

Аналогічні взаємодії, які здійснюються з метою реалізації інтересів, пов'язаних із володінням речами, регулюються з використанням детально розроблених правових засобів цивільного права. Однак можливості застосовувати їх для регулювання відносин, об'єктом яких є інформація, досить обмежені, оскільки, існуючи у формі повідомлень матеріального характеру, інформація позбавлена властивостей речі: її не можна зберегти без закріплення на матеріальному носії; вона не має ознак одиничності, адже копіюється в необмежених кількостях, не амортизується в процесі використання тощо. Через ці причини регулювання інформаційних відносин здійснюється в межах окремої галузі права, яка отримала назву «інформаційне право».

Умовою реалізації інтересів суб'єктів суспільних відносин, об'єктом яких є інформація, є стійке й безпечне функціонування інформаційної інфраструктури суспільства. Склад цієї інфраструктури і зміст суспільних відносин, що виникають у зв'язку з її використанням, зумовлюються рівнем розвитку суспільства, його економічними можливостями, здатністю до впровадження результатів науково-технічного прогресу.

У складі сучасної інформаційної інфраструктури виділяють такі складові частини:

- *організаційно-керуюча*: органи і служби, що забезпечують стале функціонування технологічних та інформаційних елементів інфраструктури; засоби масової інформації; організації, які надають інформаційні послуги;

- *технологічна*: мережі та об’єкти зв’язку, телекомунікації; засоби автоматизації управління соціальними й технологічними процесами, автоматизації обробки даних, комп’ютерні мережі та системи;
- *інформаційна*: інформаційні системи, в т. ч. у вигляді бібліотечних, архівних і музейних фондів.

Необхідність нормативного закріплення форми розглянутих відносин зумовлюється, з одного боку, значною соціальною важливістю відповідних взаємодій, а з другого - складністю однозначного встановлення факту досягнення необхідного соціального результату без допомоги держави. До прикладу, досить важко встановити повноту і ретельність проведеного пошуку необхідної інформації, здатність наданої інформації реалізувати інтереси суб’єкта, обізнаність суб’єкта про ті чи ті повідомлення, існування причинно-наслідкового зв’язку між обізнаністю з конкретними повідомленнями та зміною поведінки суб’єкта тощо.

Розглянуті характеристики основних типів взаємодій є першою ознакою суспільних відносин, що становлять предмет правового забезпечення інформаційної безпеки.

Другою ознакою є зв’язаність та взаємозалежність інформаційних правовідносин з категоріями, які складають об’єкт інформаційної безпеки: національні цінності, національні інтереси, національні цілі в інформаційній сфері. З огляду на це визначені три групи об’єктів в інформаційній сфері в тій чи тій формі мають бути закріплені в законодавчих актах.

Наступною ознакою суспільних відносин, що становлять предмет правового забезпечення інформаційної безпеки, є *наявність загроз безпеці національним цінностям, національним інтересам, національним цілям в інформаційній сфері*. Загроза безпеці цих об’єктів полягає в можливості завдавання їм шкоди внаслідок діяльності суб’єктів в інформаційній сфері. Забезпечення безпеки об’єктів національних інтересів є умовою та гарантією існування й сталого розвитку нації в конкретних історичних

умовах. Важлива особливість цих відносин криється ще й у їхній імовірнісної природі: їх може й не існувати як суспільної практики або вони можуть проявлятися як поодинокі явища; набуття ними масового характеру може суттєво зашкодити національним інтересам в інформаційній сфері. Відтак, зміст третьої ознаки відносин, що становлять предмет правового забезпечення інформаційної безпеки, полягає в зумовленості їх виникнення можливим впливом чинників, що становлять загрозу безпеці об'єктів національних інтересів в інформаційній сфері.

Таким чином, предмет правового забезпечення інформаційної безпеки утворюється сукупністю суспільних відносин, пов'язаних з інформацією, інформаційною інфраструктурою і правовим статусом суб'єктів інформаційної сфери, що належать до об'єктів національних інтересів, а також із проявом загроз безпеки цих об'єктів.

Правове забезпечення інформаційної безпеки є самостійним комплексним напрямом правового регулювання відносин у сфері прояву загроз об'єктам національних інтересів в інформаційній сфері та протидії їм на основі норм та інститутів конституційного, цивільного, адміністративного, кримінального та інформаційного права.

1.4. Методологічні засади правового забезпечення інформаційної безпеки України

Діяльність із забезпечення інформаційної безпеки держави здійснюється на основі сукупності найважливіших *принципів* - вихідних положень, покладених в основу здійснення безпекових заходів. Такі принципи становлять базові константи методологічних засад дослідження та слугують відповідними теоретичними орієнтирами механізму правового забезпечення інформаційної безпеки держави.

Принципи діяльності із забезпечення інформаційної безпеки можуть

бути розрізнені як загальні та особливі.

Загальні принципи діяльності із забезпечення інформаційної безпеки – це засади, на яких ґрунтується діяльність із забезпечення усіх видів безпеки. До них належать: гуманізм, соціальна справедливість, об'єктивність, конкретність, ефективність, підтримка й довіра народу, поєднання гласності й таємниці, законність і конституційність.

Особливі принципи забезпечення інформаційної безпеки - засади, які визначають спрямованість державної політики щодо механізмів забезпечення інформаційної безпеки. До таких передовсім слід віднести глобальність.

Принцип глобальності полягає в тому, що вказана діяльність має здійснюватися узгоджено, як усередині держави, так і в міжнародному співтоваристві. В умовах формування глобального інформаційного суспільства забезпечити повну інформаційну безпеку не спроможна жодна окремо взята країна світу. Це спричинено тим, що глобальна інформаційна інфраструктура вивела забезпечення прав людини на свободу думки і слова, віросповідання, поширення інших поглядів, пошук, отримання, передачу, виробництво й поширення інформації (в т. ч. масової) далеко за межі юрисдикції однієї держави, зумовила потребу їх міжнародного захисту. У цих умовах глобалізуються також зловживання свободою з боку індивідів, організацій і держав, тож протидія таким всеохоплюючим зловживанням природно передбачає об'єднання зусиль членів міжнародного співтовариства. Крім того, без роз'яснення міжнародній спільноті причин стурбованості держави з приводу тих чи тих загроз зовнішнього або внутрішнього характеру неможливо забезпечити адекватну дієвість реакції міжнародного співтовариства для сфери національних інтересів.

Діяльність із забезпечення інформаційної безпеки проводиться за допомогою різних методів, способів, засобів і прийомів. Їх вибір та специфіка застосовування залежать головно від об'єкта впливу та

сформульованих завдань.

Усі об’єкти інформаційного впливу можна згрупувати у три основні види:

1) суб’єкти суспільного життя;

2) інформація;

3) інформаційна інфраструктура.

Самі методи впливу на суб’єктів суспільного життя досить часто класифікують за функціями суб’єктів діяльності. При цьому виділяють загальні та спеціальні методи впливу на суб’єктів суспільного життя.

Загальні методи впливу на суб’єктів суспільного життя використовуються при виконанні всіх або основних етапів цієї діяльності. Як загальні методи впливу на суб’єктів застосовуються переконання і примус.

Спеціальні методи впливу на суб’єктів суспільного життя застосовуються при здійсненні окремих функцій або на окремих стадіях протидії загрозам.

Вибір методів діяльності щодо захисту інформаційної безпеки зумовлюється передовсім змістом національних інтересів, які підлягають захисту, і загроз цим інтересам. Скажімо, протидія загрозам конституційним правам і свободам людини та громадянина у сфері духовного життя та інформаційної діяльності здійснюється з переважним використанням методів примусу. Умови для протидії утискам конституційних прав громадян на особисту та сімейну таємницю, таємницю листування, телефонних переговорів та інших повідомлень створюють норми Кримінального кодексу України, що закріплюють кримінальну відповідальність за порушення цих конституційних прав і свобод. Натомість захист національних інтересів, пов’язаних з інформаційним забезпеченням державної політики, передбачає використання переважно методів переконання.

Важливим складником структури поняття методологічних засад

правового забезпечення інформаційної безпеки держави є *засоби забезпечення*. Категорія засобів є загальнонауковою, міждисциплінарною. Вона об'єднує інструменти, за допомогою яких провадиться діяльність, і технології їх використання. З огляду на це засоби забезпечення інформаційної безпеки - це сукупність правових, політичних та організаційних засобів, що включають засоби технологічного, кадрового, матеріального, фінансового, інформаційного та наукового забезпечення.

Правові засоби забезпечення інформаційної безпеки. Це - правові явища, що виражаються в інструментах (встановлення - суб'єктивні права, обов'язки, пільги, заборони, заохочення, покарання тощо) і діяннях (технології - акти реалізації прав та обов'язків), які протидіють загрозам інтересам суб'єктів права, реалізованим в інформаційній сфері, та забезпечують досягнення соціально корисних цілей. Вони є елементом механізму правового регулювання і значною мірою зумовлюють його ефективність. Отже, правові засоби забезпечення інформаційної безпеки відображають функціональний, прикладний бік правової системи.

Політичні засоби забезпечення інформаційної безпеки утворюються сукупністю інструментів політичної боротьби, в якій беруть участь політичні сили суспільства: страйки, пропагандистські кампанії, критика політичних опонентів, мітинги, демонстрації, вибори, референдуми тощо.

Засоби технологічного забезпечення інформаційної безпеки - це сукупність технічних і програмних засобів захисту інформації, запобігання несанкціонованому доступу до інформаційних, телекомунікаційних та обчислювальних систем і мереж зв'язку, а також методичного забезпечення їх використання.

Засоби кадрового забезпечення інформаційної безпеки - сукупність програм підготовки кадрів для різних напрямів безпекової діяльності, що використовуються у процесі підготовки навчального та методичного матеріалу.

Засоби матеріального забезпечення інформаційної безпеки -

сукупність об’єктів, що виділяються для розміщення засобів технологічного забезпечення, сил, які беруть участь у забезпеченні інформаційної безпеки, засобів організації їхньої діяльності та ін.

Засоби фінансового забезпечення інформаційної безпеки - сукупність економічних інструментів отримання, залучення, перерозподілу й використання коштів для розв’язання завдань забезпечення інформаційної безпеки.

Засоби інформаційного забезпечення інформаційної безпеки - сукупність інформаційних фондів і банків даних, які використовуються у процесі розв’язання завдань забезпечення інформаційної безпеки, а також засобів їх актуалізації.

Засоби наукового забезпечення інформаційної безпеки - сукупність наукових теорій, концепцій, категорій, закономірностей і методів, призначених для вивчення процесів і явищ розвитку інформаційної сфери суспільства, загроз національним інтересам і протидії цим загрозам.

Таким чином, забезпечення інформаційної безпеки України є складним комплексним поняттям, що охоплює велике коло процесів і явищ, пов’язаних із протидією загрозам безпеці національних інтересів в інформаційній сфері.

Особливе змістовне значення у методологічних засадах правового забезпечення інформаційної безпеки держави належить *меті*. Загальна мета права - створити умови для реалізації свободи людини, протидіяти свавіллю й насильству стосовно неї з боку інших людей, громадських організацій, держави.

Головною метою правового забезпечення інформаційної безпеки є протидія загрозам безпеці об’єктів національних інтересів в інформаційній сфері правовими засобами. Ця протидія передбачає ліквідацію загроз безпеці об’єктів національних інтересів в інформаційній сфері та мінімізацію шкоди від їхніх проявів, що досягається за допомогою попередження, припинення й мінімізації наслідків реалізації цих загроз.

Ліквідація загроз як мета функціонування правового механізму забезпечення інформаційної безпеки полягає у створенні таких умов взаємодії особистості, суспільства і держави із джерелами загроз, за яких ця взаємодія зі стадії дисгармонії чи конфлікту переходить у стадію гармонії. Ця мета може досягатися шляхом:

- правового впливу, спрямованого на зміну інтересів суб'єктів, які є джерелами або засобами реалізації загроз;
- ліквідація наявних засобів здійснення загроз;
- забезпечення невідворотного обмеження інтересів суб'єктів загроз у разі виявлення ознак підготовки до їх реалізації.

Зрозуміло, не завжди є можливість ліквідувати численні загрози безпеці об'єктів національних інтересів в інформаційній сфері через брак необхідних для цього соціальних, політичних, економічних та інших ресурсів. У цих випадках мета функціонування правових механізмів протидії загрозам може полягати в запобіганні та припиненні проявів цих загроз, а також мінімізації їхніх наслідків.

Запобігання проявам загроз об'єктам національних інтересів в інформаційній сфері полягає у створенні умов, за яких імовірність прояву цих загроз істотно знижується. Це досягається тоді, коли істотно мінімізується очікуваний від реалізації загроз політичний, економічний, соціальний чи інший ефект. Зниження загроз можна досягнути:

по-перше, застосувавши до суб'єктів, через дії котрих реалізуються загрози об'єктам національних інтересів, достатньої міри юридичної відповідальності;

по-друге, підвищивши захищеність об'єктів загроз. Приміром, загроза знищення документів, що мають важливе значення для збереження й розвитку нації, може бути значною мірою попереджена шляхом встановлення для даних документів особливого правового режиму, котрий регламентує порядок їх зберігання та доступу до них, а також можливості застосування достатньої міри юридичної відповідальності до осіб, що

порушують цей режим.

Припинення проявів загроз спрямоване на виявлення фактів прояву загроз та вжиття заходів щодо припинення негативного впливу на об'єкт національних інтересів в інформаційній сфері. Припинення проявів загрози здійснення комп'ютерних злочинів як мета правового забезпечення інформаційної безпеки полягає у створенні умов, за яких надійно й оперативно можна встановити факт початку протиправного діяння, конкретного суб'єкта, що здійснює його, а також зафіксувати ознаки об'єктивних та суб'єктивних складників злочину у необхідній для подання в судові органи формі, тобто вжити заходів для припинення протиправного діяння.

Мінімізація наслідків проявів загроз полягає у створенні правових умов для зменшення завданої об'єктам національних інтересів в інформаційній сфері шкоди, а також для ліквідації, якщо це можливо, наслідків реалізації загроз. Цього можна досягти шляхом правого закріплення вимог до захищеності даних об'єктів, а також встановлення порядку відшкодування суб'єктами, котрі завдали шкоди, коштів, витрачених на ліквідацію наслідків проявів загроз. Так, мінімізувати наслідки реалізації загроз безпеці функціонування критично важливих об'єктів національної інформаційної інфраструктури можна досягти правовим закріпленням регламентів, що встановлюють вимоги до сертифікації технічного і програмного забезпечення цих об'єктів, організації системи управління безпекою, а також процедури контролю рівня їх реальної захищеності й відповідальності посадових осіб за дотримання регламентів і приписів контрольних органів.

Правове забезпечення інформаційної безпеки утворюється сукупністю інститутів і норм інформаційного, конституційного, цивільного, адміністративного та кримінального права, що регулюють відносини у сфері протидії загрозам безпеці об'єктів національних інтересів в інформаційній сфері. У зв'язку з цим уважаємо за доцільне розглядати

правове забезпечення інформаційної безпеки самостійним комплексним напрямом правового регулювання, що здійснюється в межах реалізації державної політики в галузі забезпечення інформаційної безпеки держави.

У цьому контексті правильним убачається твердження О.Баранова, що з-поміж проблем забезпечення інформаційної безпеки особливе місце посідає правова. Недосконалість правового регулювання різноманіття інформаційних відносин гальмує як розвиток і вдосконалення політичних, економічних, матеріальних та інших відносин в суспільстві, так і власне сам процес забезпечення інформаційної безпеки. Тому це, особливо в сучасних умовах життя нашого суспільства, зумовлює потребу невідкладного вирішення правових проблем регулювання інформаційних відносин [108, с. 34].

Основною метою правового забезпечення інформаційної безпеки є створення законодавчих засад для попередження, припинення й ліквідації загроз безпеці основних об’єктів національних інтересів в інформаційній сфері, а також мінімізації наслідків проявів цих загроз.

У цьому ракурсі доцільним убачається виокремити два пріоритетних, на нашу думку, напрями вдосконалення правового забезпечення інформаційної безпеки держави на сучасному етапі:

1) підвищення структурної впорядкованості нормативних правових актів, що закріплюють правові норми розглянутого правового забезпечення;

2) удосконалення нормативного правового забезпечення інформаційної безпеки, власне, - усунення законодавчих прогалин, що перешкоджають організації ефективної протидії загрозам національним інтересам України в інформаційній сфері.

Виконання цих завдань має здійснюватися в межах скоординованої діяльності всіх суб’єктів права законодавчої ініціативи, чого можна домогтися на основі політичного документа, який визначатиме в установленому законодавством порядку основні пріоритети законотворчої

роботи в цій галузі.

При підготовці такого документа слід виходити з таких основних положень.

Документ має містити сукупність офіційних поглядів на цілі, завдання та напрями державної політики в галузі вдосконалення законодавства, яке регулює суспільні відносини щодо протидії загрозам національним інтересам України в інформаційній сфері.

Удосконалення нормативного правового забезпечення інформаційної безпеки має відбуватися на таких основних принципах:

- *принцип формування та застосування норм міжнародного права* як складової частини правової системи України;
- *принцип забезпечення балансу інтересів особистості, суспільства й держави*;
- *узгодженість діяльності органів державної влади* щодо вдосконалення нормативного правового забезпечення інформаційної безпеки.

Принцип формування і застосування норм міжнародного права як складової частини правової системи України передбачає пряму дію загальновизнаних принципів і норм міжнародного права, міжнародних договорів на всій території країни, а також активну й злагоджену участь органів виконавчої влади України в розробленні міжнародно-правових актів, які стосуються досягнення національних інтересів України в інформаційній сфері та забезпечення їхньої безпеки.

Принцип балансу інтересів людини, суспільства й держави передбачає встановлення й дотримання пріоритетів цих інтересів при регулюванні суспільних відносин в інформаційній сфері. При визначенні балансу інтересів особи, суспільства й держави маємо виходити з того, що Україна - це соціальна держава, політика якої спрямована на створення умов для гідного життя і вільного розвитку людини, реалізацію гарантій дотримання прав і свобод людини і громадянина, організацію протидії

загрозам національній безпеці України за участю громадян і громадських організацій.

Принцип узгодженості діяльності органів державної влади із нормативного правового забезпечення інформаційної безпеки передбачає організацію цієї діяльності на основі пріоритету компетенції України в безпековій сфері й повноти державної влади в галузі розвитку та використання регіональних інформаційних і телекомунікаційних систем, мереж зв'язку, регіональних інформаційних ресурсів.

Висновки до розділу 1

Зіставлення різних позицій стосовно визначення змісту поняття «інформаційна безпека» показав, що цей складний феномен ми не можемо розглянути всебічно з позиції тільки одного з аналізованих підходів. На нашу думку, найвність у доктрині різних концепція правового забезпечення інформаційної безпеки України пов'язане з тим, що інформаційна безпека як феномен соціокультурного явища є складною багаторівневою функціональною системою. Інформаційна безпека України, крім іншого, є невід'ємною складовою частиною системи забезпечення аціональної безпеки в цілому. Визначено у розділі, що основними структурними елементами системи правового забезпечення інформаційної безпеки України є особа, суспільство й держава, їх життєво важливі інтереси, а також загрози в інформаційній сфері. Багатоманітність поглядів, які доповнюють один одного, дозволяє підійти до проблеми інформаційної безпеки з позиції комплексного підходу. Це дає змогу доповнити наявні знання про таке складне і багаторівневе явище, яким є інформаційна безпека. Відтак, під поняттям «інформаційна безпека» пропонується розуміти стан захищеності життєво важливих інтересів особи, суспільства і держави в інформаційній сфері від внутрішніх і

зовнішніх загроз, що забезпечує стійкий розвиток.

Водночас, це і процес, оскільки інформаційна безпека якнайщільніше пов'язана з культурним середовищем і є атрибутом соціокультурного життя суспільства, в якому діють політична влада, суспільно-політичні сили й течії, беруть участь індивіди, соціальні групи, спонукувані економічними й соціально-політичними потребами, інтересами та цілями. Вказана обставина передбачає розкриття наявних зв'язків серед суб'єктів і об'єктів безпеки, їх інтересів, а також тенденцій і закономірностей їх розвитку, понять, за допомогою яких вирізняють загрози із сукупності різних чинників і явищ навколишньої дійсності, що вказує на існування глибокого взаємозв'язку між інформаційною безпекою й усіма сферами життєдіяльності суспільства.

З одного боку, цей взаємозв'язок зумовлений необхідністю координації дій суб'єктів суспільства, що виникає саме тоді, коли суперечності та конфлікти усередині соціальної спільноти й у взаєминах її із зовнішнім середовищем створюють загрози існуванню й розвитку соціуму. У цьому разі ціннісна система виступає головним регулятором суспільних відносин у всіх сферах життєдіяльності суспільства, визначаючи цілі та завдання в системі забезпечення інформаційної безпеки. З іншого боку, інформаційна безпека виступає однією з базових цінностей сучасного суспільства, і в цьому сенсі виявляється її домінуючий вплив, що виражає соціальні цінності та практичні заходи, спрямовані на формування і захист цих цінностей.

Складна воєнно-політична ситуація, яка склалася внаслідок збройної агресії Росії проти України, анексії та окупації частини суверенної території України, проведення антитерористичної операції (операції об'єднаних сил) в окремих районах Донецької та Луганської областей, де триває інспірований та підтримуваний Російською Федерацією збройний конфлікт, набуває загрозливих проявів також в інформаційному просторі. У сукупності зі стратегічним значенням інформаційної сфери для сталого

розвитку сучасного суспільства це зумовлює пріоритетний характер інформаційної безпеки у системі національної безпеки України. Відповідно, надзвичайно важливим є правильне осягнення змісту категорії «інформаційна безпека», що неможливо зробити без її наукового визначення. Тож, проаналізувавши різні підходи до визначення категорії «інформаційна безпека», які дають змогу зрозуміти це явище комплексно і системно, пропонуємо розглядати інформаційну безпеку як постійний процес діяльності компетентних органів, спрямований на попередження, протидію загрозам в інформаційній сфері, застосування активних заходів інформаційного впливу, а також сукупність умов такої діяльності, які реалізуються і здатні контролюватися тривалий час.

Інформаційна безпека як ключова складова національної безпеки охоплює такі пріоритетні напрями: забезпечення захисту інформаційного простору та забезпечення стану захищеності культурного генофонду людства в умовах глобалізації. Важливо ще раз підкреслити, що поряд із правовими та організаційно-технічними засобами й методами важливими компонентами процесу забезпечення безпеки інформаційного середовища є соціокультурні аспекти.

Основні результати даного розділу висвітлено у працях [109-114].

РОЗДІЛ 2.
ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ЄВРОІНТЕГРАЦІЇ УКРАЇНИ

2.1. Правове забезпечення інформаційної безпеки України як складова інформаційного права

У правознавстві, як і в науці в цілому та інших сферах суспільної діяльності, одним із провідних при вивченні складних явищ, до яких належить і право, є системний метод. Хоча визначень поняття «система» існує дуже багато, усі вони зводяться, по суті, до таких: «комплекс елементів, що взаємодіють» [115, с. 52], «будь-який набір елементів (матеріальних, енергетичних, інформаційних), виокремлених разом за певним принципом із інших елементів навколишнього світу» [116, с. 73], «будь-який об'єкт, котрий, з одного боку, розглядається як єдине ціле, а з другого, – як множина складових частин, що пов'язані чи взаємодіють між собою» [117, с. 9].

Що стосується права, то воно є вельми складною цілісною системою, яка охоплює структуру (внутрішню побудову) права, у якій відбивається об'єднання й розмежування юридичних норм. Специфіка права, на думку С.Алексєєва, в тому, що воно має низку рис, характерних для систем органічних, а «розвиненість права зумовлює зростання його органічності як системи» [118, с. 238]. Право, зазначає далі дослідник, – це складне системне утворення, єдиний організм, котрому притаманні ієрархічна будова, інтегративні властивості, генетичні й функціональні зв'язки тощо. При цьому структура є специфічним, незмінним чинником системи, який

забезпечує впорядкованість її елементів, їх внутрішню організацію, способи взаємозв'язку [119, с. 4]. Саме завдяки системності права, стверджує С.Алексєєв, юридично різнорідні норми спроможні системно регулювати суспільні відносини, тобто методами, що взаємно пов'язані, здійснюючи на них різнобічний і водночас узгоджений, цілісний вплив [119, с. 72]. Наведені ознаки системи права відзначають й деякі інші вітчизняні й зарубіжні правники.

Звертаючись до питання структурування правового забезпечення інформаційної безпеки, слід передусім зазначити, що йдеться про формування та розвиток у системі права певного структурного утворення, яке це забезпечення регулює. А передумовами цього є чинники й тенденції не лише самої сфери інформаційних інтересів та їх захисту (предмета вказаного забезпечення), але й формування комплексних галузей законодавства та загалом системи права, а також методологічних здобутків юридичної науки щодо формування структури права. Інформаційне право є найбільш динамічною галуззю з-посеред інших. А тому й виникнення нових підгалузей, інститутів інформаційного права є закономірним та очевидним результатом еволюції цієї правової галузі. Відповідно, абсолютно правильним є твердження О.Сосніна, що, перебуваючи на порозі інформаційного суспільства, зволікання з розробленням його правового фундаменту здатне породити негативні наслідки для суспільства й держави [120, с. 101].

Викладене вище дає підстави виокремити три групи передумов формування в Україні правового утворення із забезпечення інформаційної безпеки. Вони об'єднують чинники й тенденції розвитку:

по-перше, інформаційної сфери;

по-друге, системи права на сучасному історичному етапі;

по-третє, вітчизняної й зарубіжної юриспруденції.

Щодо першої групи слід насамперед підкреслити величезне зростання ролі інформації в усіх сферах життєдіяльності людства.

Особливо це стосується економіки, здатності виробляти найскладнішу продукцію, значного підвищення попиту на відомості, які сприяють налагодженню такого виробництва, а також на відповідні інформаційні послуги. У результаті для все більшої частини населення знання й інформація стають основними предметами праці, а інформаційні технології – знаряддям виробництва. Інформаційні технології, зазначається у так званій Декларації тисячоліття (принципах побудови інформаційного суспільства), відкривають якісно нові горизонти прогресивного розвитку людини й суспільства.

Утім, як свідчить історія, науково-технічний прогрес має й інший бік. Нерідко його досягнення стають джерелом загроз не тільки для окремих людей, громад, держав, а й для всього людства. Відтак, не викликає сумнівів потреба забезпечення в інформаційному суспільстві захищеності законних інтересів. Вона може полягати у відповідних положеннях об’єктивного права або випливати із його загального духу, в існуванні належних механізмів (державних інститутів) захисту законних прав та інтересів та їх відновлення в разі порушення.

Не секрет, що у процесі суспільного розвитку неминуче виникають різноманітні конфлікти інтересів, котрі, як зазначав американський соціолог, відомий дослідник соціальних конфліктів Льюїс Козер, спричиняють «боротьбу за цінності та претензії на певний соціальний статус, владу та матеріальні й духовні блага, яких бракує на всіх; боротьбу, де метою сторін, які конфліктують, є нейтралізація, завдання шкоди чи знищення суперника» [121, с. 41]. Саме право і є тим суспільним інструментом, який дає змогу залагоджувати, зменшувати подібні конфлікти чи навіть зовсім їх уникати.

Утім, цей інструмент теж потребує постійного вдосконалення разом із розвитком суспільства. Зазвичай виникнення конфлікту юридичного як суперечки суб’єктів права із застосуванням чи тлумаченням відповідних норм пов’язане із існуванням у правозастосовній практиці правових

колізій, зумовлених недосконалістю чинного законодавства. Тут на передній план виходить охоронна (запобіжна) функція права, яка полягає у захисті, забезпеченні недоторканності усталених суспільних відносин, а також недопущенні чи припиненні відносин, шкідливих для людини, суспільства та держави.

В умовах інформаційної агресії з боку РФ та виникнення нових глобальних викликів у цій сфері, з огляду на потребу ефективного захисту українського суспільства й держави вагомість такої функції останньої, як правове забезпечення інформаційної безпеки, значно зростає. Слід також підкреслити, що інформаційна безпека є сьогодні однією із найважливіших складових національної безпеки України, значною мірою визначаючи стан захищеності, зокрема і правової, її життєво важливих інтересів. Окінавська хартія глобального інформаційного суспільства [122] також визнала правове забезпечення інформаційної безпеки одним із пріоритетів при розбудові такого суспільства.

Як бачимо, названі вище передумови створення у системі права структури, пов’язаної із забезпеченням інформаційної безпеки, випливають із науково-технічного прогресу, формування суспільства інформаційного типу, проникнення інформаційних технологій в усі сфери життя, виникнення на цьому ґрунті нових загроз та викликів і потреби протидіяти цим загрозам.

До *другої групи* вказаних передумов належать чинники, пов’язані із предметом правового регулювання, тобто з’ясуванням місця правового забезпечення інформаційної безпеки в загальній системі інформаційних відносин. Саме системний підхід при дослідженні складних динамічних феноменів, яким і є інформаційні відносини, дає змогу не лише виявити внутрішні рушійні сили їхніх складників, а й розкрити механізми їх взаємодії з іншими елементами й на різних щаблях.

У цьому контексті слушними вбачаються міркування І. Бачило про те, що в інформаційній сфері право не втрачає свого головного

призначення: «Воно покликане регулювати відносини, пов’язані з інформацією… у процесах інформаційного забезпечення усіх інших відносин найрізноманітніших суб’єктів. Право регулює, диктує й водночас відчуває усі перипетії, притаманні сьогочасному інформаційному середовищу. Воно й саме змінюється, виявляючи нові об’єкти регулювання, трансформуючи методи свого впливу на суспільні відносини» [123, с. 27].

Як ми з’ясували вище, правове забезпечення інформаційної безпеки можна визначити як цілісну систему правового регулювання суспільних відносин, що виникають при протидії загрозам національній безпеці України в інформаційній сфері. Тобто, вказаний правовий феномен має власний предмет правового регулювання. Особливості регульованих ним правовідносин випливають насамперед зі специфіки самої інформаційної сфери життя суспільства, зміст якої становить соціальна діяльність зі створення, поширення, трансформації та споживання інформації. При цьому об’єктом відносин, які належать до такої діяльності, має бути інформація та відповідна інфраструктура.

Водночас, забезпечення інформаційної безпеки є одним із різновидів інформаційної діяльності, яка полягає у виконанні певним суб’єктом у межах свого правового статусу функцій із охорони та захисту інформаційних масивів і технологій, засобів і каналів зв’язку. Ця діяльність спрямована на запобігання загрозам безпеці об’єктам національних інтересів у цій сфері, протидію неправомірним зазіханням різноманітних суб’єктів, що можуть зашкодити вказаним об’єктам. Цілком зрозуміло, що са́ме право є головним засобом і найдійовішим інструментарієм зазначеної діяльності.

Досить слушним вбачається твердження О.Золотар, що питання правового забезпечення інформаційної безпеки визначаються на межі інформаційної політики держав та політики національної безпеки [124, с. 71].

Отже, відокремленим предметом аналізованого структурного новоутворення правової системи є суспільні відносини, що виникають при протидії загрозам національній безпеці України в інформаційній сфері. При цьому вказана окремішність зумовлена здебільшого особливостями правового забезпечення інформаційної безпеки як різновиду інформаційної діяльності. Про це може також свідчити структура законодавства, пов'язаного з інформаційною сферою, де правове забезпечення інформаційної безпеки як частина інформаційної діяльності представлене такими щільно взаємопов'язаними складовими, як захист державної, комерційної, банківської, лікарської та іншої таємниці, персональних даних, захист від розповсюдження підривної, шкідливої, недостовірної інформації тощо.

Відтак, убачається нагальною потреба чіткого правового врегулювання суспільних відносин у вказаній сфері, виокремлення у вітчизняній правовій системі структури, відповідальної за правове забезпечення інформаційної безпеки. Це створить умови для системного, комплексного розгляду законодавчих положень щодо забезпечення інформаційної безпеки, оперативного виявлення та усунення лакун і суперечностей у них.

Таким чином, поряд із зазначеним вище виокремленням предмета правового регулювання формується новий комплексний інформаційний феномен – інформаційне право, а в межах останнього й на основі чинного вітчизняного законодавства – модель формування утворення з правового забезпечення інформаційної безпеки.

Нарешті, *третя група чинників* створення зазначеної структури зумовлена, як зазначалося вище, тенденціями розвитку сучасної юриспруденції, спрямованими на вдосконалення системи права та її складових частин. Так, у юридичній науці закладено вельми міцне теоретичне підґрунтя щодо функціонування в системі права різноманітних комплексних утворень. Стосовно нової сукупності суспільних відносин,

що виникають в інформаційній сфері й навколо неї, цей доробок втілено у певних настановах, або засадах, які сприяють з'ясуванню змісту цих відносин, спрямовують процес їх пізнання.

Набуваючи рівня наукових принципів, за якими здійснюються наукові дослідження, ці теоретичні погляди й настанови стають своєрідними засадничими чинниками, передумовами створення нового знання.

Перелічені вище чинники й тенденції формування інформаційного суспільства, виникнення пов'язаних із цим проблем, загроз і викликів об'єктивно зумовили підвищення вагомості правових аспектів цього процесу й, відповідно, зростання уваги до питань інформаційної безпеки з боку юридичної науки. Саме вона відіграла, напевне, провідну роль у створенні теоретично виваженої, стрункої моделі забезпечення інформаційної безпеки людини, суспільства, держави.

Можна стверджувати, що вказаний доробок вітчизняних і зарубіжних правників створив підвалини науки інформаційного права. Це, у свою чергу, зумовило пожвавлення досліджень безпекових питань, пов'язаних з інформаційною сферою, а також відкрило нові грані загальної проблематики щодо правового забезпечення в умовах інформаційного суспільства таких напрямів, як:

- безпека особи, суспільства й держави;
- удосконалення інститутів відповідальності (суспільні відносини, пов'язані з інформаційною сферою, допоки інформаційне право не набуло статусу окремої галузі, регулювалися в межах інституту таємниці – державної, комерційної та ін., а відповідальність за правопорушення передбачалася виключно цивільно-, адміністративно- чи кримінально-правова).

Як уже зазначалося вище, правовідносини, пов'язані з інформацією, пронизують ледь не всі сфери життєдіяльності суспільства. Тому регулювання цих відносин має бути комплексним, із застосуванням норм

різних галузей. Себто комплексність притаманна не лише галузі інформаційного права загалом, а й усім її складовим частинам – підгалузям, інститутам, субінститутам.

Варто додати, що сама природа феномена інформації зумовлює такий характер галузі. Норберт Вінер, один із «батьків» кібернетики, дав таке визначення інформації: «…позначення змісту, отриманого із зовнішнього світу у процесі нашого пристосування до нього й прилаштування до нього наших відчуттів» [85, с. 55]. Сьогодні інформація за своїм значення для розвитку людства перевищила будь-які інші матеріальні чи енергетичні ресурси. Багатоманітні суспільні відносини, які складаються у цій сфері, регулюються нормами таких традиційних правових галузей, як конституційне, цивільне, адміністративне, кримінальне право та ін. Проте лавиноподібне зростання інформаційних технологій і масове користування ними, специфіка інформаційної сфери та її об’єктів висунули на порядок денний необхідність систематизації вказаних норм та об’єднання їх у самостійну комплексну галузь – інформаційне право.

Відомі дослідники інформаційного права В.Пилипчук та В.Брижко розкривають актуальність проблеми формування нормативно-правової бази у сфері інформаційних відносин та її подальшого розвитку в контексті євроінтеграції України, імплементації норм європейського та міжнародного інформаційного права у національне інформаційне законодавство, а також проблеми систематизації останнього. При цьому до основних напрямів упорядкування та регулювання інформаційних відносин, які утворюють правове поле інформаційної діяльності, належить й інформаційна безпека держави [125, с. 11, 18].

М. Мирошниченко в авторефераті дисертації теж підкреслює, що для протидії масштабним негативним впливам важливим є інтеграція України до світового та регіонального європейського інформаційного просторів [126, с. 7].

Слушним є зауваження К. Захаренка про те, що дуже важливо, щоб і в Україні постійно активізувався та актуалізувався науково-теоретичний дискурс, спрямований на інтегральне та структурно-функціональне дослідження багатовимірної проблематики інформаційної безпеки [127, с. 45].

Як бачимо, потреба формування такої комплексної правової галузі, як інформаційне право, цілком об'єктивно випливає із самої його природи й зумовлена наведеними вище чинниками. З нагальності й різнобічності питань, пов'язаних з інформацією, кількість котрих з останньої чверті XX століття зростає ледь не з геометричною прогресією, випливає необхідність виокремлення відповідних суспільних відносин і формування усередині галузі спеціалізованих інститутів, підгалузей та інших структурних утворень, які мають свій специфічний предмет правового регулювання. Цей предмет – багатоманітні різновиди відносин у різних сферах й умовах діяльності, пов'язаних з одним об'єктом – інформацією.

Такими структурними утвореннями галузі інформаційного права є інститути, тобто підпорядковані єдиній меті сукупності нормативно-правових актів і положень, які регулюють усе розмаїття відносин у сфері створення й використання інформаційно-комунікаційних ресурсів і технологій, захисту законних інтересів суб'єктів цієї діяльності тощо. Зрозуміло, що вказані об'єктивні потреби зумовили не лише сплеск наукових досліджень проблематики, скажімо, комерційної таємниці чи захисту персональних даних, а і прийняття останнім часом низки відповідних законодавчих актів.

Цілком очевидним є щільний взаємозв'язок забезпечення інформаційної безпеки з іншими складовими частинами інформаційного права, а також багатьох інститутів інших галузей права. Так, функції забезпечення інформаційної безпеки здійснюються при:

- підтриманні правових режимів певних видів інформації;

- забезпеченні відповідальності за порушення нормативних вимог щодо інформаційної безпеки;
- встановленні правового режиму інформаційних ресурсів інформаційних технологій та ін.

Таким чином, за допомогою загальної теорії систем ми виявили, що у вітчизняній системі права з’явився новий елемент, котрий регулює відносини, пов'язані з правовим забезпеченням інформаційної безпеки, а також проаналізували причини й передумови його виникнення. Головними чинниками цього є передусім бурхливий розвиток інформаційних технологій, значне підвищення вагомості інформаційних ресурсів, становлення в Україні інформаційного суспільства, виникнення загроз людині, суспільству й державі у цій сфері й формування на цьому ґрунті нових суспільних відносин, пов’язаних з інформацією.

Тому ми солідарні з думкою О.Яреми, що правове забезпечення інформаційної безпеки є частиною системи інформаційного права, що зумовлено комплексною природою останнього [128, с. 251]. Проведений аналіз зазначених передумов дає підстави стверджувати, що вирішальними у виникненні в системі вітчизняного права нового структурного елемента, пов’язаного із правовим забезпеченням інтересів суб’єктів інформаційних відносин, стали три групи чинників, стійких тенденцій інституційного характеру.

Це, по-перше, величезне зростання ролі й значущості інформації в усіх сферах життєдіяльності, масовості використання відповідних засобів і технологій; розвиток на цій основі інформаційного суспільства та інформаційних суспільних відносин. Зрозуміло, вказані процеси мають не лише позитивний бік. Навколо інформаційних ресурсів і технологій виникають конфлікти інтересів суб’єктів інформаційних відносин, загрози їх життєво важливим інтересам. Усі ці питання потребують регулювання, захисту й забезпечення правовими засобами.

По-друге, у процесі діяльності щодо забезпечення інформаційної безпеки як різновиду інформаційних правовідносин виникають відносини, пов’язані із захистом відповідних законних інтересів особи, суспільства й держави від зовнішніх і внутрішніх загроз, і, таким чином, виокремлюється новий предмет правового регулювання.

Нарешті, по-третє, це чинники суто науково-методологічні, а також об’єктивний суспільний запит до юридичної науки щодо вдосконалення правового забезпечення інформаційної безпеки.

Усе це зумовило теоретичне обґрунтування існування в системі права такої галузі, як інформаційне право, а також об’єктивне виникнення утворення з правового забезпечення інформаційної безпеки як складової частини останнього – **підгалузі інформаційного права**. Тому ми не зовсім згодні з позицією тих науковців, які вважають, що інформаційну безпеку слід розуміти як відокремлений інститут інформаційного права, що розглядає не тільки захист інформації, але й організаційні, політичні, правові та інші заходи, спрямовані на забезпечення стійкого, стабільного розвитку суспільства й держави [83, с. 22].

Утім, слід визнати наявність багатьох невирішених проблем. Так, питання інформаційної безпеки в деяких сферах життєдіяльності суспільства залишаються неврегульованими, відповідне законодавство має також певні вади, зумовлені браком структурованості правового забезпечення інформаційної безпеки. Існують у законодавстві недоліки термінологічного характеру. Зокрема, відсутнє законодавче визначення поняття «інформаційна безпека держави», а також низки інших важливих понять, пов’язаних з кібернетичними загрозами, кібератаками та ін. Отже, вдосконалення чинного законодавства України з питань забезпечення інформаційної безпеки вбачається шляхом закладення міцної теоретичної бази, наукового обґрунтування природи, структури та місця в системі права утворення з правового забезпечення інформаційної безпеки. У цьому контексті слушним є зауваження І.Панової, що сучасна система

українського інформаційного права у зв’язку із розвитком суспільних відносин зазнає істотних змін, наповнюється новим змістом. З’являються і розвиваються нові правові інститути – захисту персональних даних, інформаційної безпеки, журналістики тощо [129].

Що стосується правового забезпечення інформаційної безпеки, то кожен із згаданих інститутів інформаційного права регулює «свою» ділянку цієї сфери. Це, приміром, інститути таємниці, інститут захисту інформації з обмеженим доступом, інститут відповідальності за порушення у цій сфері та ін. Тому цілком логічним убачається припущення, що правове забезпечення інформаційної безпеки є правовим феноменом, ширшим за традиційне розуміння правового інституту.

Отже, така атрибутивна характеристика природи інформаційного права, як комплексність, стосується й усіх його інститутів. Це, своєю чергою, зумовлює зв'язок між обґрунтуванням комплексної природи сукупності правових інститутів, що регулюють правове забезпечення інформаційної безпеки, та обґрунтуванням її стосунку саме до галузі інформаційного права.

Ще одним системоутворювальним чинником, котрий зумовлює формування галузей права, є предмет правового регулювання. Стосовно правового забезпечення інформаційної безпеки цим предметом ми визначили суспільні відносини, пов’язані із забезпеченням безпеки об’єктів і суб’єктів функціонування інформаційного середовища, що дозволяє віднести це структурне утворення в системі вітчизняного права саме до галузі інформаційного права.

Як уже зазначалося вище, переважна більшість фахівців уважають захист та охорону інформації й відповідних ресурсів, а отже й відносин, що виникають у цій сфері, різновидами саме інформаційної діяльності та інформаційних правовідносин. Продовжуючи логічний ланцюжок від загального – «інформаційна безпека» до окремого – «захист інформації», доходимо висновку, що забезпечення інформаційної безпеки як різновид

інформаційної діяльності порівняно із захистом інформації охоплює значно ширше коло питань. Своїм об'єктом ця діяльність має інформацію, щодо якої в особи, суспільства й держави виникають певні інтереси, котрі потребують правового врегулювання, – регламентації, правового захисту, забезпечення стану захищеності, охорони тощо. Відносини, які можна назвати інформаційними, що пов'язані з інформацією, відповідними ресурсами, технологіями, комунікаціями, засобами, формують специфічну галузь відносин, котра містить, зокрема, спеціальний комплекс відносин щодо забезпечення інформаційної безпеки держави. У свою чергу, в цьому комплексі виокремлюється певне структурне утворення, пов'язане із правовим забезпеченням інформаційної безпеки. Усе це дає підстави для висновку, що назване нами структурне утворення, яке регулює інформаційні правовідносини, є невід'ємною частиною галузі інформаційного права.

Як уже зазначалося, інформація, середовище та інфраструктура, яке вона створює, сукупність суб'єктів, пов'язаних з ним, суспільні відносини, котрі тут виникають, формують інформаційну сферу життєдіяльності людини, суспільства, держави. Задля забезпечення безпеки цієї сфери держава повинна виробити й утілювати в життя єдину, цілеспрямовану політику. У складних умовах сьогодення українська держава виробила доктрини інформаційної та кібернетичної безпеки, формується та вдосконалюється відповідне законодавство, спрямоване на захист національних інтересів України у цій сфері.

Нині є всі підстави стверджувати, що у країні створена система, яка досить чітко регулює відносини, що складаються у зв'язку із забезпеченням інформаційної безпеки держави. Деякі аспекти цих відносин унормовані положеннями конституційного, адміністративного та інших «базових» галузей правової системи. Проте, як вище вже доводилося, об'єднати всі ці положення й регулювати цей різновид діяльності має окреме правове утворення зі своєю власною структурою

(комплексні інститути, субінститути тощо) та внутрішньою організацією. Так, до комплексних інститутів правового забезпечення інформаційної безпеки держави належать:

1) інститут таємниці (державної, комерційної, лікарської та ін.);

2) інститут захисту інформації, який містить субінститути ліцензування діяльності у цій сфері та захисту персональних даних;

3) інститут відповідальності за правопорушення в інформаційній сфері.

Вельми вагомим внеском у дослідження цієї проблематики є стаття О.Баранова «Інститути інформаційного права», де вчений класифікував їх таким чином: за процесом створення інформації (інститут права на свободу думки, інститут ЗМІ та ін.); відповідно до процесу поширення інформації (інститут телекомунікацій, інститут поштового зв’язку та ін.); інститути забезпечення інформаційної безпеки, у рамках якої дослідник відокремив суспільні відносини, пов'язані із забезпеченням мінімізації збитку від несанкціонованого поширення, використання і знищення інформації (інститут правового режиму інформації, інститут захисту інформації та ін.) [130, с. 40, 42, 43].

Указане самостійне комплексне правове утворення, виходячи із мети діяльності й характеру відповідних суспільних відносин, за допомогою сукупності нормативних правових засобів – дозволів, стимулів, заборон, обмежень тощо – має формувати окремий правовий режим. Наприклад, правовий режим захисту інформації з обмеженим доступом передбачає комплексне застосування таких правових засобів, як обмеження, покладання обов’язку, заборона тощо. Прикладом можуть слугувати переліки відомостей, що мають різний ступінь доступу (обмеження), вимога до володільця інформації, що становить комерційну таємницю, вживати певних заходів з її охорони (ставлення в обов’язок), вимога нерозповсюдження персональних даних (заборона).

Формування правової галузі шляхом інтегрування інститутів права вважається багатьма дослідниками найвищим рівнем її побудови. Відомий теоретик права С.Алексєєв зазначав, зокрема, що завдяки виділенню деяких нормативних положень з наступним їх групуванням за певними ознаками в окремих галузях зі споріднених інститутів формуються більші за розміром структури, так звані об'єднання. У кодифікованих нормативно-правових актах такі структури зазвичай утворюють частини чи розділи. Найбільш складним і розвинутим із таких об'єднань визнається правова підгалузь [118, с. 64].

Оскільки правове забезпечення інформаційної безпеки держави має у своєму складі згадувані вище специфічні правові інститути, але за своєю комплексною природою та предметом регулювання належить до сфери інформаційного права, його не можна вважати самостійною правовою галуззю. Відтак, розглядуваний нами феномен є об'єднанням правових інститутів з високим рівнем диференціації, інтегрування та спеціалізації своїх сукупних структурних елементів, який можна назвати підгалуззю інформаційного права.

Підтвердженням останньої тези може бути й те, що вказане правове об'єднання містить положення, які внормовують різні види однорідних відносин (скажімо, пов'язані з державною та іншою таємницею), а також такі, що передбачають набуття певних прав і обов'язків (приміром, співробітників, котрі працюють з персональними даними). Утім, зазначене питання залишається актуальним у науковому сенсі, позаяк до теперішнього часу не стало предметом самостійного комплексного дослідження.

Тим часом, назріло прийняття єдиного, консолідуючого законодавчого акта з питань інформаційної безпеки, що зумовлено об'єктивними реаліями формування підгалузі правового забезпечення інформаційної безпеки, – Закону України «Про забезпечення інформаційної безпеки України».

Отже, правове забезпечення інформаційної безпеки України є складовою частиною комплексної галузі інформаційного права, котре, у свою чергу, як і всі інші комплексні галузі, належить до певної «базової» галузі права. Комплексна за предметною ознакою галузь інформаційного права є також комплексною і за методами правового регулювання (дозвіл, заборона, примус, покарання тощо). Тобто, підгалузь правового забезпечення інформаційної безпеки також тісно взаємодіє з такими «основними», на думку багатьох правників, галузями, як конституційне, адміністративне, цивільне, кримінальне право. Ця підгалузь консолідує норми вказаних галузей, що стосуються сфери регульованих нею відносин, сполучає й застосовує притаманні їм методи, способи, засоби та прийоми правового регулювання.

Зокрема, в інститутах таємниці та захисту інформації, відповідальності за порушення в інформаційній сфері сполучаються методи захисту і примусу з дозволом, а також покаранням.

Слід підкреслити, що присутність приватних інтересів, пов’язаних, скажімо, з комерційною таємницею, за імперативного характеру регулювання не свідчить про перетворення приватноправових відносин на публічно-правові. Передусім це стосується комерційної таємниці підприємств, які мають особливо важливе та стратегічне значення як для економіки держави, так і для підтримки життєздатності суспільства взагалі.

Констатуючи формування в межах правової науки нової спільноти, яка об’єднала елементи адміністративного, фінансового та інформаційного права, І.Бачило вважає, що інформаційне право – це новітня комплексна галузь публічного права, котра в широкому розумінні входить до сімейства адміністративного права [131, с. 97-98]. Очевидний щільний зв'язок управлінських та інформаційних процесів є зайвим підтвердженням наведеної думки дослідника. Так, згадуваний вище засновник кібернетики Н.Вінер поняття «управління» й «комунікація» фактично ототожнював,

позаяк керування одного суб'єкта діями іншого відбувається шляхом передання певних сигналів, що містять потрібну інформацію, у процесі комунікації. Дослідники вже давно схильні вважати інформацію передовсім засобом управління, відзначаючи безпосередню залежність прийняття управлінських рішень від наявності належної інформації. При цьому до виникнення самостійної комплексної галузі інформаційного права, котра консолідувала відповідні положення, ця сфера регулювалася здебільшого адміністративним правом, яке, власне, й унормовувало правовідносини в управлінській сфері. Що ж стосується забезпечення інформаційної безпеки держави, то тут варто підкреслити, що ряд фахівців безпекову діяльність взагалі відносять до сфери адміністративно-політичного управління. Відтак, правове забезпечення інформаційної безпеки як підгалузь інформаційного права теж слід віднести до адміністративно-правової родини, тим більше, що й основний метод правового регулювання – імперативний, яким послуговується ця підгалузь, теж запозичений із права адміністративного.

У контексті нашого дослідження не можна також оминути увагою взаємовплив правового забезпечення інформаційної безпеки держави як підгалузі інформаційного права та цивільного права. Так, цивільним законодавством регулюються питання, пов'язані з інтелектуальною власністю, об'єкти котрої як набуток розумової, творчої людської діяльності є насамперед різновидом інформації. На користь останньої тези говорить феномен так званого дуалізму інтелектуальної власності, який відзначається правниками-цивілістами.

Таким чином, розглядувані нами галузі перетинаються і взаємодіють у сфері об'єктів інтелектуальної власності як різновидів інформації, а підгалузь правового забезпечення інформаційної безпеки держави, зокрема, послуговується цивільно-правовими методами і способами в межах діяльності із захисту інформації. Отже, маємо всі підстави стверджувати, що захист інтелектуальної власності є складовою безпекової

діяльності в інформаційній сфері, а правові відносини, що виникають у зв'язку із вказаною діяльністю, є предметом як цивільного, так і інформаційного права. Крім того, підгалузь правового забезпечення інформаційної безпеки держави послуговується нормами цивільного законодавства щодо захисту об'єктів інтелектуальної власності, стосовно яких запроваджено режим комерційної таємниці. Останній інститут, як уже згадувалося, більшість фахівців відносить до складу інформаційного права.

Підбиваючи підсумки аналізу місця інституту правового забезпечення інформаційної безпеки держави в системі інформаційного права, зазначимо, що, по-перше, вказане правове структурне новоутворення у вітчизняній правовій системі має низку ознак підгалузі інформаційного права. Так, норми, які її складають, підпорядковані єдиній меті правового регулювання – забезпеченню інформаційної безпеки людини, суспільства, держави. Крім того, це утворення має відокремлений предмет правового регулювання, правовий режим, характеризується системним застосуванням притаманних галузі методів правового регулювання, значним інтегруванням та спеціалізацією правових інститутів, що його складають (а у складі останніх – субінститутів).

По-друге, правове забезпечення інформаційної безпеки України є підгалуззю інформаційного права. Це зумовлено їх комплексною природою, а також тим, що правові відносини, які виникають у зв'язку із забезпеченням інформаційної безпеки, охоплюються загальногалузевими правовідносинами. Водночас, вказана підгалузь є цілком самостійним правовим утворенням, до структури якого входять норми як власне інформаційного права, так і інших правових галузей, котрі регулюють специфічні суспільні відносини, що виникають з приводу захисту інформації з обмеженим доступом, ліцензування діяльності із захисту інформації, а також визначають відповідальність за правопорушення в інформаційній сфері.

Нарешті, по-третє, структуру правового забезпечення інформаційної безпеки держави як підгалузі інформаційного права складають інститути таємниці, захисту інформації (із субінститутом ліцензування такої діяльності), а також відповідальності за порушення у цій сфері.

2.2. Правова природа основних складових елементів інформаційної безпеки України

Проблематика забезпечення інформаційної безпеки України сьогодні привертає увагу науковців та практиків у різних сферах, утім питання визначення складових інформаційної безпеки та критеріїв, що використовуються з цією метою, досі залишається недостатньо розробленим. Не визначені складові інформаційної безпеки й на рівні законодавства. Тож актуальним убачається дослідження критеріїв виокремлення складових інформаційної безпеки та з'ясування їх сутності.

Попри те, що Конституція України з моменту свого затвердження відносить забезпечення інформаційної безпеки до найважливіших функцій держави [23], нормативне визначення інформаційної безпеки є відносно «свіжим». У Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» зазначалося, що інформаційна безпека – це «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається завдання шкоди через:

- неповноту, невчасність та невірогідність інформації, що використовується;
- негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій;
- несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» [132].

Таке визначення, як бачимо, не дає змоги дійти чіткого висновку щодо сутності складових інформаційної безпеки, так само, як і низка опосередкованих визначень, які розглядають інформаційну безпеку у контексті більш загального поняття – національної безпеки або ж торкаються її окремих аспектів, на кшталт інформаційної безпеки телекомунікаційних мереж [133].

На методологічному рівні предметна сфера інформаційної безпеки є єдиною, структурованою за завданнями та предметом дослідження, збалансованою за терміносистемою. Її системоутворювальним чинником виступають, безумовно, інформація та інформаційні процеси. Проте для виокремлення складових інформаційної безпеки на доктринальному рівні використовується досить широкий спектр критеріїв, що зумовлює диференціацію підходів до розуміння системного змісту поняття «інформаційна безпека».

Якщо звернутися до зарубіжних наукових джерел, можна переконатись, що найбільш популярною є точка зору, відповідно до якої складовими інформаційної безпеки визнаються цілісність, доступність та конфіденційність інформації [134-136].

Під цілісністю інформації розуміють її властивість не бути модифікованою неавторизованим користувачем і/або процесом, тобто, зберігатись у стані, визначеному її створювачем та законним володільцем, в тому числі й достовірність інформації як її відповідність дійсності в сенсі адекватності відображення.

Конфіденційність - це властивість інформації бути недоступною користувачам, які не мають на це права. Ця ознака пов’язана з розмежуванням інформації за режимом доступу.

Доступність інформації полягає в тому, що уповноважений користувач може користуватися нею відповідно до правил, встановлених політикою безпеки, не очікуючи понад установлений часовий проміжок, тобто це – властивість інформації перебувати у необхідному користувачеві

вигляді та місці в той час, коли вона йому необхідна.

Справді, належний стан вищезгаданих властивостей є важливим для забезпечення безпеки інформації. Крім того, завдяки забезпеченню безпеки інформації формується нова її властивість – безпечність, котра також є вагомим чинником інформаційної безпеки. Остання ж, окрім власне безпеки інформації, містить й інші складові. Так, в окремих випадках заподіяння шкоди належному стану властивостей інформації становить лише один із видів протиправних наслідків. Шкода завдається й іншим елементам інформаційної сфери, до яких, окрім інформації, належать також інформаційні системи (суб'єкти й інфраструктура) та інформаційні відносини. Отже, безпека інформації має розглядатися як частина більш масштабного цілого.

Відповідно, як науковці близького зарубіжжя, так і вітчизняні дослідники приділяють значну увагу питанням інформаційно-психологічної та державно-ідеологічної складової інформаційної безпеки, існування яких зумовлюється поділом інформаційної сфери на інформаційно-технічну та інформаційно-психологічну [137-140]. На підставі критерію функціональності вони пропонують також визнавати складовими інформаційної безпеки такі її аспекти: соціальсний; нормативно-правовий; економічний; фінансовий; військовий; екологічний; програмно-технічний та ін. [141, с. 74].

На думку Б.Кормича, інформаційна безпека має суб'єктно-об'єктний склад, відтак з точки зору критерію основного об'єкта складовими інформаційної безпеки є інформаційна безпека особи, інформаційна безпека суспільства та інформаційна безпека держави. Крім того, держава, людина та суспільство одночасно виступають і в якості суб'єктів інформаційної безпеки, своїми діями здійснюючи захист важливої для них інформації та інформаційних процесів. Зокрема, до сфери інформаційної безпеки держави віднесені конкретні дії щодо забезпечення безпечних умов перебігу існуючих інформаційних процесів та забезпечення

безпечного розвитку таких процесів у майбутньому, що охоплює регулювання питань захисту самої інформації, захисту інформаційної інфраструктури держави, захисту інформаційного ринку та створення безпечних умов розвитку інформаційних процесів [142, с. 28-32].

Підкреслюючи за результатами комплексного аналізу системність інформаційної безпеки, О.Тихомиров веде мову передусім про «структурні складові забезпечення інформаційної безпеки» та виокремлює їх за різними критеріями. Зокрема: за сферами суспільного життя (забезпечення інформаційної безпеки в економічній, політичній, військовій, науково-технологічній, екологічній, соціальній та інших сферах); за об'єктами національної безпеки (забезпечення інформаційної безпеки особи, суспільства та держави); за сучасними аспектами розуміння інформаційної безпеки (забезпечення інформаційно-психологічної безпеки, забезпечення інформаційної безпеки у сфері прав і свобод людини та забезпечення інформаційно-технічної, в тому числі кібернетичної, безпеки); за основними видами інформаційної діяльності (забезпечення законних можливостей створення, збирання, одержання та використання інформації, законного порядку поширення інформації, належного зберігання інформації, охорона та захист інформації, створення і розвиток інформаційних ресурсів тощо); за формами державного забезпечення інформаційної безпеки (забезпечення якісного інформування, процесів інформатизації; правова регламентація сфери інформаційних відносин; боротьба з правопорушеннями в інформаційній сфері); за напрямами пізнавального процесу в галузі забезпечення інформаційної безпеки (професійна освіта, наукові дослідження, інформаційно-просвітницька діяльність тощо); залежно від елементів змісту діяльності із забезпечення інформаційної безпеки (за об'єктами забезпечення інформаційної безпеки: розвиток і вдосконалення інформаційно-телекомунікаційної інфраструктури, недопущення доведення її до критичного рівня; забезпечення належного використання національних інформаційних

ресурсів (захист ресурсів від несанкціонованого втручання, їх інноваційне оновлення, впровадження новітніх технологій створення, оброблення та поширення інформації, формування відкритих інформаційних ресурсів і забезпечення доступу до них громадян); захист інформації (забезпечення конфіденційності, цілісності та доступності тощо); захист свідомості суб'єктів від деструктивного інформаційного впливу (створення сприятливого психологічного клімату в національному інформаційному просторі задля утвердження загальнолюдських та національних моральних цінностей); за суб'єктами забезпечення інформаційної безпеки: міжнародне забезпечення (міжнародне співробітництво в галузі забезпечення інформаційної безпеки, гарантування інформаційного суверенітету держави, сприяння задоволенню інформаційних потреб громадян за кордоном); державне забезпечення (діяльність державних організацій, спрямована на забезпечення інформаційної безпеки); недержавне забезпечення (діяльність громадських і недержавних комерційних організацій та окремих громадян, спрямована на сприяння державному забезпеченню інформаційної безпеки); за характером предмета діяльності із забезпечення інформаційної безпеки: протидія негативним інформаційним процесам і явищам; сприяння посиленню позитивних інформаційних процесів; сприяння трансформації нейтральних інформаційних процесів у позитивні; за складовими механізму протидії загрозам інформаційній безпеці: моніторинг інформаційної сфери; ранжування загроз; профілактика й попередження негативного впливу загроз; нейтралізація загроз; за характером здійснення державного впливу: безпосереднє створення необхідних умов життєдіяльності суб'єктів в інформаційній сфері; опосередкований вплив шляхом підвищення інформаційного потенціалу суб'єктів і сприяння їх самоорганізації; за засобами забезпечення інформаційної безпеки: правове забезпечення (правова регламентація відносин в інформаційній сфері; контрольно-наглядова діяльність, ліцензування, сертифікація, експертизи тощо);

техніко-технологічне забезпечення; залежно від особливостей забезпечення доступу до інформації (за правовим режимом доступу до інформації; за заходами із захисту секретної інформації тощо) [143, с. 67].

Звісно, поняття «інформаційна безпека» та «забезпечення інформаційної безпеки» не є тотожними і з точки зору функціонально-діяльнісного підходу співвідносяться як об'єкт діяльності – позитивна цінність – та власне діяльність, здійснювана за допомогою певних сил і засобів. Проте, ці дві категорії не можуть співіснувати одна без одної. Вони є взаємовиключними. Адже неможливо уявити «безпеку» без процесу її «забезпечення». Утім, наведена вище класифікація в аспекті визначення складових забезпечення інформаційної безпеки дозволяє дійти певних висновків і щодо складових інформаційної безпеки, котрі можуть бути виокремлені за допомогою аналогічних критеріїв. Водночас, критерій, скажімо, об'єкта національної безпеки дозволяє структурувати інформаційну безпеку радше за рівнями, ніж за складовими.

Поняття інформаційної безпеки тісно пов'язане з поняттям інформаційного суверенітету держави. Враховуючи, що система забезпечення національної безпеки будується «від інтересів держави», більшість функцій, у тому числі у сфері забезпечення інформаційної безпеки, здійснюється саме державою, що дозволяє досягти балансу інтересів в інформаційній сфері. Щодо суспільного виміру інформаційної безпеки, то так звана «недержавна система безпеки» є не лише суб'єктом власного забезпечення, який самостійно визначає мету, принципи та методи забезпечення безпеки відповідно до законодавства України в межах загальної системи, але й становить об'єкт забезпечення інформаційної безпеки з боку держави. Своєю чергою, безпека людини становить складову метасистеми національної безпеки, яка об'єднує безпеку особи, суспільства та держави в різних сферах, зокрема в інформаційній.

Узагальнення критеріїв сучасних аспектів розуміння інформаційної безпеки, основних видів інформаційної діяльності та змісту діяльності із

забезпечення інформаційної безпеки (за класифікацією О.Тихомирова) дає змогу визначити, що метою забезпечення інформаційної безпеки є: попередження неправомірних дій з інформаційними ресурсами та системами, в тому числі здійснення шкідливих інформаційних впливів; захист прав та забезпечення реалізації законних інтересів суб‘єктів інформаційної сфери; забезпечення належного стану ключових властивостей інформації.

Це, відповідно, дає підстави припустити, що інформаційна безпека формується такими трьома складовими:

1) безпека інформації;
2) безпека «від інформації» (безпека інформаційних систем, зокрема суб’єктів інформаційної сфери та соціальних зв’язків між ними, від інформаційних впливів вербального, технічного чи будь-якого іншого характеру);
3) належний порядок реалізації прав та інтересів суб’єктів інформаційної сфери.

Кожна із цих складових може проявлятися на різних рівнях залежно від:

- виду, приналежності, режиму доступу до інформації (для безпеки інформації);
- характеру, виду, способів розповсюдження дефектної інформації, суб’єктів, які поширюють та яким адресується дефектна інформація, характеру відповідних суспільних відносин (для безпеки від інформаційних впливів);
- суб’єктів інформаційної сфери з приводу реалізації ними «інформаційних» прав (для належного порядку реалізації прав та інтересів суб’єктів інформаційної сфери).

Стосовно безпеки інформації слід зазначити, що йдеться про необхідність забезпечення безпеки не лише інформації з обмеженим доступом, а й іншої, позаяк в умовах інформаційного суспільства

надається правова охорона інформації як об’єкту цивільних прав, і має бути відвернена загроза не лише несанкціонованого доступу до інформації (порушення конфіденційності), але й порушення її цілісності та достовірності, а в необхідних випадках – і доступності.

Не менш важливою, ніж безпека інформації, є так звана безпека «від інформації». Під нею слід розуміти безпеку інформаційних систем, у тому числі біологічних та соціальних, - суб’єктів інформаційної сфери, та соціальних зв’язків між ними (зокрема й тих, що утворюються при забезпеченні інших складових національної безпеки) від інформаційних впливів, що здатні викликати знищення або пошкодження, спотворення тих чи інших об’єктів (зокрема, нематеріального характеру), а також інформаційно-психологічну безпеку людини й суспільства. Забезпечення інформаційно-психологічної безпеки полягає в мінімізації негативних впливів на свідомість людини та суспільства, пов’язаних передусім із маніпулюванням свідомістю з різною метою, а також поширенням суспільно небезпечної інформації, зокрема, деструктивної ідеології (культу насильства та жорстокості, расизму, радикального націоналізму, порнографії тощо) [143, с. 70-71].

Належний порядок реалізації інформаційних прав та інтересів суб’єктів інформаційної сфери як складова інформаційної безпеки безпосередньо пов’язаний із двома іншими її складовими, оскільки йдеться, по-перше, про права та інтереси суб’єктів суспільних відносин, які належать до біологічних та соціальних інформаційних систем (тому що саме в такій своїй якості вони виступають в інформаційній сфері); по-друге, про забезпечення взаємної нешкідливості інформаційних впливів на суб’єктів інформаційної сфери; і по-третє, про права суб’єктів правовідносин як володільців інформації. Власне ж інформаційні впливи є процесами поширення інформації, зверненими до обмеженого або необмеженого кола інформаційних систем (в окремих випадках до цієї категорії можуть належати так звані «ентропійні інформаційні впливи»,

тобто утримання від передачі або поширення необхідної інформації).

При цьому безпека інформації становить конститутивне підґрунтя інформаційної безпеки, що, у свою чергу, зумовлюється конститутивним значенням інформації як елемента інформаційної сфери.

Що ж стосується кібернетичної безпеки, то її виокремлення зумовлене специфікою середовища, в якому функціонують інформаційні системи, здійснюється обіг інформації, реалізація прав та законних інтересів суб'єктів інформаційної сфери тощо. А отже кібернетичний аспект може бути притаманний усім складовим інформаційної безпеки, тож мова в даному разі має вестися не про самостійну складову, а про забезпечення інформаційної безпеки у кіберпросторі (зауважимо, що в Законі України «Про основні засади забезпечення кібербезпеки України», прийнятому 5 жовтня 2017 року, кібербезпека визначена як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі) [144-145].

Слід також зазначити, що комплексне функціональне визначення інформаційної безпеки як постійного процесу діяльності компетентних органів, спрямованої на попередження, протидію загрозам в інформаційній сфері, а також застосування активних заходів інформаційного впливу та сукупності умов такої діяльності, які реалізуються й здатні контролюватися тривалий час, дозволяє виділити пасивну (протидія інформаційним загрозам) та активну складові (створення інформаційних загроз) інформаційної безпеки.

Підбиваючи проміжні підсумки, зазначимо, що вся інформаційна сфера в теперішній час включає дві головні складові, які, своєю чергою, визначають **основні складові інформаційної безпеки держави:**

1) *технічна* (штучно створене людиною середовище техніки і технологій);

2) *психологічна* (природній світ з його емоціями).

Принципові відмінності між названими складовими інформаційної безпеки та зміст інформаційно-психологічної складової схематично зображено на рис. 2.1.

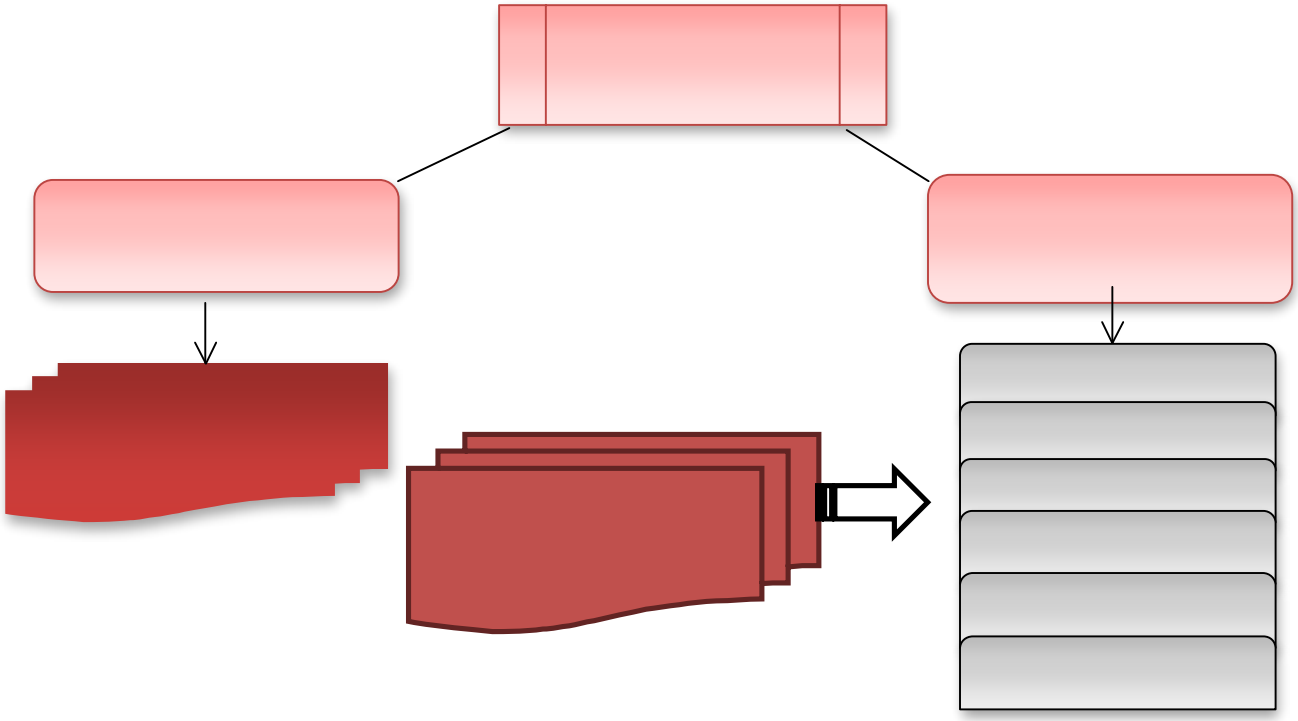

Рис. 2.1. Складові інформаційної безпеки

Джерело: розроблено автором.

Таким чином, предметом правового забезпечення інформаційної безпеки держави виступають суспільні відносини, які включають дві сфери: технічну (комп'ютерні системи, телекомунікаційні мережі) та інформаційно-психологічну (суспільна думка, національні цінності, почуття й емоції суспільства та окремих індивідів).

Предметом нашої уваги першочергово виступатиме інформаційно-психологічна складова інформаційної безпеки України, під якою розуміємо захищеність передусім психічного здоров'я людини і суспільств як головної національної цінності, а також національних інформаційних

ресурсів (насамперед – державних секретів та комерційної таємниці, втрата чи розголошення яких може завдати суттєвої шкоди національній безпеці держави та її національним інтересам). Підкреслимо, що основним об'єктом захисту в цьому разі виступає суспільна свідомість населення України. Адже відомо, що інформаційно-психологічний вплив шляхом маніпулювання суспільною свідомістю здатен викликати значні дисфункціональні процеси у суспільстві, наслідком яких можуть стати соціальні потрясіння, соціальне напруження, розбалансованість важелів стримувань і противаг гілок влади та інше.

Інформаційну безпеку України необхідно виділити як одну із найважливіших складових системи національної безпеки. Вона є окремим елементом, але водночас тісно переплітається з усіма видами безпеки, і від рівня її забезпечення залежить успішне функціонування всіх решти. Ми погоджуємося з О.Корейком, що сьогодні інформаційний складник не існує поза межами загальної національної безпеки, так само як і національна безпека не буде всеосяжною без інформаційної своєї складової [146, с. 9]. Саме нині, в епоху бурхливого зростання обсягів застосування інформаційних технологій у всіх сферах життєдіяльності, успішне вирішення проблем у галузі правового забезпечення інформаційної безпеки держави передбачає більш ефективну діяльність у процесі забезпечення національної безпеки. Зупиняючись на найважливіших питаннях з погляду безпечного розвитку, виділимо роль інформаційної безпеки у процесі забезпечення кожного з безпекових видів у системі інформаційної безпеки.

Пріоритетами *духовної безпеки* держави виступає мова як головний ідентифікатор нації, національна культура та спадщина народу, наука та освіта, мистецтво, а також засоби масової інформації - провідне джерело інформування суспільства. Найдієвішими з-поміж методів захисту духовної сфери є методи інформаційно-психологічного протиборства та пропаганди.

Основними засобами впливу в контексті духовної безпеки виступають методи маніпулювання людською свідомістю з метою латентного управління й деморалізації особистості, а також дезінформація. Стратегічною метою таких впливів є порушення та спотворення поглядів людей на навколишній світ і самих себе шляхом культивування уявних цінностей, насадження деструктивних пріоритетів, завдань і цілей перед суспільством та окремим індивідом.

Військова безпека держави сьогодні забезпечується завдяки упровадженню інформаційних технологій. Системи засобів озброєння і системи управління мають високий ступінь комп'ютеризації, тому рівень їх уразливості від впливу інформаційної зброї підвищується як у мирний, так і у воєнний час. Події на сході нашої держави яскраво підтверджують цю тезу.

Наступною ланкою інформаційної безпеки в системі національної безпеки держави є *економічна безпека*. Новий вид інформаційної економіки є результатом розвитку можливостей інформаційних технологій, зростання потреб населення в інформаційних послугах і формування глобальних інформаційно-телекомунікаційних систем. Роль інформаційної економіки потужна, оскільки впливає на всі сфери суспільного розвитку [147, с. 370]. Сьогодні фахівці слушно зазначають, що інформаційна безпека національної економіки є невід’ємним атрибутом суверенності, цілісності та незалежності будь-якої держави, а побудова ефективної безпекової інформаційної системи уможливлює сталий інноваційний, соціально-економічний та політичний розвиток держави [148, с. 45].

Особливого значення набуває розвиток інформаційної економіки в геополітиці держав, тому стає стратегічно важливим плином в соціально-економічному розвитку кожної країни, що потребує першочергової уваги на всіх рівнях та етапах державотворення. Відповідно актуалізується потреба правового врегулювання нових суспільних відносин, як от:

електронна комерція, Інтернет-розрахунки, криптовалюта тощо.

У свою чергу, формування глобального інформаційного простору, базисом якого є комп'ютерна мережа, ставить перед державою низку серйозних питань щодо забезпечення економічної безпеки. Вказані проблеми стосуються методів і технологій захисту інформаційних ресурсів, що концентруються в інформаційних мережах. Ця ситуація пов'язана з формуванням інформаційної політики держави стосовно забезпечення захищеності життєво важливих інтересів країни у сфері інформаційної безпеки.

Вельми вагомою складовою виступає *соціальна безпека* суспільства. Ця складова інформаційної безпеки передбачає захист у соціальній сфері інтересів народу і країни, формування громадських структур і соціальних відносин, системи життєзабезпечення, способу життя, що відповідає вимогам прогресу сучасного суспільства та гідного рівня життя людей.

Можливості сьогоднішніх інформаційних технологій значно підвищили ефективність впливу інформаційних засобів на психіку і свідомість людей, відкрили нові методи і прийомами прихованого маніпулювання. Людина - головна мета інформаційного механізму управління. Загроза дегуманізації набула настільки реальних обрисів, що у структурі сучасних цінностей найголовнішим благом стало виступати саме життя людини. Державно-правова захищеність людини від фізичних посягань зазвичай вища, ніж від зазіхань на психіку людей. Правова сфера часто відстає від процесів суспільного розвитку, а в духовній сфері це відставання в рівні захищеності стало просто катастрофічним. Відтак, першорядного значення набуває правова захищеність свідомості людей.

Спотворені методи використання інформаційних технологій призвели до деформаційних змін соціальної сфери. Це відбилося передовсім у спонуканні соціального розшарування суспільства за допомогою розподілу інформаційних послуг і благ, диссолюції інститутів, спрямованих на розвиток особистості, підбурюванні до розколу на підставі

етнічної, національної, ідеологічної, релігійної, мовної ознак. У соціальній сфері українського суспільства наслідки зазначеної інформаційної агресії суттєво проявляються вже тривалий час.

У контексті даного дискурсу слід окремо звернути увагу на засоби масової інформації, які багато в чому є чи не найважливішим елементом інформаційного суспільства. У теперішній час засоби масової інформації по суті монополізували процес задоволення інформаційних потреб населення у світі, країні, регіоні, на підставі чого спроможні нав'язувати ідеологічні погляди й настанови. Тому критично назріла нагальна потреба порушувати питання про ступінь довіри до інформації, яка транслюється ЗМІ, та її якість, позаяк засоби масової інформації здатні сьогодні виступити в ролі надпотужної сили, спрямованої як на стабілізацію суспільства, так і на спричинення соціального вибуху. Не зайвим буде додати, що відповідні заходи стосовно ЗМІ мають здійснюватися виключно у правовому полі. Таким чином, без належного правового забезпечення інформаційної безпеки неможливо досягти бажаного рівня соціальної безпеки.

Глобальних масштабів набула нині й проблема забезпечення *екологічної безпеки*. Новітні технології несуть непередбачувані й досі не знані загрози здоров'ю населення, навколишньому середовищу. Це, наприклад, побічні ефекти дії лікарських препаратів, впровадження генетично модифікованих продуктів, застосування нових видів зброї, техногенні катастрофи, такі як Чорнобиль, Бхопал, Фукусіма, забруднення і знищення природи, в тому числі й Світового океану, руйнування озонового шару Землі тощо.

Розв’язання значного числа зазначених проблем залежить від екологічного моніторингу стану навколишнього середовища, моделювання природних процесів з розрахунком на зростання антропогенних навантажень і техногенних впливів. На наш погляд, ефективні результати зазначених дій більш очікувані за умови застосування новітніх

інформаційних технологій, у чому і проявляється головна сутність інформаційної безпеки.

Тісний зв'язок екологічної та інформаційної безпеки є очевидним: країна, що володіє значним інформаційним потенціалом, спроможна досягти економічного процвітання та успішного вирішення екологічних завдань.

З усього вищесказаного доходимо висновку, що унікальна специфіка інформаційної безпеки дозволяє їй охопити увесь безпековий спектр: економічну, соціально-політичну, військову та екологічну безпеку. Цим і зумовлюється її пріоритетне значення у процесі забезпечення національної безпеки держави. Як було показано, від забезпечення інформаційної безпеки на сучасному етапі розвитку суспільства залежать умови забезпечення основних видів безпеки людини, суспільства, держави, нації.

Більше того, сьогодні активно дискутується питання про так звану екологію інформації. Показовою з цього приводу є праця Фелікса Сталдера, яка так і називається – «Екологія інформації» [149]. На підставі свого дослідження вчений резюмує, що медіа створюють інтегроване середовище (environment), основу якого становлять потоки інформації. Все частіше в діяльності людини це середовище стає головним. Екологія інформації прагне зрозуміти його властивості, щоб використовувати потенціал цього середовища, уникати небезпек і позитивно впливати на його розвиток.

У цьому контексті ми підтримуємо Р. Проданюка, який зазначає, що інформаційна безпека може розглядатись як одна із соціальних інституцій контролю за підтриманням інформаційної рівноваги, функція якої полягає в підтриманні екологічності інформаційного простору [150, с. 87].

Розвиток інформаційних технологій на початку 21 століття визначив загальні тенденції поступу людства та окреслив характерні проблеми даної епохи, серед яких:

1. Формування нового планетарного простору, в основі якого інформаційні й телекомунікаційні технології забезпечують ефективну взаємодію між людьми. Основними характеристиками таких процесів є безмежність, доступність, гіперпов'язаність, «стирання» територіальних кордонів, рух у масштабі часу, розвиток Інтернету речей тощо. Як наслідок, відбувається становлення нового інформаційного суспільства.

2. Усі без винятку суспільні процеси (політичні, соціальні, економічні) залежать від використання інформаційних технологій, оскільки вони мають вирішальне значення у формуванні існуючої реальності й мають неабиякий вплив на її розвиток.

3. Недостатня увага з боку як міжнародних інституцій, так і національних урядів, до проблем правового забезпечення інформаційної безпеки стали причиною виникнення та надшвидкого поширення понять «інформаційна зброя», «інформаційний тероризм» та «інформаційна війна», а також деструктивних впливів від позначуваних цими термінами явищ. Значне применшення завдань інформаційної безпеки стало причиною непрогнозованих економічних, соціальних, екологічних, політичних та інших потрясінь у системі безпеки. Унаслідок цього вирішення питань інформаційної безпеки із значним запізненням вийшло на перший план в усіх сферах суспільного життя і державної діяльності, як на національному, так і на міжнародному рівнях.

Усе це дає змогу виокремити в досліджуваній нами системі *глобальну безпеку*, адже на рівні світової спільноти інформаційна безпека набуває статусу всеосяжної проблеми сучасності. У даній іпостасі глобальна безпека характеризується такими ознаками:

- вона стосується усіх без винятку країн світу;

- є об'єктивною умовою й основним механізмом майбутніх напрямів всесвітнього розвитку;

- в умовах формування світового інформаційного суспільства в якості першої стадії ноосфери інформаційна безпека стає актуальним

завданням;

- незадовільне забезпечення вимог інформаційної безпеки породжує загрози інформаційного тероризму, інформаційної війни тощо.

Відтак, можемо стверджувати, що для підвищення рівня забезпечення інформаційної безпеки, запобігання негативним інформаційно-психологічним впливам на суспільству й людину потрібні зусилля усього міжнародного співтовариства.

Отже, при функціонуванні світового інформаційного простору інформаційна безпека повною мірою може бути забезпечена тільки зусиллями всіх країн, тому виникає потреба у формуванні загальносвітової інформаційної безпеки. Зрозуміло, що такі процеси є тривалими і потребують злагодженої роботи та конструктивного діалогу. Тому доцільно такі перемови розпочинати на рівні субінститутів, зокрема, проекту Міжмор'я (Intermarium) та подібних. У результаті система глобальної інформаційної безпеки стане важливим чинником переходу до сталого розвитку у глобальному вимірі.

У рамках таких міжнародних проектів розвитку інформаційної безпеки глобального масштабу мають вирішуватися такі питання:

- забезпечення стану захисту глобального інформаційного середовища від загроз і небезпек реального й потенційного характеру;

- розвиток інформаційного простору в безпечному для людини, суспільства та біосфери напрямку;

- розвиток інформаційної культури.

На шляху реалізації зазначеної стратегії важливо не забувати, що світовий інформаційний простір не має географічних і державних кордонів, а тому його захист і зміцнення залежать одночасно від всього міжнародного співтовариства, рівнозначно як його вразливість і шкода від нього відбивається на всіх країнах. З огляду на це слід розглянути питання узгодження стандартів і національних законів, а також завдання співпраці з їх реалізації, укладання міждержавних угод щодо функціонування

міжнародного інформаційного простору в соціальних, політичних, культурних, юридичних площинах.

2.3. Правові засади організації системи інформаційної безпеки України

У період бурхливого зростання застосування інформаційно-комунікаційних технологій у всіх сферах життєдіяльності, успішне вирішення проблем, пов'язаних з інформаційною безпекою, безпосередньо стосується й процесу забезпечення національної безпеки. Натомість, від успішного вирішення питань даної сфери залежить забезпечення глобальної загальносвітової безпеки. Як бачимо визначальну роль інформаційної безпеки, яка сьогодні стає системо формуючим чинником глобальної безпеки як в Україні так і у світі.

Аналіз формування нової реальності, усвідомлення її в цілісності, без відриву від інформаційних технологій, спонукає до пошуку шляхів безпечного розвитку, подолання негативних ефектів від застосування сучасних технологій, перегляду ціннісних орієнтирів. Подальше становлення соціуму, яке ґрунтується на розвитку інформаційно-комунікаційних технологій, та забезпечення динамічної рівноваги технологічної еволюції вимагає безпечних умов інформаційної сфери.

Усі автори єдині в думці, що світ вступає в епоху грандіозних соціальних змін, технологічних і культурних перетворень, їхні прогностичні позиції досить близькі. Потенціал техніки, незмінно нарощуваний, робить вирішальний вплив на всі сфери життя людського суспільства. Зростає продуктивність праці, змінюється в десятки, сотні разів його зміст. Вони змінюють лад культури і впливають на формування всієї цивілізації. Людський інтелект, його міць багаторазово збільшуються

завдяки революції інформаційно-комунікаційних технологій. Соціальна структура суспільства опиняється під надмірним впливом технологічних нововведень. Ро́боти вже витіснили людей із багатьох галузей. Суть у тому, що відбуваються трансформації, бо народжується новий цивілізаційний устрій, в якому сфера праці, наука та освіта, державне управління, культура будуть носити принципово інший характер.

На відміну від індустріального суспільства, яке в основі має машинну технологію, специфіка постіндустріального суспільства криється в використанні інформаційно-інтелектуальної технології.

На сьогодні в Україні закладена основа правового регулювання забезпечення національної безпеки, й інформаційної безпеки зокрема, завдяки чому одержали своє законодавче закріплення основні поняття, що стосуються національної безпеки, а також правове обґрунтування системи її забезпечення. Водночас, основні нормативно-правові акти у сфері інформаційної безпеки потребують доопрацювання, зокрема щодо визначення й законодавчого закріплення поняття та змісту категорії «система інформаційної безпеки». Існує також необхідність розробки теоретичних і правових засад забезпечення інформаційної безпеки України.

Мусимо при цьому констатувати, що в сучасній науковій літературі поки не склався єдиний термінологічний ряд теорії забезпечення інформаційної безпеки. На практиці це призводить не лише до активізації наукової дискусії, але й до неадекватного розуміння змісту тих чи інших положень, висновків і рекомендацій прикладного характеру, що стосуються сфери інформаційної безпеки України. Зокрема, наразі немає усталеного підходу до визначення системи інформаційної безпеки як на доктринальному, так і на нормативному рівнях.

Відповідно до ст. 17 Конституції України захист інформаційної безпеки, нарівні із захистом суверенітету та територіальної цілісності України, є найважливішою функцією держави та справою всього

українського народу [23]. Тож інформаційна безпека, безперечно, є однією з найважливіших складових національної безпеки України. Оскільки інформаційна сфера має своїм змістом знання про інші сфери життєдіяльності суспільства, вона одночасно існує як самостійно, так і у взаємозв'язку з ними, адже здійснює їх «інформаційне обслуговування». Це зумовлює виняткове значення інформаційної сфери та загроз, спрямованих на неї, позаяк, слушно зазначає Г.Сащук, «…під впливом інформаційних атак може цілеспрямовано змінюватися світогляд та мораль як окремих осіб, так і суспільства в цілому, нав'язуються чужі інтереси, мотиви, спосіб життя» [151]. А на думку В. Ліпкана, «національні інтереси, загрози їм, управління цими загрозами в усіх галузях національної безпеки знаходять свій вираз, реалізуються через інформацію та інформаційну сферу» [32, с. 41]. Відтак, забезпечення інформаційної безпеки є запорукою забезпечення інших складових національної безпеки, тому що всі типи взаємин між суб'єктами інформаційного суспільства ґрунтуються на споживанні й обміні інформацією, а когнітивний простір багато в чому не лише обслуговує й супроводжує, а й підміняє реальний.

Досліджуючи питання системи інформаційної безпеки, слід передусім визначитись із тим, що саме ми розуміємо під інформаційною безпекою, адже наразі з цього приводу наука досі не дійшла єдності. У даній частині праці розглянемо теоретичні підходи до розуміння досліджуваного нами явища, які можуть вплинути на формування системи інформаційної безпеки держави. Зокрема, О.Данільян, О.Дзьобань та М.Панов визначають інформаційну безпеку як безпеку об'єкта від інформаційних загроз або негативних впливів, пов'язаних з інформацією, та нерозголошення даних про той чи інший об'єкт, що є державною таємницею [152].

В.Гурковський уважає, що інформаційна безпека - це суспільні відносини, пов'язані із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в

інформаційному просторі, що є необхідною умовою збереження та примноження духовних і матеріальних цінностей державоутворювальної нації, її існування, самозбереження і прогресивного розвитку України як суверенної держави, що залежить від цілеспрямованої інформаційної політики гарантій, охорони, оборони, захисту її національних інтересів [153, с. 75].

Н.Нижник, Г.Ситник та В.Білоус під інформаційною безпекою розуміють стан правових норм і відповідних їм інститутів безпеки, які гарантують постійну наявність даних для прийняття стратегічних рішень та захист інформаційних ресурсів країни [154].

В.Ярочкін та Т.Шевцова зазначають, що інформаційна безпека - це проведення правових, організаційних та інженерно-технічних заходів при формуванні та використанні інформаційних технологій, інфраструктури та інформаційних ресурсів, захисті інформації високого значення і прав суб'єктів, що беруть участь в інформаційній діяльності [155, с. 41].

На думку Р.Калюжного, інформаційна безпека – це вид суспільних інформаційних правовідносин стосовно створення, підтримки, охорони та захисту бажаних для людини, суспільства й держави безпечних умов життєдіяльності, спеціальних правовідносин, які пов'язані зі створенням, зберіганням, поширенням і використанням інформації [156, с. 20].

К.Бєляков також пропонує під інформаційною безпекою розуміти не лише технологічну, а і правову захищеність інформаційної сфери суспільства, що забезпечує її формування та розвиток в інтересах громадян, організацій та держави в цілому [157, с. 254].

Так само Б.Кормич уважає, що інформаційна безпека - це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування та розвитку людини, всього суспільства й держави [43].

В.Ліпкан, Л.Харченко та О.Логінов розглядають інформаційну

безпеку як процес управління загрозами та небезпеками державними й недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України [40, с. 75]. В.Шульга теж схиляється до того, що інформаційну безпеку слід розглядати через властивість управління загрозами й небезпеками [158].

А.Лукашов визначає інформаційну безпеку як функціонування системи засобів, що забезпечують захищеність інформаційних систем, котрі являють собою впорядковану сукупність інформаційних ресурсів, інформаційних технологій та комплексу програмно-технічних засобів, якими здійснюються інформаційні процеси в людино-машинному або автоматичному режимі [159].

Ю.Фісун характеризує інформаційну безпеку як «стан захищеності інформаційного середовища, який відповідає інтересам держави, що забезпечує формування, використання і можливості розвитку незалежно від впливу внутрішніх і зовнішніх інформаційний загроз» [44, с. 90].

За визначенням І.Панаріна, інформаційна безпека – це стан інформаційного середовища суспільства й політичної еліти, що забезпечує її формування і розвиток в інтересах керівництва країни, громадян і суспільства [160, с. 128].

І.Бондар пропонує розглядати національну безпеку України в інформаційній сфері, тобто інформаційну безпеку, як інтегральну цілісність чотирьох складових – персональної, публічної (суспільної), комерційної (корпоративної) й державної безпеки [59, с. 73].

І.Громико інформаційною безпекою називає захищеність державних інтересів, за якої забезпечуються запобігання, виявлення й нейтралізація внутрішніх та зовнішніх інформаційних загроз, збереження інформаційного суверенітету держави й безпечний розвиток міжнародного інформаційного співробітництва [161, с. 134].

На думку О.Баранова, під інформаційною безпекою слід розуміти такий стан захищеності життєво важливих інтересів особистості,

суспільства й держави, за якого мінімізується заподіяння шкоди через неповноту, невчасність і недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації [162, с. 57]. В.Остроухов також визначає інформаційну безпеку як стан захищеності об'єкта (особистості, суспільства, держави, інформаційно-технічної інфраструктури), за якого досягається його нормальне функціонування незалежно від внутрішніх і зовнішніх інформаційних впливів [163, с. 136].

Наведені вище визначення, які можна назвати традиційними, в цілому відображають погляди багатьох інших дослідників та співвідносяться із законодавчим визначенням інформаційної безпеки, наведеним у Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки»: інформаційна безпека – це «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через:

- неповноту, невчасність та невірогідність інформації, що використовується;
- негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій;
- несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» [164].

Як бачимо, законодавче визначення не відбиває співвідношення національної та інформаційної безпеки, а також не дає уявлення про систему інформаційної безпеки, так само, як і визначення, котрі торкаються окремих аспектів інформаційної безпеки, зокрема інформаційної безпеки телекомунікаційних мереж [133] або кібербезпеки [165].

На доктринальному рівні система інформаційної безпеки вибудовується з використанням доволі широкого спектру критеріїв, що

зумовлює диференціацію підходів до змісту поняття «система інформаційної безпеки».

У зарубіжних наукових джерелах під системою інформаційної безпеки зазвичай розуміють систему безпеки інформації у складі таких структурних елементів, як цілісність, доступність та конфіденційність інформації [166-168].

При цьому цілісністю інформації вважається її властивість не бути модифікованою неавторизованим користувачем і/або процесом, тобто, зберігатись у стані, визначеному її створювачем та законним володільцем. Це в тому числі стосується й достовірності інформації як її відповідності дійсності в аспекті адекватності відображення. Конфіденційність – це властивість інформації бути недоступною користувачам, які не мають на це права. Вона пов’язана з розмежуванням інформації за режимом доступу. Доступність інформації полягає в тому, що уповноважений користувач може використовувати її відповідно до правил, установлених політикою безпеки, не очікуючи понад заданий проміжок часу. Тобто, це – властивість інформації перебувати в необхідному користувачеві вигляді та місці тоді, коли вона йому потрібна [169, с. 190]. Утім, зазначені характеристики не дають уявлення про систему інформаційної безпеки як складову національної безпеки.

Натомість науковці пострадянського простору, зокрема й вітчизняні вчені, приділяють значну увагу питанням інформаційно-психологічної та державно-ідеологічної складової інформаційної безпеки, існування яких зумовлюється поділом інформаційної сфери на інформаційно-технічну та інформаційно-психологічну [170, с. 62; 171; 172; 173]. На підставі критерію функціональності вони також пропонують визнавати складовими системи інформаційної безпеки її аспекти: соціальний, нормативно-правовий, економічний, фінансовий, військовий, екологічний, програмно-технічний та інші [174, с. 74].

За твердженням Б. Кормича, інформаційна безпека має суб’єкт-

об’єктний склад. Відтак, виходячи з критерію основного об’єкта, система інформаційної безпеки складається з інформаційної безпеки особи, інформаційної безпеки суспільства та інформаційної безпеки держави. Крім того, вказані об’єкти інформаційної безпеки виступають одночасно і як її суб’єкти, своїми діями забезпечуючи захист важливої для них інформації та інформаційних процесів [142, с. 29].

О.Довгань розглядає інформаційні структури як компоненти інформаційної безпеки, тобто, як елементи системи інформаційної безпеки [175, с. 119] та вважає її об’єктом інформаційного суверенітету [176, с. 111]. Систему інформаційної безпеки характеризують також такі поняття, як інформаційний простір, інформаційні ресурси, інформаційна інфраструктура та інформаційні технології [177, с. 84].

На відмінності між системою інформаційної безпеки та системою забезпечення інформаційної безпеки можуть бути екстрапольовані відповідні закономірності, виявлені щодо системи національної безпеки та системи забезпечення національної безпеки [178, с. 5-8]. Так, основними елементами системи забезпечення інформаційної безпеки є її суб‘єкти й об‘єкти, а також прямі та зворотні зв'язки між ними. Основними об‘єктами системи забезпечення інформаційної безпеки як складової національної безпеки є національні цінності, національні цілі та національні інтереси. Розглядаючи ці чинники через призму їх носіїв, можна так класифікувати об‘єкти системи забезпечення інформаційної безпеки:

- людина і громадянин (життя, здоров‘я, культура, традиції тощо).
- суспільство (розвиток демократії, збереження культури і духовно-історичної спадщини, збереження і розвиток інформаційних ресурсів, досягнення й розвиток суспільної злагоди, політична стабільність, віротерпимість тощо);
- держава (конституційний лад, суверенітет і територіальна цілісність України, політична, економічна та соціальна стабільність,

законність і правопорядок, розвиток рівноправного взаємовигідного міжнародного співробітництва тощо).

Суб'єктами системи забезпечення інформаційної безпеки виступають держава (у тому числі її інститути, службові особи), суспільство (соціальні верстви та групи, громадські організації), а також окремі громадяни.

В.Ярочкін фактично ототожнює систему забезпечення інформаційної безпеки та систему інформаційної безпеки, адже пропонує під першою розуміти організовану сукупність спеціальних органів, служб, засобів, методів і заходів, що забезпечують захист життєво важливих інтересів особи, суспільства й держави від внутрішніх і зовнішніх загроз. Компонентами концептуальної моделі інформаційної безпеки (на прикладі безпеки інформації) за такого підходу визначаються:

- об'єкти загроз;
- загрози;
- джерела загроз;
- цілі загроз;
- джерела інформації;
- способи неправомірного заволодіння конфіденційною інформацією (способи доступу);
- напрямки захисту інформації;
- способи захисту інформації;
- засоби захисту інформації [179, с. 40].

Натомість О.Довгань пропонує модель системи забезпечення інформаційної безпеки, яка утворюється об'єктами інформаційної безпеки та суб'єктами інформаційної безпеки відповідно. При цьому до об'єктів інформаційної безпеки належать:

- конституційні права і свободи людини і громадянина, фізичне та психологічне здоров'я населення, захищеність людини від деструктивних та маніпулятивних інформаційних впливів;

- інформаційне забезпечення, гарантії інформаційних прав та права на розвиток населення всіх регіонів України;
- інформаційний суверенітет, безпека національного сегмента глобального інформаційного простору, інформаційної інфраструктури, захищеність, цілісність, доступність та безпечність інформаційних ресурсів, продукції та послуг.

До суб'єктів забезпечення інформаційної безпеки у такій системі віднесені:

- Президент України, Верховна Рада України, Кабінет Міністрів України;
- Рада національної безпеки і оборони України, Національний банк України;
- Міністерство інформаційної політики України, Державний комітет телебачення і радіомовлення України, Національна рада України з питань телебачення і радіомовлення;
- Державна служба спеціального зв'язку і технічного захисту інформації України, Національна комісія України, що здійснює державне регулювання з питань зв'язку та інформатизації;
- Служба безпеки України, розвідувальні органи України, Державна прикордонна служба України, Збройні сили України та інші військові формування, утворені відповідно зо законів України;
- центральні органи виконавчої влади, місцеві органи державної влади та органи місцевого самоврядування, судові органи, прокуратура України та інші органи охорони правопорядку, віднесені законодавством до суб'єктів забезпечення національної безпеки України;
- засоби масової інформації, підприємства, заклади, установи та організації різних форм власності, що здійснюють інформаційну діяльність, наукові установи та вищі навчальні

заклади України інформаційного профілю, інститути громадянського суспільства, громадяни України та інші особи (за згодою) [180, с. 13].

На думку В.Пилипчука, до основних суб'єктів системи забезпечення інформаційної безпеки, які мають забезпечувати або брати участь у розробці та реалізації державної інформаційної політики, слід віднести такі:

Міністерство інформаційної політики України;

Міністерство юстиції України;

Державний комітет телебачення і радіомовлення України;

Національну раду України з питань телебачення і радіомовлення;

Державну службу спеціального зв'язку і захисту інформації України;

Національну комісію, що здійснює державне регулювання у сфері зв'язку та інформатизації;

інші державні й недержавні органи, заклади, установи, підприємства та організації.

Найбільш актуальними проблемами інформаційної безпеки дослідник вважає, зокрема: ефективність державної інформаційної політики та політики національної безпеки в інформаційній сфері; забезпечення кібербезпеки; захист прав, свобод і безпеки людини і громадянина в інформаційній сфері [181, с. 25-26], що дозволяє скласти певне уявлення про систему інформаційної безпеки.

О.Баранов наголошує на необхідності забезпечення інформаційної безпеки у трьох її складових:

1) забезпечення запобігання завдання шкоди через неповноту, невчасність та невірогідність інформації;
2) забезпечення запобігання завдання шкоди через негативний інформаційний вплив;

3) забезпечення запобігання завдання шкоди через негативні наслідки функціонування інформаційних технологій [108, с. 33].

Система інформаційної безпеки, таким чином, утворюється безпекою інформації, безпекою від негативних інформаційних впливів, безпекою інформаційних технологій. Утім, гуманітарна складова інформаційної безпеки містить у собі величезну сукупність проблем, пов'язаних з дотриманням конституційних прав і свобод громадян у сфері духовного розвитку й інформаційної діяльності. Тож безпеку інформаційної сфери не можна сприймати суто як захист телекомунікаційних мереж або мереж зв'язку, засобів масової інформації від проникнення небажаної або шкідливої інформації. Так, необхідність дослідження загроз інформаційній безпеці людини в контексті її інформаційних прав та свобод підкреслює О.Золотар, наголошуючи, що інформаційна безпека людини передбачає, зокрема, реалізацію життєво важливих інтересів людини та гармонійний розвиток в умовах інформаційного суспільства незалежно від наявності інформаційних загроз [182, с. 77].

Отже, позаяк метою забезпечення інформаційної безпеки є передусім попередження шкідливих інформаційних впливів та неправомірних дій щодо інформаційних ресурсів та інформаційних систем (біологічних, соціальних та технічних), захист прав та забезпечення реалізації інтересів суб'єктів інформаційної сфери, а також забезпечення захищеності істотних властивостей інформації, нами обґрунтовано, що система інформаційної безпеки складається з безпеки інформації, безпеки від інформаційних впливів, а також захисту інформаційних прав та належного порядку реалізації інтересів суб'єктів інформаційної сфери [183, с. 155].

При цьому безпека інформації як захищеність її основних властивостей має забезпечуватися не лише щодо інформації з обмеженим доступом, але і стосовно іншої інформації, оскільки належить відвертати загрози порушення не лише конфіденційності інформації, а і її цілісності,

достовірності, а також доступності.

Під безпекою від інформаційних впливів слід розуміти безпеку інформаційних систем та зв'язків між ними (зокрема й інформаційно-психологічну безпеку людини та суспільства) від інформаційних впливів, що здатні спричинити шкоду. Забезпечення інформаційно-психологічної безпеки полягає в мінімізації негативних впливів на свідомість людини та суспільства, пов'язаних передусім із маніпулюванням свідомістю з різною метою та поширенням суспільно небезпечної інформації, в тому числі деструктивної ідеології (культу насильства та жорстокості, расизму, радикального націоналізму, порнографії тощо) [184, с. 71]. Захист інформаційних прав та забезпечення реалізації інтересів суб'єктів інформаційної сфери як підсистема інформаційної безпеки пов'язані з двома іншими її складовими, бо йдеться насамперед про потребу у безпечному інформаційному середовищі та цивільні права на інформацію.

Що стосується інформаційної безпеки як інформаційного виміру національної безпеки, то мається на увазі не стан окремих структур, сторін або відносин нації, а її здатність ефективно функціонувати, незважаючи на негативні чинникам й усупереч їм не поступатися своїми інтересами під тиском зовнішніх, внутрішніх або комплексних загроз. Таким чином, категорія «інформаційна безпека» на національному рівні має стосуватися країни, держави, що розуміємо як органічну єдність території, населення та влади, і тлумачитися на холістичних засадах, виходячи з якісної своєрідності цілого щодо його частин. Ця своєрідність полягає в тому, що інформаційна безпека країни передбачає й означає інформаційну безпеку всіх її структур і утворень, але допускає можливе ослаблення її щодо деяких з них. Водночас, зміцнення інформаційної безпеки окремих об'єктів, сегментів або сфер, узятих окремо, важливе для інформаційної безпеки як складової національної безпеки (її інформаційного виміру), але не створює її.

Отже, інформаційна безпека виступає як стан і умови

життєдіяльності соціуму, які забезпечують сприятливе середовище для розвитку особистості, суспільства й держави, а так само й інших об’єктів. Натомість інформаційна безпека кожного з цих об’єктів окремо виступає не як її частини, а як її мета й результат. У широкому сенсі інформаційна безпека має включати такі проблеми, як: протистояння культурній експансії з боку країн з розвиненою аудіовізуальною промисловістю; збереження національної та мовної самобутності; нейтралізація впливу недоброякісної, недостовірної, хибної інформації (дезінформації) на реалізацію національних інтересів. Слід звернути увагу й на те, що «безпеки взагалі» немає, адже атрибутом існування об’єкта будь-якої природи є наявність загроз. Відтак, модель системи інформаційної безпеки передбачає з’ясування: кому, що, чим і як загрожує, а також можливі механізми та способи протидії загрозливим чинникам.

В.Пилипчук та О.Дзьобань до основних видів загроз інформаційній безпеці відносять такі:

- витіснення вітчизняних інформаційних агентств, засобів масової інформації із внутрішнього інформаційного ринку та посилення залежності духовної, економічної та політичної сфер громадського життя України від закордонних інформаційних структур;
- маніпулювання інформацією (дезінформація, приховування чи перекручування інформації);
- інформаційний вплив іноземних політичних, економічних, військових та інформаційних структур на розробку й реалізацію зовнішньої політики держави;
- поширення за кордоном дезінформації про зовнішню політику України;
- порушення прав громадян і юридичних осіб в інформаційній сфері в Україні й за кордоном;

- спроби несанкціонованого доступу до інформації та впливу на інформаційні ресурси, інформаційну інфраструктуру органів державної влади, котрі реалізують державну зовнішню політику, українських представництв і організацій за кордоном, представництв України при міжнародних організаціях [185, с. 47-48].

О.Дзьобань та О.Соснін обґрунтовано наголошують на необхідності постійного контролю стану безпеки в інформаційній сфері, ранжування загроз за ступенем впливу на національні інтереси, раціонального перерозподілу сил і засобів для нейтралізації загроз [186, с. 33].

Слід також враховувати, що зміст інформаційної безпеки не можна зводити тільки до захищеності - він значно ширший. Забезпечення безпеки передбачає не тільки збереження певного існуючого стану, а й створення можливостей для виходу на новий, якісно більш високий рівень розвитку. Відповідно, безпека - не стільки незмінний стан об’єкта, скільки його здатність відтворюватися, розбудовуватися, стало й прогресивно розвиватися в умовах конфліктів, невизначеності й ризиків. Так само неприйнятним убачається визначення інформаційної безпеки як «захищеності інтересів», адже інтереси – це потреби, без задоволення яких нормальне існування соціуму неможливе, тож їх потрібно не захищати, а реалізовувати. Захисту потребують цінності, необхідні для нормальної життєдіяльності людини, суспільства, держави, й умови, що забезпечують їхній доступ до цих цінностей, а також можливість користуватися ними. Себто безпека передбачає насамперед наявність необхідних цінностей і доступу до них. Відсутність цінностей вимагає пошуку їх нових джерел або їх замінників, а ускладнений доступ до них - усунення перешкод або вжиття заходів для їхнього подолання, що, у свою чергу, визначає зміст категорії «національні цілі».

Таким чином, інформаційну безпеку України слід визначити як стан, за якого в умовах дії різнопланових загроз забезпечується самозбереження,

сталий і прогресивний розвиток інформаційної сфери, в тому числі захищеність *національних цінностей*, необхідних для існування суверенної Української держави та виконання нею своїх функцій, а також досягнення відповідних *національних цілей* та реалізація *національних інтересів*. Інформаційна сфера при цьому утворюється сукупністю:

- суб‘єктів інформаційних процесів;
- інформаційної інфраструктури;
- інформаційного простору;
- інформаційних ресурсів;
- суспільних відносин, що складаються у зв‘язку з формуванням, зберіганням, передачею та розповсюдженням інформації.

За такого визначення система інформаційної безпеки з точки зору її об’єктів відповідає класичній формулі для об’єктів національної безпеки: «територія - народонаселення - система державного управління». Однак стосовно інформаційної безпеки замість території вважаємо за доцільне використовувати поняття «інформаційний простір», яке охоплюватиме, зокрема, й інформаційну модель території та її інформаційне обслуговування.

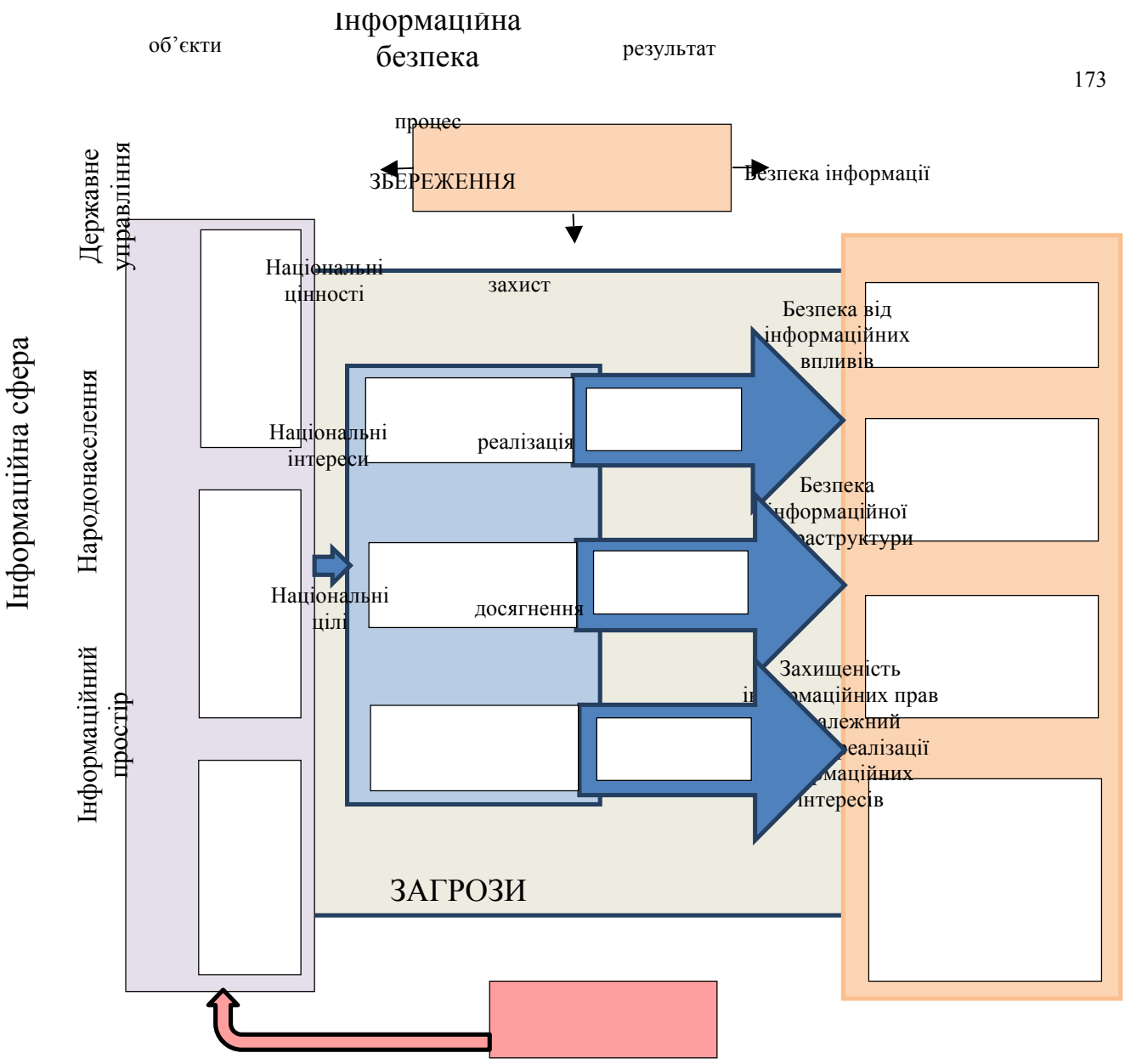

Рис. 2.2. Система інформаційної безпеки держави

Джерело: розроблено автором

Відповідно до викладеного вище функціональна система інформаційної безпеки України як складової частини та інформаційного виміру національної безпеки набуває такого схематичного вигляду (рис. 2.2.):

На нашу думку, розмежування інформаційної безпеки (як стану динамічної системи) та забезпечення інформаційної безпеки (як процесу підтримання цього стану, включаючи самовідтворення, збереження та

розвиток) дозволяє певним чином зняти суперечності між організаційно-структурним і функціонально-діяльнісним підходами до визначення сутності феномену інформаційної безпеки та її системи. Таким чином, система інформаційної безпеки як певне утворення, що характеризується подільністю, відкритістю, адаптивністю та наявністю структури, мети й пріоритетів оптимальної взаємодії елементів [187, с. 86], виступає об'єктом для системи забезпечення інформаційної безпеки, до якої також належать сили й засоби забезпечення інформаційної безпеки.

2.3.2. Співвідношення інформаційної та кібернетичної безпеки

Зауважимо, що система інформаційної безпеки, особливо на рівні її вислідних компонентів, може бути структурована за різними критеріями. Щодо кібернетичної безпеки, то Законом України «Про основні засади забезпечення кібербезпеки України» від 9 травня 2018 року [188] вона визначена як «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі». Виокремлення кібербезпеки зумовлене специфікою середовища, у якому функціонують інформаційні системи, здійснюється обіг інформації, реалізації законних інтересів суб'єктів інформаційних процесів. Тож «кібернетичний вимір» властивий усім складовим інформаційної безпеки.

Зважаючи на відсутність єдності науковців щодо місця кібербезпеки у системі інформаційної безпеки, запропонуємо авторське розуміння її основних складових, а також її співвідношення з інформаційною безпекою держави.

Кібернетичний, або *спеціальний програмно-математичний вплив* реалізується з використанням засобів знищення, перекручення або розкрадання інформаційних масивів. Після подолання систем захисту противника з його інформаційних масивів отримується інформація, володіння якою вважається необхідним; доступ до них для законних користувачів при цьому обмежується чи взагалі унеможливлюється. У рамках кібервпливу вдаються також до дезорганізації роботи технічних засобів, виведення з ладу телекомунікаційних мереж, комп'ютерних систем тощо.

Кібервплив провадять у *кібернетичному просторі* (кіберпросторі), під яким розуміють сферу діяльності в інформаційному просторі, утворену сукупністю комунікаційних каналів мережі Інтернет та інших телекомунікаційних мереж, технологічної інфраструктури, що забезпечує їх функціонування, і будь-яких форм здійснюваної за їх допомогою людської активності (окремого індивіда, організації, держави тощо).

Кіберзагрози, або *інформаційно-технічні загрози*, хоча і є відносно новим видом інформаційних загроз, становлять суттєву небезпеку, серед іншого й через доволі швидкі темпи розвитку цього напряму. За сферами впливу кіберзагрози класифікують на дві групи. Перша з них пов'язана з атаками на бізнес і включає комерційне шпигунство, крадіжки баз даних, інформаційні дії з метою завдання шкоди репутаційному капіталу і т. ін. У разі подібних атак хакерам протистоять комп'ютерні фахівці корпорацій, кіберспецслужби. Якщо йдеться про кіберзагрози другої групи, то вони спрямовані на пристрої, що забезпечують життєдіяльність суспільства, контролюють пересування, роботу великої кількості служб і мають на меті злом комп'ютерних систем, крадіжку даних, нелегальне набуття можливості безкоштовно користуватися різними сервісами, видалення і зміну інформації про себе, свою (або замовника) активність і т. ін.

У Європейській Конвенції з кібернетичних злочинів наведено таке визначення цього поняття: *кіберзлочини – це правопорушення, спрямовані*

проти конфіденційності, цілісності та доступності комп'ютерних систем, мереж і даних, а також їх неправомірне використання [189]. Віртуальний характер кіберзлочинів, а також засоби, за допомогою яких вони здійснюються, дозволяє зловмисникам швидко знищити сліди. Це значно ускладнює з'ясування обставин і пошук винуватців, тож постає нагальна потреба в розробленні нових методів розслідування кіберзлочинів і відповідних законодавчих норм, що регламентують сферу інформаційної безпеки.

Таким чином, на сучасному етапі бойові дії ведуться і в *інформаційному просторі* – принципово новому середовищі, де формується, перетворюється, передається, використовується, зберігається інформація, що впливає на індивідуальну і суспільну свідомість, інформаційну інфраструктуру і власне інформацію. Можна констатувати наявність не лише інформаційного простору як частини загального геостратегічного ландшафту, а й передумов для створення, розвитку й поширення інформаційної зброї. З огляду на це збройні конфлікти дедалі більше тяжіють до формату багатовимірних інформаційних воєн і можуть одночасно вестися на різних рівнях.

В інформаційно-технічному протиборстві головними об'єктами нападу і захисту є системи управління та зв'язку, телекомунікаційні системи, радіоелектронні засоби, а також інформаційні ресурси держави – інформація на матеріальних носіях або наявна в будь-який інший формі. Саме в цій сфері сформувалося поняття ІЗ як *сукупності засобів розвідки, управління, зв'язку, навігації та радіоелектронної боротьби*. Загальновживаним термін «інформаційна зброя» став після завершення військової операції «Буря в пустелі» (Ірак, 1991), у ході якої комплексне застосування вищенаведеного переліку засобів на театрі військових дій зіграло вирішальну роль у досягненні стратегічної мети.

На жаль, на законодавчому рівні питання системи інформаційної безпеки досі комплексно не вирішено. Навіть нова Доктрина

інформаційної безпеки України [190], яка готувалася в умовах, коли наша країна потерпає від гібридної агресії Російської Федерації, а отже - вже треба було б усвідомлювати значення інформації, інформаційних впливів та інформаційної сфери в цілому, не орієнтує на вирішення усього комплексу виявлених проблем, не загострює проблеми необхідності їх законодавчого врегулювання.

Так, виходячи з необхідності вдосконалення нормативно-правового забезпечення та попередження й нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері, з початком гібридної війни проти України виникла необхідність кардинальних змін у системі забезпечення інформаційної безпеки нашої держави. Основний план заходів було запроваджено рішенням РНБО від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України», затвердженим Указом Президента України N 449/2014 від 01 травня 2014 року [191]. Згідно з цим рішенням Кабінету Міністрів України було доручено розробити й подати на розгляд парламенту законопроекти про внесення змін у закони України щодо протидії інформаційній агресії іноземних держав, передбачивши, зокрема: визначення механізму протидії негативному інформаційно-психологічному впливу, в тому числі шляхом заборони ретрансляції телевізійних каналів; запровадження для іноземних ЗМІ системи інформування та захисту журналістів, які працюють у місцях збройних конфліктів, вчинення терористичних актів, при ліквідації небезпечних злочинних груп. Крім того, приписувалося підготувати проект стратегії розвитку інформаційного простору України, розробити і впровадити комплексні заходи організаційного, інформаційного й роз’яснювального характеру щодо всебічного висвітлення заходів з реалізації державної політики у сфері забезпечення інформаційної безпеки, а також посилити контроль за дотриманням законодавства з питань інформаційно-психологічної та кібернетичної безпеки. Відповідно до вказаного плану

заходів й було розроблено Доктрину інформаційної безпеки України [190].

Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу РФ в умовах розв'язаної нею гібридної війни. Її правовою основою є Конституція України, закони України, Стратегія національної безпеки України, затверджена Указом Президента від 26 травня 2015 року № 287, а також міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

У тексті Доктрини йдеться про національні інтереси України в інформаційній сфері, актуальні загрози національним інтересам та національній безпеці, пріоритети державної політики в інформаційній сфері й механізм її реалізації. Втілення положень цього документа покладено на Кабінет Міністрів, Міністерство інформаційної політики, Міністерство закордонних справ, Міністерство культури України, Державне агентство України з питань кіно, Національну раду України з питань телебачення і радіомовлення, Державний комітет телебачення і радіомовлення України, Службу безпеки України, розвідувальні органи, Державну службу спеціального зв'язку та захисту інформації, Національний інститут стратегічних досліджень, а також на Верховну Раду України, оскільки Доктриною передбачається внесення змін до чинного законодавства України.

Доктрина спрямовує на захист українського суспільства від «агресивного інформаційного впливу Російської Федерації», розвиток публічної дипломатії, в тому числі культурної та цифрової, видалення шкідливої інформації з українського сегменту Інтернету та квотування національного аудіовізуального контенту, захист права на вільний доступ до інформації, створення механізмів захисту від пропаганди тощо.

Утім, в експертному середовищі Доктрина отримала переважно негативну оцінку, на кшталт: «Доктрина інформаційної безпеки України – це лише декларація» або «Замість інтеграції Україна встановлює паркан»

тощо [192]. Справді, у Доктрині держава виклала бачення розвитку й функціонування свого інформаційного простору і визначила, що Російська Федерація є противником, котрий веде системну інформаційну війну. У документі є пропозиції, як реагувати на агресію та забезпечувати інформацією громадян. Доктрина також визначає поняття «стратегічного наративу» і вказує, що медіа мають самі себе регулювати, але при цьому мають нести соціальну відповідальність. Доктрина закладає державну систему постійного моніторингу веб-ресурсів та блокування сайтів, що загрожують безпеці, однак виписані в документі підстави для блокування доволі абстрактні - орган державної влади на свій розсуд зможе тлумачити, що загрожує безпеці, а що ні. Відповідно, виникає небезпека встановлення цензурних шлюзів, які відокремлять український Інтернет від світу. Крім того, механізм реалізації Доктрини, навіть у її позитивних аспектах, не містить жодної конкретики, тож у чинній редакції вона не може слугувати базовим документом, на підставі якого мають формуватися й інші правові акти у сфері забезпечення інформаційної безпеки, в тому числі стратегічні та програмні.

Відтак, погоджуємося з О. Довганем, сьогодні вкотре слід порушувати питання щодо розробки нормативного акта (закону), яким визначатиметься єдиний понятєво-категорійний апарат, державна політика забезпечення інформаційної безпеки, об’єкти інформаційної безпеки та суб’єкти її забезпечення, правові зони відповідальності відомств, залучених до сфери забезпечення інформаційної безпеки, механізми координування їх діяльності щодо реагування на виклики та загрози національній безпеці в інформаційній сфері, порядок правового закріплення взаємовідносин державних безпекових структур з іншими органами та відомствами, віднесеними законодавством до суб’єктів забезпечення національної безпеки України, тощо [193, с. 37-38]. Вважаємо, що такий нормативний акт неодмінно має дати чітке визначення як системи інформаційної безпеки, так і системи забезпечення

інформаційної безпеки.

З цього приводу зазначимо, що на засіданні РНБО України 17 січня 2018 року члени Ради обговорили та підтримали проект Закону України «Про національну безпеку України», який, за повідомленням офіційного сайту РНБО, «розроблявся у тісній взаємодії з експертами НАТО, США та Європейського Союзу з метою приведення української законодавчої бази у відповідність до стандартів держав-членів НАТО» [194]. На жаль, за результатами аналізу цього проекту доходимо висновку, що він не відповідає вимогам нормопроектувальної техніки, передусім:

- базується на підміні понять «суспільна безпека» («соціальна безпека») у розумінні «безпека суспільства» та «громадська безпека»;
- передбачає «точкове» регулювання відносин щодо окремих об’єктів, котрі входять до систем, перелік складових яких не є вичерпним (зокрема, систем на кшталт суспільної безпеки, національної безпеки, системи державних органів, які беруть участь у забезпеченні національної безпеки, та ін.);
- містить положення, які не стосуються предмета регулювання, задекларованого в назві проекту, та суперечливі норми права, дублює, повторює правові норми, які містяться в інших нормативно-правових актах.

Проект також не містить визначень основоположних дефініцій у сфері забезпечення національної безпеки, зокрема таких, як «національні цінності», «національні цілі», «система забезпечення національної безпеки», «система національної безпеки», «вид (сфера) національної безпеки», «об’єкти національної безпеки», «основи національної безпеки» тощо, а відтак, не може слугувати підґрунтям для визначення відповідних понять у контексті забезпечення інформаційної безпеки.

Усе це зайвий раз доводить нагальну потребу розробки та прийняття Закону України «Про інформаційну безпеку України» як базового

нормативно-правового акта, що регулюватиме відповідні питання. Такий закон як фундамент для побудови ефективної стратегії інформаційної безпеки має містити не абстрактні декларації, а чітко визначені основоположні категорії у сфері інформаційної безпеки та підходи до формування системи її забезпечення, механізм її функціонування, повноваження і схему взаємодії суб'єктів забезпечення інформаційної безпеки тощо.

Висновки до розділу 2

Дослідження місця правового забезпечення інформаційної безпеки держави в системі інформаційного права дає підстави стверджувати, що, по-перше, вказане правове структурне новоутворення у вітчизняній правовій системі має низку ознак підгалузі інформаційного права. Так, норми, які її складають, підпорядковані єдиній меті правового регулювання – забезпеченню інформаційної безпеки людини, суспільства, держави. Крім того, це утворення має відокремлений предмет правового регулювання, правовий режим, характеризується системним застосуванням притаманних галузі методів правового регулювання, значним інтегруванням та спеціалізацією правових інститутів, що його складають (а у складі останніх – субінститутів).

По-друге, правове забезпечення інформаційної безпеки держави є підгалуззю інформаційного права. Це зумовлено їх комплексною природою, а також тим, що правові відносини, які виникають у зв'язку із забезпеченням інформаційної безпеки, охоплюються загальногалузевими правовідносинами. Водночас, вказана підгалузь є цілком самостійним правовим утворенням, до структури котрого входять як норми власне інформаційного права, так і норми й положення інших правових галузей, котрі регулюють специфічні суспільні відносини, які виникають з приводу

захисту інформації з обмеженим доступом, ліцензування діяльності із захисту інформації, а також норми, що визначають відповідальність за правопорушення в інформаційній сфері.

Нарешті, по-третє, структуру правового забезпечення інформаційної безпеки держави як підгалузі інформаційного права складають інститути таємниці, захисту інформації, відповідальності за порушення у цій сфері тощо.

Сьогодні Україна відстоює свій євроінтеграційний курс в умовах окупації Криму й частини Донецької та Луганської областей унаслідок неоголошеної війни, яка ведеться російською Федерацією проти нашої держави з активним використанням методів інформаційного протиборства. У зв'язку зі значним негативним інформаційним впливом на інформаційний суверенітет нашої держави, питання правового забезпечення інформаційної безпеки України набувають особливої актуальності.

У цьому контексті важливим убачається розмежування інформаційної безпеки як стану динамічної системи та забезпечення інформаційної безпеки як процесу підтримання цього стану (включаючи самовідтворення, збереження та розвиток), що дозволяє зняти суперечність між організаційно-структурним і функціонально-діяльнісним підходами до визначення сутності феномену інформаційної безпеки та її системи.

Концепція національної безпеки сьогоднішнього дня - це політичний документ, що задає державі курс здійснення політики безпеки. У її контексті роль інформаційної безпеки полягає як певного інструментарію за допомогою якого здійснюється потужних деструктивний вплив.

У цьому ключі важливо відзначити роль захисту на державному рівні цінної інформації і управління інформаційними взаємодіями в процесі забезпечення національної безпеки, яка істотно зростає. На наш погляд, із усвідомленням можливості заподіяння шкоди інтересам людини, суспільства, держави при інформаційному обміні за допомогою певних

засобів інформаційних комунікацій бере свій початок інформаційна безпека. У методологічному сенсі важливо не лише перелічити складові системи інформаційної безпеки, а й доповнити вербалізацію цих явищ операціоналізацією і концептуалізацією понять, що їх позначають. Отже, наразі набуло непересічної актуальності питання розробки та прийняття Закону України «Про інформаційну безпеку України» як базового закону, що регулюватиме питання інформаційної безпеки.

Основні результати даного розділу висвітлено у працях [195-202].

РОЗДІЛ 3.
ТЕОЕРТИКО-ПРАВОВИЙ АНАЛІЗ СУЧАСНИХ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ В УМОВАХ ЄВРОІНТЕГРАЦІЇ

3.1. Класифікація загроз інформаційній безпеці України

Інтенсивна інформатизація усіх сфер життєдіяльності суспільства є сьогодні одним із визначальних глобальних чинників подальшого соціально-економічного, інтелектуального та духовного розвитку людства. Водночас, світова спільнота вступає в новий етап своєї історії, котрий має всі підстави охарактеризувати його як еру інформаційних воєн. Так, інформаційна складова є ключовим елементом гібридної війни Російської Федерації проти нашої держави. Це створює реальні загрози національній безпеці України, позаяк цілеспрямовано нищиться вітчизняна інформаційна інфраструктура на тимчасово окупованих територіях, проти України здійснюються кібернетичні атаки, блокуються канали поширення актуальної інформації щодо поточної соціально-політичної ситуації в країні, руйнівні інформаційні операції ведуться на тлі розгортання потужної пропагандистської кампанії проти України, спрямованої, зокрема, на перешкоджанням реалізації цивілізаційного вибору українського суспільства. Відтак, в умовах швидкого формування і розвитку інформаційного суспільства в Україні та глобального інформаційного простору, широкого використання інформаційно-комунікаційних технологій у всіх сферах життя особливого значення набувають проблеми інформаційної безпеки [190]. При цьому одним із

стратегічних пріоритетів забезпечення інформаційної безпеки державою визначено створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них [165].

Спираючись на положення Закону України «Про національну безпеку України» [203], можна стверджувати, що система загроз слугує базою для стратифікації національної безпеки (з урахуванням джерела, характеру і специфіки загроз) на зовнішньополітичну, внутрішньополітичну, державну, воєнну, економічну, соціальну, гуманітарну, екологічну та інформаційну безпеку, а також безпеку державного кордону. Втім, виходячи з визначення національної безпеки, наведеного в цьому ж законі, перелік сфер, у яких можуть проявлятися загрози національній безпеці, не є вичерпним. Зокрема, залежно від середовища формування і масштабів загроз національним інтересам, традиційним став поділ національної безпеки відповідно до джерел загроз на зовнішню та внутрішню [71, с. 13]. Але за сучасних умов такий поділ стає вельми умовним, адже зовнішні загрози можуть випливати із внутрішніх джерел, а також інтегруватися із загрозами внутрішніми.

Саме необхідність протидії загрозам зумовлює можливість і потребу дослідження національної безпеки з точки зору функціонально-діяльнісного підходу, відповідно до якого національна безпека розглядається як динамічне явище, котре постійно змінюється та еволюціонує. Цей підхід орієнтує на аналіз національної безпеки як процесу збереження і підтримання її сталого стану як єдиного утворення, оптимального розвитку всіх рівнів і видів безпеки як цілого, що забезпечує реалізацію національних інтересів [61, с. 39] в умовах можливого розгортання загроз. Він також дозволяє оцінювати можливості суспільства щодо належного забезпечення «гомеостатичного стану» об’єктів національної безпеки як сталості певного набору характеристик, за умови підтримання яких зберігається життєздатність вказаних об’єктів, а також

спроможність до спротиву намаганням зовнішніх чинників змінити стійкі внутрішні характеристики [204, с. 66].

Відповідно, національна безпека перебуває у взаємозв'язку із чинниками, які щодо неї можуть розглядатися як загрози, адже «національна безпека є системою оптимізації взаємовідносин між усвідомленими загрозами та ресурсами, що має суспільство для протидії цим загрозам. Загрози для суспільства є завжди, а рівень захищеності від них ніколи не буває максимальним. Тому національна безпека є динамічним засобом досягнення й підтримки балансу між реальними та потенційними загрозами, з одного боку, та здатністю суб'єкта протидіяти їм, з іншого» [206, с. 84].

Попри те, що поняття загрози неодноразово наводилося у різних доктринальних та нормативно-правових джерелах, досі немає єдиного підходу до визначення його змісту та ролі у теорії безпекознавства. Зокрема, А.Антонов і В.Балашов визначають загрозу як процес настання таких змін у стані особи, суспільства й держави, що оцінюються ними як здатні створити перешкоди для реалізації їхніх інтересів або унеможливити її [206, с. 48]. Водночас, слово «загроза», приміром, у словнику С.Ожегова [207, с. 673], означає можливу небезпеку, тобто, небезпеку, поки що не реалізовану. Тобто поняття «загроза» припускає не лише процес настання змін, але й можливість його настання. Під загрозою також розуміють «можливість або неминучість виникнення чогось небезпечного, прикрого, тяжкого для кого-, чого-небудь», «те, що може заподіювати яке-небудь зло, якусь неприємність» [208, с. 95].

Що стосується загроз безпеці, то їх у загальному вигляді визначають як сукупність чинників і умов, які створюють небезпеку певному об'єкту. В.Гордієнко звертає увагу на багатозначність термінів «загроза», «небезпека», «виклик» та «ризик», які в теорії безпекознавства використовуються і як самостійні, і як взаємовизначальні, ба навіть як синонімічні [209, с. 111-113]. Дослідник пропонує розглядати загрозу як

найвищий ступінь небезпеки (безпосередню небезпеку), а небезпеку – як потенційну загрозу. Своєю чергою, небезпека розглядається як завдання шкоди тим чи іншим інтересам, для реалізації чого необхідне створення відповідних умов (можливостей і намірів). Тож небезпека передбачає наявність або намірів, або можливості завдання шкоди, тоді як загроза містить і те, й інше. Небезпеки можуть виходити з багатьох джерел і стосуватися багатьох об'єктів, маючи безадресний характер. Натомість загроза, маючи конкретні джерело й об'єкт, завжди носить персоніфікований характер. Загроза за такого підходу розглядається як «сукупність умов та факторів, що створюють реальну і потенційну небезпеку (виклик, ризик) об'єктам… безпеки» [209, с. 113].

М.Гацко, поділяючи погляди В.Гордієнка на доцільність змістовного розмежування понять «небезпека» і «загроза», вибудовує відповідний причинно-наслідковий ланцюг у такий спосіб: виклик – небезпека – загроза, зазначаючи, що загрози і небезпеки перебувають у відношеннях залежності, які в разі зниження рівня загрози можуть призводити до зростання небезпеки [210].

М.Дзлієв і А.Урсул уважають, що загроза – це найбільш конкретна й безпосередня форма небезпеки, створювана цілеспрямованою діяльністю відверто ворожих сил; небезпека – усвідомлювана, але не фатальна ймовірність завдання шкоди кому-небудь, чому-небудь, зумовлена наявністю об'єктивних і суб'єктивних чинників, що мають вражаючі властивості; об'єктивно існуюча можливість негативного впливу на соціальний організм, у результаті якого йому може бути заподіяна певна шкода, що погіршує його стан, надає його розвиткові небажаних динаміки й параметрів (характер, темпи, форми тощо) [211, с. 42].

А.Возженіков відзначає, що загроза за своєю суттю не тотожна небезпеці, оскільки поняття «небезпека» є ширшим за спектром свого прояву. Загроза може становити небезпеку й виражатися через небезпеки, якщо йдеться про природне середовище, однак у соціальному, де йде

протиборство суб'єктів безпеки, вона становить сукупність намірів і можливостей одного суб'єкта завдати шкоди інтересам іншого. Тому поняття загрози науковець пропонує формулювати не тільки через категорію «небезпека», а й через категорії «намір» і «можливість»: «загроза безпеці – це сукупність умов і чинників, намірів і можливостей, здатних становити небезпеку життєво важливим інтересам особистості, суспільства й держави» [212, с. 95].

І.Кардашова розуміє під загрозою «сукупність умов і чинників, що створюють небезпеку життєво важливим інтересам особи, суспільству й державі» [213, с. 75-76].

В.Горбулін та А.Качинський розглядають загрозу як родову ознаку безпеки (можливість чи неминучість виникнення соціальних, природних або техногенних явищ із прогнозованими, але неконтрольованими небажаними подіями, що можуть статись у певний момент часу в межах даної території, спричинити смерть людей чи завдати шкоди їхньому здоров'ю, призвести до матеріальних і фінансових збитків, погіршити стан довкілля тощо) [71, с. 14, 27]. Небезпеку ж науковці вважають якісним станом - безпекою на її нульовому рівні [61, с 37].

Погоджуючись із розумінням безпеки й небезпеки як полярних станів об'єкта, пов'язаних зі збереженням або зміною його системних характеристик, під загрозами надалі розумітимемо чинники, здатні призвести до небезпеки, тобто до негативних змін системних характеристик об'єктів безпеки [214, с. 33].

У теорії забезпечення національної безпеки категорія «загроза» має не менш важливе значення, ніж категорія «життєво важливі інтереси», і тісно пов'язана з останньою, оскільки джерела загроз містяться передусім у багатоманітності й розбіжності інтересів. Загрозу також пропонують розглядати як «посягання на інтерес» [215, с. 124], що, одначе, вбачається сумнівним з точки зору досягнення мети чіткого визначення змісту цієї категорії. Адже інтерес – це усвідомлена потреба, а посягання на потребу,

так само, як і захист потреби, не впливають ані на її існування, ані на усвідомлення.

У цьому контексті становить інтерес типологія загроз національним інтересам США, що включає три категорії:

1) регіональні (збройні конфлікти);

2) транснаціональні (наркобізнес, нелегальна торгівля зброєю, міжнародна злочинність, піратство, екологічні загрози тощо);

3) асиметричні загрози.

Основною причиною, що зумовила виокремлення такої категорії загроз, як асиметричні, є ситуації, коли військова, економічна, науково-технологічна й інша могутність США та їхніх союзників значно перевищує потугу реальних і потенційних противників, що, однак, не гарантує забезпечення національної безпеки. При цьому виділяють асиметричні загрози тактичного, оперативного та стратегічного рівня, коротко- та довгострокові. Основою наявності асиметричних загроз є різне сприйняття інтересів сторін. Скажімо, загрозу від США та їхніх союзників супротивники сприймають як загрозу виживанню, тоді як США визначають обмежені цілі, що зазвичай не стосуються життєво важливих інтересів держави-противника. Наявність асиметричної загрози заподіяння неприйнятної для США шкоди може стримувати їх від рішучих дій та заходів проти держави-противника, котра значно слабша від них. Крім того, застосування такою державою тероризму, спеціальних інформаційних операцій дає змогу маскувати джерело загрози, зробити малоефективною протидію США [216, с. 58; 217, с. 24].

За визначенням О.Прохожева, загроза національній безпеці – це фактично будь-які внутрішні або зовнішні умови і фактори, що чинять негативний вплив на процес розвитку і вимагають для підвищення рівня соціального розвитку зниження своїх кількісних характеристик [218, с. 132].

О.Брега розглядає загрозу національній безпеці як одну з «елементарних часток теорії та практики забезпечення національної безпеки», яка характеризується об'єктивно-суб'єктивним змістом [219].

Загрози національній безпеці можна класифікувати за різними підставами, що свідчить про їх складну та багатошарову систему. Зокрема, у політології загрози національній безпеці класифікують таким чином:

- за місцем знаходження джерела – зовнішні та внутрішні; за масштабами можливих наслідків – загальнонаціональні, регіональні, локальні, поодинокі;
- за ступенем сформованості – потенційні, реальні; за ступенем суб'єктивного сприйняття – завищені, занижені, мінімальні, умовні, адекватні;
- за характером виникнення – загрози природного, техногенного й соціального характеру;
- за сферами життєдіяльності – загрози в економічній, політичній, оборонній, міжнародній, соціальній, інформаційній, науково-технічній, екологічній, культурній та духовній сферах [220] тощо.

С.Сулакшин поділяє загрози національній безпеці на зовнішні (безпосередня агресія; інформаційно-психологічна війна; соціальні) та внутрішні (природні; техногенні; соціальні), апріорні та апостеріорні, а також адресовані території, народонаселенню та державі [221]. М.Литвин та В.Кохан, досліджуючи питання внутрішньої безпеки, пропонують вирізняти загрози національній безпеці України у політичній, економічній, соціальній та військовій сферах, у сферах екології, культури, освіти та просвітництва, боротьби зі злочинністю, а також загрози, що викликають аварії та катастрофи техногенного, природного та іншого характеру [222]. В.Ліпкан уважає, що поділу на внутрішні й зовнішні підлягають передусім джерела загроз [223, с. 54].

Як зазначає М.Хусаїнов, принципова відмінність постконфронтаційного періоду полягає в тому, що на заміну домінуючій загрозі світові та інтересам наддержав приходить велика кількість потенційних загроз меншого масштабу, однак досить серйозних за своїми наслідками, що зачіпають інтереси багатьох країн [224, с. 68]. Процеси глобалізації зумовлюють загрози у таких галузях, як комунікації, транспорт, обмін інформацією, обіг капіталу тощо. Причому ці загрози у разі їх реалізації здатні паралізувати роботу військових, економічних, фінансових, енергетичних структур і навіть державного апарату з надзвичайно складними наслідками. Паралельно з розширенням діапазону традиційних загроз процеси глобалізації спричинили виникнення їх нової генерації. Специфіка останніх корініться у характерномк для глобалізації «відтериторіюванні» явищ та процесів, які функціонують у транскордонному суспільному просторі й відірвані від будь-якої конкретної територіальної локалізації [225, с. 21].

Справді, аналіз найбільш актуальних в умовах сьогодення загроз національній безпеці [226, с. 30] дозволяє дійти висновку щодо взаємозв’язку джерел виникнення і способів прояву більшості внутрішніх і зовнішніх загроз [224, с. 67]. Відповідно, на доктринальному рівні з’являються пропозиції щодо розширення типології зовнішніх та внутрішніх загроз національній безпеці шляхом виокремлення нового типу загроз – транскордонних, що мають глобальний характер та об’єднують одночасно ознаки внутрішніх та зовнішніх загроз: за формою прояву є переважно внутрішніми, а за своєю сутністю (за джерелами виникнення та стимуляції, складом можливих учасників тощо) можуть бути й зовнішніми [216, с. 54]. До цього типу загроз слід передусім відносити загрози інформаційній безпеці держави, що стимулюють розвиток нефізичної концепції безпеки [225, с. 23].

Чинна Стратегія національної безпеки України, затверджена Указом Президента України «Про рішення Ради національної безпеки і оборони

України від 6 травня 2015 року «Про Стратегію національної безпеки України» 26 травня 2015 року № 287/2015, серед основних загроз національній безпеці, які мають безпосередній стосунок до інформаційної сфери, визначає агресивні дії Росії, спрямовані на виснаження української економіки й підрив суспільно-політичної стабільності з метою знищення держави Україна і захоплення її території. Це, зокрема, інформаційно-психологічна війна, приниження української мови і культури, фальшування української історії, формування російськими засобами масової комунікації викривленої інформаційної картини світу, а також ведення інформаційної війни проти України. Водночас це також відсутність власної цілісної комунікативної політики нашої держави, недостатній рівень медіа-культури українського суспільства, уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак, фізична й моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом. Слід зауважити, що у Стратегії відмежовуються прояви інформаційно-психологічної війни (п.3.1), загрози кібербезпеці й безпеці інформаційних ресурсів (п.3.7) від загроз суто інформаційній безпеці (п.3.6), що, на нашу думку, не є виправданим.

Підсистема інформаційної безпеки посідає особливе місце в системі національної безпеки. Інформаційні відносини і процеси пронизують усі інші, які мають місце в суспільстві, тож інформаційна сфера існує одночасно на двох рівнях: самостійно й у взаємозв'язку з іншими сферами життєдіяльності суспільства шляхом їх інформаційного обслуговування та забезпечення взаємодії за допомогою інформації. Інформація завжди втілює певне змістовне навантаження, а отже, інформаційна сфера має своїм змістом знання (інформацію) про інші сфери життєдіяльності суспільства [227, с. 4] Це забезпечується формуванням інформаційних моделей інших сфер життєдіяльності суспільства, їх інфраструктури, суб'єктів та взаємодії останніх. Відтак, інформаційна сфера та її окремі

елементи дають змогу чинити опосередкований вплив на соціальну, економічну, політичну, духовну та інші сфери життєдіяльності людського суспільства. Тому забезпечення інформаційної безпеки є запорукою забезпечення інших складових державної безпеки та національної безпеки в цілому.

Отже, хоча всі складові у структурі національної безпеки пов'язані між собою, треба зважати, що окремі види безпеки є не лише самостійними, але й такими, що мають відповідні виміри в інших сферах життєдіяльності суспільства, закладаючи фундамент забезпечення їх безпеки. З-поміж таких видів, які отримали назву «інтегративні» [228], слід передусім назвати інформаційну безпеку. Таким чином, загрози інформаційного характеру можуть спрямовуватися до будь-яких складових державної безпеки, проте їхній негативний вплив завжди опосередковуватиметься завданням шкоди інформаційній безпеці держави. Приміром, економічна безпека в сучасних умовах інформаційно-мережевої економіки безпосередньо залежить від безпеки інформаційної, адже головним ресурсом розвитку виробництва наразі стає інформаційний продукт [229, с. 162]. Не випадково виняткову небезпечність загроз інформаційній безпеці підкреслює у своїй роботі Г.Сащук: «…Враховуючи той факт, що під впливом інформаційних атак може цілеспрямовано змінюватися світогляд та мораль як окремих осіб, так і суспільства в цілому, нав'язуються чужі інтереси, мотиви, спосіб життя, на перший план випливає аналіз сутності та форм проявів сучасних методів прихованого агресивного впливу, вияву дій, що мають цілеспрямований агресивний характер і які протирічать інтересам національної безпеки, та вироблення механізмів протидії їм у всіх напрямах» [151].

Тож, система загроз інформаційній безпеці має комплексний характер і в загальному вигляді містить такі їх типи: загрози безпеці інформації та інформаційної інфраструктури; загрози безпеці суб'єктів інформаційної сфери та соціальних зв'язків між ними від інформаційних

впливів; загрози належному порядку реалізації прав та інтересів суб'єктів інформаційної сфери. Тому варто погодитись із визначенням загроз інформаційній безпеці держави як сукупності умов та чинників, які становлять небезпеку життєво важливим інтересам держави суспільства й особи у зв'язку з можливістю негативного інформаційного впливу на свідомість та поведінку громадян, а також інформаційні ресурси та інформаційно-технічну інфраструктуру [230, с. 89].

До найбільш важливих властивостей загроз інформаційній безпеці держави слід віднести вибірковість, передбачуваність та шкідливість.

Вибірковість характеризує націленість загрози на заподіяння шкоди тим чи іншим конкретним властивостям об'єкта безпеки.

Передбачуваність – це наявність ознак виникнення загрози, що дозволяють заздалегідь прогнозувати можливість виникнення загрози та визначати конкретні об'єкти, на які вона буде спрямована.

Шкідливість – можливість завдати об'єкту безпеки шкоди різної тяжкості [231, с. 17].

А прецінь, зважаючи на динамічність суспільно-політичної обстановки та виникнення якісно нових небезпечних для нашої держави чинників, закріплення фіксованого переліку загроз інформаційній безпеці України, котрий до того ж не має вичерпного характеру, навряд чи є доцільним. Тож пропоновані науковцями переліки є зазвичай розширеними та більш актуальними порівняно із наведеним вище. Наприклад, до основних загроз національній безпеці України в інформаційній сфері пропонують відносити: поширення ідей, що провокують конфлікти на національному, релігійному і соціальному ґрунті та масові заворушення, а також розпалення серед українського населення ідей сепаратизму; заклики з боку окремих груп та осіб щодо посягання на державний суверенітет, територіальну цілісність, економічний, науково-технічний і оборонний потенціал нашої держави; проведення на шкоду інтересам України спеціальних інформаційних операцій та актів

зовнішньої інформаційної агресії; комп'ютерна злочинність; інформаційний тероризм; розвідувально-підривна діяльність іноземних спеціальних служб; розголошення інформації, яка становить державну та іншу передбачену законом таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства й держави; намагання маніпулювати громадською думкою, зокрема шляхом поширення недостовірної, неповної або упередженої інформації; дискредитація політики нашої держави та авторитету окремих державних діячів; прояви обмеження свободи слова й доступу громадян до інформації та інших їхніх прав і свобод; поширення засобами масової інформації культу насильства, жорстокості, порнографії та інших проявів аморальності; поширення ідеологій та впливу деструктивних неокультів; значний обсяг іноземної присутності в інформаційному просторі України; небезпечне для економічної незалежності України зростання частки іноземного капіталу у стратегічних галузях економіки, пов'язаних з інформаційною сферою; науково-технологічне відставання України від розвинутих країн; низька конкурентоспроможність продукції з обслуговування інформаційної сфери; нерозвиненість внутрішнього ринку високотехнологічної продукції та відсутність його ефективного захисту від іноземної технічної та технологічної експансії; зниження внутрішнього попиту на підготовку науково-технічних кадрів для наукових, конструкторських, технологічних установ та високотехнологічних підприємств, незадовільний рівень оплати науково-технічної праці, падіння її престижу, недосконаліть механізмів захисту прав інтелектуальної власності; відтік учених, фахівців, кваліфікованої робочої сили за межі України; інспірування інших деструктивних процесів в інформаційній сфері нашої держави [230, с. 90-92]. Утім, слід враховувати, що й такі розгорнуті переліки загроз не можуть вважатися вичерпними та константними. Джерелами загроз при цьому можуть виступати: людина, технічні пристрої, моделі, алгоритми,

програми, технологічні схеми обробки, зовнішнє середовище тощо [232, с. 67].

Найбільш небезпечні загрози інформаційній безпеці держави, передусім транскордонні та такі, що мають політичне забарвлення, вже тривалий час вивчаються в рамках проблеми інформаційної війни, поняттям якої вони охоплюються. Інформаційну війну, з урахуванням існуючих поглядів на її природу [233-240], можна визначити як сукупність цілеспрямованих інформаційних впливів, що здійснюються з використанням інформаційної зброї (алгоритму цілеспрямованого впливу на інформаційну систему шляхом передачі їй інформації або здійснення з інформацією інших запланованих дій), а також дій, не опосередкованих її використанням, спрямованих на заволодіння інформацією, що не є загальнодоступною, її несанкціоноване поширення, модифікацію або знищення, здійснювані задля досягнення запланованої мети. Небезпека, реальність та ефективність проявів інформаційної війни забезпечуються сугестивним характером впливів, таємним або завуальованим характером несанкціонованого одержання інформації чи її застосування, інших шкідливо-результативних дій в інформаційній сфері, які, своєю чергою, безпосередньо створюють умови для утиску інтересів, насамперед національних, або порушення процесів функціонування інформаційних систем [241, с. 290].

Інформаційна війна – це найвищий ступінь інформаційного протиборства, спрямований на розв’язання суспільно-політичних, ідеологічних, національних, територіальних конфліктів між державами, народами, націями та соціальними групами шляхом широкомасштабної реалізації засобів і методів інформаційної зброї. На думку В.Горбуліна, О.Додонова, Д.Ланде [240, с. 7] та І.Сопілко [242, с. 77], інформаційні війни, котрі є лише елементами реальних багатоаспектних протистоянь військово-політичного характеру, прийнято називати інформаційними операціями. При цьому основними методами інформаційної війни

слугують блокування або перекручування інформаційних потоків і процесів прийняття противником рішень [242, с. 77].

Так, з метою виправдання свого втручання у внутрішні справи України Росія вже тривалий час скеровує свою пропаганду проти української влади, намагається дискредитувати європейський вибір нашої держави, виставляє ООС (АТО) «каральною акцією» з «хаотичними бойовими діями», які призводять до невиправданих жертв серед мирного населення, поширює чутки про непрофесійність та деморалізацію українського війська [243, с. 181]. Крім того, в інформаційний простір України запускаються проекти тотального соціального зомбування, які начебто не пов'язані з політичними питаннями та подіями на сході, але насправді спрямовані на просування брехливої ідеології міфічного «Русского міра» та використовують маніпулятивні технології, маскуючись під пропаганду добра, людяності, взаємодопомоги з метою здійснення масштабного впливу на свідомість українців [244, с. 207].

До проявів інформаційної війни можна віднести і так звану інформаційну злочинність [245], левова частка якої припадає на кіберзлочини. Відомі факти правоохоронної практики свідчать про те, що прояви інформаційної злочинності – це переважно організована злочинність у своїй найбільш небезпечній частині. У рамках сучасних тенденцій до розширення мережевої архітектури організованої злочинності в теперішній час створюються неформальні групи хакерів у навчальних закладах та безпосередньо у віртуальному просторі. Є також відомості про залучення організованими злочинними групами хакерів до підготовки злочинів у кредитно-банківській сфері, на фондовому ринку, до протиправного заволодіння інформацією, що накопичується в інформаційно-довідкових і облікових комп'ютерних системах правоохоронних органів. Не виключена й розробка організованими злочинними співтовариствами планів інформаційних операцій, в тому числі інформаційних диверсій [246, с. 203].

Якщо за станом на 2015 рік Україна посідала 5 місце у світовому рейтингу з ризику зіткнення з веб-загрозами [247, с. 87], то після атаки вірусу «Petya» наприкінці 2017-го, від якої постраждали енергетичні компанії, банки, урядові установи тощо, антирейтинг нашої країни з питань кібербезпеки відчутно зріс. За оцінками фахівців, 2017 рік у цілому характеризували такі тенденції у сфері загроз інформаційній безпеці: неконтрольовані ризики, пов'язані з так званим «Інтернетом речей» та поширенням мережевих з'єднань; стрімке зростання «кіберзлочинів як сервісу» – надання цифрових послуг кримінальними синдикатами; зростання правових ризиків у сфері регулювання мережевих комунікацій; хакерські атаки, спрямовані на підрив репутації брендів та політичних сил [248].

Одним із джерел загроз інтересам суспільства в інформаційній сфері є також безперервне ускладнення інформаційних систем, тому особливою групою актуальних для України загроз інформаційній безпеці є загрози, зумовлені віртуалізацією [249, с. 139] – соціальним відчуженням людини, зануренням її в особистісний віртуальний світ. Змінені стани свідомості – транс, одержимість, сп'яніння, депривація сну тощо є ознаками віртуальної інтенції в людині і при цьому атрибутивно виступають знаково-символьною структурою віртуальності [250]. За прискорених темпів інформаційного прогресу, особливо з розвитком «Інтернету речей», людина взагалі ризикує перетворитися на придаток до інформаційних технологій та інформаційних ресурсів [242, с. 79; 251].

Утім, технічний аспект не є головним у структурі інформаційної безпеки. Необхідно забезпечити не лише безпеку інформації від знищення, перекручення, блокування, несанкціонованого витоку або порушення встановленого порядку маршрутизації, але й інформаційну безпеку суспільства. Власне ж суспільство є носієм такої глобальної загрози інформаційній безпеці людини, як інформаційна дискримінація, котра проявляється в розподілі людей на тих, що мають доступ до інформації, і

тих, котрі його позбавлені. Принципове значення для сучасного суспільства при цьому має факт існування інформаційної картини світу. Відповідно, одним із найпоширеніших видів інформаційних загроз стає розповсюдження так званих патогенних текстів, які суперечать чинній ідеологічній системі, спрямовані, зокрема, на підрив національних та державних інтересів, загрожують суспільній моралі, чинять шкідливий психологічний вплив, призводять до нехтування основними правами і свободами, втручаються в особисте життя тощо. Як слушно зазначає З.Живко, закрити національний інформаційний простір від такого інформаційного впливу, передусім зовнішнього, за допомогою адміністративних заходів неможливо, тож слід оберігати його від загроз безпеці так само, як наземний, повітряний і морський [252, с. 117-118].

3.2. Протидія загрозам інформаційній безпеці України: правові підходи

Основними принципами державного регулювання у сфері, що розглядається, є орієнтація на державно-правовий механізм забезпечення інформаційної безпеки та реалізація національних інтересів і цілей. Ефективність механізму забезпечення інформаційної безпеки визначається передусім його здатністю сприяти збереженню єдності нації, стабільності суспільних відносин, відтворенню національно-культурних цінностей, подоланню політичних, військових, економічних, соціальних криз, створенню передумов стабільного розвитку, а також здатністю ефективно протидіяти загрозам інформаційній безпеці. Останнє, у свою чергу, викликає до життя власне механізми протидії інформаційним загрозам, які на сучасному етапі характеризуються підвищеною небезпечністю, адже інформаційне протиборство нарощує свої можливості в результаті стрімкого зростання обсягу та значення інформації в сучасному світі.

Відтак, безпека сучасної держави безпосередньо залежить від стану її інформаційного простору. Комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації [190; 229, с. 162; 151].

У теорії національної безпеки механізм протидії загрозам національній безпеці зазвичай розглядають у широкому або у вузькому сенсі. У вузькому сенсі він виступає як складова частина державного механізму і становить систему державних організацій, органів, установ, а також недержавних інституцій, спеціально створюваних для забезпечення національної безпеки або таких, що наділяються окремими функціями щодо забезпечення національної безпеки, у їхній взаємодії та практичному функціонуванні (сили забезпечення національної безпеки).

У широкому сенсі механізм протидії загрозам національній безпеці включає не лише сили, але й систему засобів, за допомогою яких здійснюється протидія відповідним загрозам з метою захисту життєво важливих інтересів суспільства й держави. Такими засобами виступають технології, а також технічні, програмні, лінгвістичні, правові, організаційні засоби, включаючи телекомунікаційні канали, що використовуються з метою збирання, формування, обробки, передачі або приймання інформації щодо стану національної безпеки та стосовно заходів, спрямованих на її зміцнення, а також власне методи, способи і прийоми, використовувані суб’єктами забезпечення національної безпеки для вирішення завдань щодо протидії загрозам національній безпеці.

Механізм забезпечення національної безпеки - це динамічна система, у межах якої можна виділити такі стадії: формулювання інтересів, захист яких забезпечуватиметься; виявлення та прогнозування внутрішніх і зовнішніх загроз життєво важливим інтересам; вироблення системи заходів щодо протидії загрозам; нейтралізація загроз; здійснення заходів

щодо відновлення нормального функціонування об’єктів безпеки. Численність засобів протидії інформаційним загрозам та варіативність їх комбінацій залежно від специфіки загроз дають змогу вести мову у множині - про механізми протидії інформаційним загрозам національній безпеці.

Залежно від місцезнаходження джерела можливої загрози всі загрози національній безпеці, в тому числі інформаційні, традиційно поділяються на дві групи - зовнішні та внутрішні. Для інформаційної безпеки того чи іншого об’єкта внутрішніми вважаються ті загрози, які «виникають безпосередньо на об’єкті та зумовлюють взаємодію між його елементами або суб’єктами», тоді як зовнішніми – ті, що «виникають внаслідок його взаємодії із зовнішніми об’єктами» [231, с. 18; 220].

До зовнішніх загроз інформаційній безпеці при цьому відносять:

- діяльність іноземних розвідувальних і спеціальних служб;

- діяльність іноземних політичних і економічних структур, злочинних груп і формувань, а також окремих осіб чи їх об’єднань, спрямована проти інтересів громадян, суспільства й держави;

- діяльність політичних та економічних структур, злочинних груп і формувань, а також окремих осіб чи їх об’єднань усередині країни, спрямована проти інтересів громадян, держави й суспільства (у випадках, коли джерело загрози може бути розцінене як зовнішнє для конкретної інформаційної системи, котрій може бути завдана шкода внаслідок реалізації інформаційної загрози);

- стихійні лиха й катастрофи.

Інформаційні загрози прицільно спрямовуються на інформаційну інфраструктуру (інформаційні ресурси) і на саму інформацію та її потоки, як-от: бази і банки даних, архіви, масиви документів, бібліотеки, музейні фонди тощо, де на різних носіях зберігається той чи інший тип інформації. Інформаційна інфраструктура є сукупністю інформаційних систем, що включає:

- інформаційно-телекомунікаційні структури – державні й корпоративні комп'ютерні мережі, телекомунікаційні мережі та системи спеціального й загального користування, мережі й канали передачі даних, засоби управління інформаційними потоками;
- інформаційні, комп'ютерні й телекомунікаційні технології, що формують кібернетичний простір;
- засоби масової інформації;
- організаційні структури, які забезпечують функціонування та розвиток єдиного інформаційного простору, зокрема, збір, обробку, зберігання, розповсюдження, пошук і передачу інформації.

Чинна Стратегія національної безпеки України з-поміж основних загроз національній безпеці, які мають безпосередній стосунок до інформаційної сфери, визначає агресивні дії Росії, що здійснюються для виснаження української економіки й підриву суспільно-політичної стабільності з метою знищення держави Україна й захоплення її території. Це, зокрема, – інформаційно-психологічна війна, приниження української мови і культури, фальшування української історії, формування російськими засобами масової комунікації альтернативної реальній викривленої інформаційної картини світу. Крім того, це – відсутність власної цілісної комунікативної політики держави, недостатній рівень медіа-культури українського суспільства, уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак, фізична й моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом [82]. Слід зауважити, що у Стратегії розмежовуються прояви: інформаційно-психологічної війни (п.3.1); загрози кібербезпеці і безпеці інформаційних ресурсів (п.3.7); загрози інформаційній безпеці (п.3.6), що, на наш погляд, не є доцільним.

Доктрина інформаційної безпеки України (п.4) містить перелік

актуальних загроз національним інтересам та національній безпеці України в інформаційній сфері, а саме:

- здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення й дестабілізація суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні;

- проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі;

- інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах;

- інформаційне домінування держави-агресора на тимчасово окупованих територіях;

- недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України;

- неефективність державної інформаційної політики, недосконаліть законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства;

- поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні [190].

Стратегія кібербезпеки України передбачає також, що сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів, зокрема шляхом порушення штатних

режимів роботи автоматизованих систем керування технологічними процесами на об’єктах критичної інфраструктури. Більшого поширення набуває політично вмотивована діяльність у кіберпросторі у вигляді атак на урядові та приватні веб-сайти в мережі Інтернет. Дедалі частіше об'єктами кібератак та кіберзлочинів стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які забезпечують безпеку, оборону, захист від надзвичайних ситуацій. Новітні технології застосовуються не лише для скоєння традиційних видів злочинів, але і для вчинення принципово нових їх видів, притаманних суспільству з високим рівнем інформатизації [165].

Зокрема, С.Домбровська так визначає головну інформаційну загрозу державній безпеці України: це - загроза через інформаційний вплив іншої сторони на свідомість, підсвідомість, інформаційні ресурси, інформаційну сферу машинно-технічних систем та інші об’єкти інформаційної інфраструктури країни, нав’язування особі, суспільству й державі бажаної (для іншої сторони) системи цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної та державної діяльності, керування їхньою поведінкою і розвитком у бажаному для іншої сторони напрямку. Тобто, йдеться про загрозу суверенітету України в життєво важливих сферах суспільної й державної діяльності, що реалізується на інформаційному рівні, адже менш розвинена в інформаційному відношенні країна відстає у виробництві нових знань (технологій) і змушена користатися готовими рішеннями, які їй нав’язують ззовні, внаслідок чого вона потрапляє в залежність від зовнішніх інформаційних ресурсів і технологій [253, с. 2].

При розробці стратегій забезпечення національної безпеки також обов’язково враховується сучасний рівень впливу на суспільну свідомість за допомогою інформаційних маніпуляцій. Розвідки й контррозвідки держав застосовують в інформаційному протиборстві методи дезінформації та пропаганди, намагаючись добувати секретні відомості й

дезорієнтувати противника хибною інформацією. Сучасні інформаційні війни спрямовуються передусім на «мішені» двох класів. Це по-перше, технічні засоби противника (комп'ютерні мережі, інше устаткування), а, по-друге, - людські ресурси. Якщо метою атак на інформаційні системи є виведення з ладу критичних секторів життєзабезпечення держави-противника – енергетичного, оборонного, управлінського та ін., - то метою другого типу атак є психологічна «обробка» населення [254, с. 9-10]. Зазвичай інформаційна агресія вибудовується у три етапи: створення «ядра» (акумулювання значної кількості людей, незадоволених поточним станом речей); формування середовища (альтернативного інформаційного простору); створення атмосфери (зміна суспільної думки «точковими ударами») [255, с. 52-52; 256]. Інформаційне насильство, використовуване в інформаційному протистоянні, є латентним, не завжди розпізнаваним. Тому завданням держави в таких війнах є захист власної інформації та інформаційних систем, свідомості населення від маніпуляцій противника, а також закриття йому доступу (джерела зовнішніх загроз) до інформації, розкриття якої може завдати шкоди обороноздатності країни.

Глобальна мережа Інтернет є в теперішній час основною ареною протистояння різних сил і засобів, що вимагає нового рівня забезпечення національної безпеки від різнопланових загроз інформаційного опосередкування. Сьогодні інформаційна агресивність віртуального простору суттєво впливає на трансформацію діяльності всіх національних, а також міжнародних антитерористичних і антиекстремістських структур. Крім того, терористичні, екстремістські утворення, організовані злочинні угруповання вдаються до маскування проявів екстремізму й тероризму в інформаційному просторі позитивними гаслами й риторикою «добра та миру». Тому профілактичні заходи в інформаційній сфері компетентних органів державної влади мають спрямовуватися насамперед на формування імунітету суспільної свідомості до впливу деструктивних ідей. Задля цього важливо виробити систему заходів щодо запобігання й, за

необхідності, зміни характеру та вектора інформаційного впливу в соціальних мережах, себто, розробити механізм протидії відповідним загрозам [257-258].

Реалізація зовнішніх загроз передбачає пошук уразливості в інформаційній структурі для доступу до основних вузлів інформаційної інфраструктури, сховищ інформації, організаційної мережі, осіб-секретоносіїв тощо. Інструментами реалізації зовнішніх інформаційних загроз виступають різнопланові види так званої інформаційної зброї (не лише віруси, «хробаки», «трояни» та інші форми шкідливого програмного забезпечення, але й інші знаряддя інформаційного впливу).

Протидія зовнішнім загрозам інформаційній безпеці України відбувається в умовах прогресування тенденції до переформатування сфер впливу у світовому просторі на тлі глобалізації політичних, соціально-економічних, культурних відносин. Виявлення та аналіз відповідних загроз ускладнюється низкою чинників, як-от:

- наявність у частини населення відчуття відсутності зовнішніх загроз країні;
- у Воєнній доктрині та Доктрині інформаційної безпеки достеменно не визначені потенційні зовнішні загрози країні, що призводить до відсутності чіткої класифікації й ранжування загроз за ступенем важливості й порівняльною динамікою їх наростання;
- відсутність ясного розуміння причин і джерел виникнення цих загроз тощо.

Забезпечення безпеки в умовах внутрішніх і зовнішніх динамічних змін потребує наявності дієвого механізму забезпечення безпеки, зокрема механізмів протидії загрозам. Механізм протидії інформаційним загрозам від зовнішніх джерел можна визначити як інтегровану цілісну сукупність необхідних і достатніх функціональних і правових елементів, за допомогою яких суб’єкт формує раціональну систему впливу на загрози

інформаційній безпеці та зумовлені ними ризики, забезпечуючи в такий спосіб результативне виконання завдань і функцій, покладених на систему забезпечення інформаційної безпеки та національної безпеки в цілому.

Механізми протидії інформаційним загрозам від зовнішніх джерел як частина загального механізму забезпечення інформаційної безпеки держави та національної безпеки в цілому мають передбачати:

- мету забезпечення безпеки, що полягає у збереженні цілісності й захищеності інформаційної сфери у процесі її функціонування й розвитку;

- рівень безпеки, що диференціює структурні складові системи, які можуть стикатися з потенційними й реальними небезпеками;

- сфери безпеки, що визначають можливості функціонування й розвитку інформаційної сфери;

- параметри безпеки, що встановлюють припустимі межі відхилень у потенціалі системи інформаційної безпеки, кількості її елементів, їх якості, властивостях, зв’язках;

- перелік загроз, наслідки їх реалізації й механізм запобігання зумовлені: внутрішніми закономірностями функціонування системи інформаційної безпеки та впливом на неї зовнішнього середовища, що веде до небажаних і необоротних порушень у її відтворенні й розвиткові; змінами, що настають у разі реалізації загроз (такі, що компенсуються або не компенсуються; оборотні та необоротні; такі, що зачіпають або не зачіпають життєздатність системи); організаційно оформленою сукупністю стратегічних і тактичних дій, що забезпечують підтримку функціонування системи інформаційної безпеки та її здатність до самовідтворення.

З-поміж інформаційних загроз від зовнішніх джерел наразі найбільшу небезпеку для національної безпеки України становлять:

- спроби несанкціонованого доступу до інформації та впливу на інформаційні ресурси, інформаційну інфраструктуру органів виконавчої влади, що реалізують зовнішню та внутрішню політику України, українських представництв і організацій за кордоном, представництв

України при міжнародних організаціях.

- недостатня поінформованість населення зарубіжних країн (передусім тих, що межують з Україною) про зовнішньо- та внутрішньополітичну діяльність України;

- поширення за кордоном дезінформації про зовнішню та внутрішню політику України;

- інформаційний вплив іноземних політичних, економічних, військових і інформаційних структур на розробку й реалізацію стратегії зовнішньої та внутрішньої політики України;

- порушення прав українських громадян і юридичних осіб в інформаційній сфері за кордоном.

Механізми протидії інформаційним загрозам зовнішніх джерел передбачають необхідність організації багаторівневої й різноспрямованої системи заходів з урахуванням передусім специфіки зовнішніх чинників - геополітичної конфігурації, регіональної кон'юнктури і структурно-функціональної ролі країни, а також впливу транснаціональної організованої злочинності.

Отже, своєчасний моніторинг характеру, особливостей, масштабів загроз та їх наступне прогнозування мають особливе значення. Прогнозування є важливим і самостійним елементом профілактики інформаційних загроз від зовнішніх джерел, та, відповідно, забезпечення національної безпеки. Основним методом прогнозування є моделювання, головними принципами якого є: встановлення мети моделі; виділення обмеженої кількості ключових чинників, які привносять істотні зміни в досліджувану систему; з’ясування характеру взаємозв’язків між виділеними чинниками; встановлення принципу множинності зв’язків між чинниками й виявлення сутнісних зв’язків, які й визначають характер розвитку та зміни системи.

Стратегічні знання, отримані за результатами прогнозування, дозволяють ілюструвати модель розвитку досліджуваного середовища, а

також обґрунтовувати змістовні особливості її структурних елементів. При цьому для моніторингу, прогнозування і профілактики загроз придатне будь-яке середовище, котре характеризується наявністю зовнішніх джерел, з яких можуть продукуватися та відтворюватися загрози інформаційній безпеці особистості, суспільства й держави.

Слід враховувати, що в умовах стрімкого розвитку інформаційного суспільства, який також зумовлює вдосконалення методів ведення інформаційних воєн, звичні технології та механізми протидії зовнішнім загрозам національній безпеці застаріли, і на передній план виходять нові способи стримування розгортання загроз та мінімізації зумовлених ними ризиків. Методи протидії інформаційним загрозам від зовнішніх джерел можна умовно поділити на дві групи:

- профілактичні, або превентивні, - які застосовуються для недопущення розгортання відповідних загроз або для запобігання подальшим ризикам на початковому етапі розгортання таких загроз;

- оперативні методи, які використовуються безпосередньо у відповідь на агресивні кроки, що виходять від зовнішніх джерел інформаційних загроз та пов’язані з їх розгортанням та реалізацією.

З-поміж заходів превентивної протидії інформаційним загрозам від зовнішніх джерел вирізняють чотири основні групи: нормативно-правові, адміністративні, інформаційні й економічні.

Оперативна протидія має здійснюватися тільки після виявлення достовірної інформації щодо структур, груп або осіб, котрі є рушійними силами, а також оцінки ступеня загрози й наявних ресурсів для її нейтралізації. Лише після ефективної роботи з інформацією можна обрати оптимальний оперативний метод протидії, який відповідає наявним ресурсам і є достатнім для нейтралізації загрози відповідного ступеня. Серед оперативних заходів протидії інформаційним загрозам зовнішніх джерел виділяють, зокрема, такі:

- персоніфікація дій джерела загрози, в тому числі інформаційних

впливів;

- делегітимізація дій джерела загрози;
- спростування чуток і розвінчування дезінформації з боку джерела загрози;
- формування потрібного інформаційного емоційного фону й політичних настанов щодо реагування на дії джерела загрози; робота зі ЗМІ; зовнішній тиск на джерело загрози;
- зміна моделі комунікації, нав'язуваної джерелом загрози [259, с. 78].

Механізм протидії інформаційним загрозам зовнішніх джерел, розгортання яких відбувається в ході гібридної війни, має включати:

- постійний контроль інформаційного простору (преса, телебачення, радіо, Інтернет);
- обмеження розмірів простору, об'єктів інформаційної інфраструктури та соціальних груп, що піддаються ураженню інформаційною дією;
- посилення авторитету своєї влади, уряду, армії серед населення країни, аби перешкодити переходу на бік ворога та підтримці дій, які він нав'язує;
- ефективна інформаційна політика: стратегічна спрямованість та зворотний зв'язок із суспільством [260, с. 394].

Окрім того, можна виокремити політичні, економічні та інші механізми протидії інформаційним загрозам зовнішніх джерел. Так, ураховуючи політичні цілі, що випливають із єдиної стратегічної мети забезпечення національної безпеки України, можна виділити окремі політичні механізми протидії інформаційним загрозам від зовнішніх джерел:

- механізми розробки та прийняття рішень у Раді безпеки ООН, взаємодія в рамках ОБСЄ, механізми зміцнення й розвитку в межах інших міждержавних утворень, які є засобом політичної, економічної та

військової євроінтеграції України;

- механізми державного й військового управління, впливу політичних партій, уведення адміністративно-правових режимів тощо, пов'язані з управлінням внутрішньополітичними процесами, що прямо впливають на забезпечення інформаційної безпеки країни;

- механізми просування інтересів держави в міжнародній інформаційній сфері, інформаційне забезпечення державної політики України, пов'язане з доведенням до вітчизняної й міжнародної громадськості достовірної інформації про державну політику країни, розвиток сучасних інформаційних технологій, захист інформаційних ресурсів тощо;

- механізми протидії зовнішнім загрозам політичній, економічній та іншій безпеці України тощо.

Зрозуміло, що механізми протидії інформаційним загрозам від зовнішніх джерел можуть видозмінюватися, позаяк конкретний механізм створюється відразу із з'ясуванням наявності певної загрози й формулюванням стратегічної мети щодо її нейтралізації. Слід також враховувати, що за сучасних умов розподіл інформаційних загроз на внутрішні й зовнішні є вельми умовним. Оскільки інформаційні загрози завжди мають комплексний характер, замахи на зовнішню безпеку країни формують загрози внутрішній безпеці, а внутрішня дестабілізація веде і до зовнішньої уразливості держави. Крім того, інформаційні загрози національній безпеці України видозмінюються, розробляються й зосереджують як за кордоном, так і усередині нашої держави (і джерелом зовнішньої загрози, скажімо, для безпеки інформаційних ресурсів певного державного органу України, може будь-яка група або особа, навіть така, що перебуває в Україні, якщо вона не може бути включена до архітектури безпеки цього державного органу), або можуть виходити з віртуального простору, що взагалі ускладнює можливість чіткого визначення локації їх джерела. Вони взаємно впливають одне на одне, набувають комплексного

характеру і тому для їхньої локалізації й нейтралізації потрібен системний підхід. Зокрема, для протидії інформаційним загрозам, що походять з віртуального простору, потрібне налагодження механізму, який включає:

- розвиток українського сегмента Інтернету;
- створення й контролювання українських аналогів соціальних мереж;
- розвиток нормативно-правової й законодавчої бази забезпечення інформаційної безпеки в мережі Інтернет;
- виявлення джерел інформаційних кампаній у соціальних мережах;
- зсув акценту від технократичного до гуманітарних аспектів забезпечення інформаційної безпеки;
- розвиток державної підтримки науково-практичних досліджень гуманітарних аспектів інформаційної безпеки;
- урахування можливих негативних наслідків використання новітніх інформаційних технологій [261, с. 36; 262, с. 44] тощо.

Слід також враховувати, що загрози, передусім зовнішні, належать до сторонніх щодо системи забезпечення безпеки чинників, а відтак, неможливо не лише досягти стану їх абсолютної відсутності, але і скласти вичерпний перелік, адже вони трансформуються в умовах мінливого середовища. Тож, у сучасному світі відбувається зміщення акцентів із загроз на ризики, оскільки такий підхід дозволяє відходити від розуміння загроз як констант та застосовувати різнопланові підходи для унеможливлення їх розгортання, особливо за умов невизначеності [263]. Тобто, механізми протидії інформаційним загрозам від зовнішніх джерел, які базуються на принципах управління ризиками і передбачають процес прийняття та виконання управлінських рішень, спрямованих на зниження імовірності виникнення несприятливих наслідків та мінімізацію можливої шкоди, викликаної реалізацією загроз, за сучасних умов є найбільш перспективними й результативними. Відповідні механізми дають змогу

впливати передусім на керовані елементи (ризики), досягаючи вагомих для забезпечення її прийнятного стану результатів за рахунок застосування відносно незначних зусиль [264-269; 67, с. 89], а також успішно поєднувати профілактичні й оперативні методи протидії інформаційним загрозам від зовнішніх джерел.

3.3. Функціональний аналіз суб'єктів забезпечення інформаційної безпеки України в умовах євроінтеграції

Безпека особи, суспільства й держави, інформаційна зокрема, є складним, багаторівневим явищем, котре одночасно може розглядатися як процес та показник стану реалізації національних інтересів. При цьому до основних принципів забезпечення національної безпеки належать:

- дотримання та захист прав і свобод людини і громадянина;
- законність;
- системність та комплексність застосування органами державної влади та місцевого самоврядування заходів забезпечення безпеки;
- пріоритет попереджувальних заходів забезпечення безпеки;
- взаємодія державних органів з міжнародними організаціями, інститутами громадянського суспільства, громадянами та іншими суб'єктами з метою забезпечення безпеки.

Для реалізації зазначених принципів створюється система забезпечення національної безпеки, органічною складовою якої є система забезпечення інформаційної безпеки, призначена для втілення державної політики в інформаційній сфері. Важливе значення для ефективного функціонування системи забезпечення інформаційної безпеки держави має її суб'єктний склад, компетенція суб'єктів забезпечення інформаційної безпеки та належна організація взаємодії між ними.

Варто підкреслити, що функціональний зміст суб'єктів забезпечення інформаційної безпеки значною мірою визначається аналогічним змістом забезпечення національної безпеки. Тому, якщо вести мову про систему забезпечення національної безпеки в цілому, то слід зазначити, що до її складу традиційно включають сили та засоби забезпечення національної безпеки. Під силами в такому разі розуміють суб'єктний склад системи забезпечення національної безпеки, тоді як під засобами – технології, а також технічні, програмні, лінгвістичні, правові, організаційні засоби, включаючи телекомунікаційні канали, що застосовуються з метою збирання, формування, обробки, передання або приймання інформації щодо стану національної безпеки та стосовно заходів, спрямованих на її зміцнення. Так само система забезпечення інформаційної безпеки як складова системи забезпечення національної безпеки включає в себе відповідні сили й засоби.

В умовах розвитку інформаційного суспільства забезпечення інформаційної безпеки є функцією кожного суб'єкта інформаційної сфери, причому синергетичні властивості інформаційної безпеки зумовлюють певний дуалізм: кожен суб'єкт може одночасно виступати й об'єктом інформаційної безпеки, а крім того, - джерелом потенційних та реальних загроз або каналом їх поширення. Тому можливості щодо забезпечення інформаційної безпеки визначаються потенціями не лише спеціально призначених для цього державних інституцій, але й кожного суб'єкта інформаційних відносин щодо власного інформаційного самозахисту. Водночас, держава посідає особливе місце в системі суб'єктів забезпечення інформаційної безпеки, адже, як зазначає О.Тихомиров, це єдиний суб'єкт, у потенціалі якого, поряд з економічними, політичними, ідеологічними засобами опосередкованого впливу, закладені можливості прямого управлінського впливу на інформаційні відносини за допомогою правових засобів [143, с. 49].

Відповідно до ст. 17 Конституції України забезпечення інформаційної

безпеки, як і захист суверенітету й територіальної цілісності України, віднесено до найважливіших функцій держави. Остання ж провадить свою діяльність через відповідні органи державної влади. Зокрема, ч.3 ст.17 Конституції України визначає коло суб'єктів, на яких покладено забезпечення державної безпеки та виконання комплексу інших заходів, пов'язаних із забезпеченням національної безпеки. Це – військові формування та правоохоронні органи держави, організація і порядок діяльності яких визначаються законом.

Відповідно до ст. 12 Закону України «Про національну безпеку України» сектор безпеки і оборони України складається з чотирьох взаємопов'язаних складових: сили безпеки; сили оборони; оборонно-промисловий комплекс; громадяни та громадські об'єднання, які добровільно беруть участь у забезпеченні національної безпеки. Функції та повноваження складових сектору безпеки і оборони визначаються законодавством України.

До складу сектору безпеки і оборони входять: Міністерство оборони України, Збройні сили України, Державна спеціальна служба транспорту, Міністерство внутрішніх справ України, Національна гвардія України, Національна поліція України, Державна прикордонна служба України, Державна міграційна служба України, Державна служба України з надзвичайних ситуацій, Служба безпеки України, Управління державної охорони України, Державна служба спеціального зв'язку та захисту інформації України, Апарат Ради національної безпеки і оборони України, розвідувальні органи України, центральний орган виконавчої влади, що забезпечує формування та реалізує державну військово-промислову політику.

Інші державні органи та органи місцевого самоврядування здійснюють свої функції із забезпечення національної безпеки у взаємодії з органами, які входять до складу сектору безпеки і оборони [203].

Зважаючи на те, що головною метою системи забезпечення

інформаційної безпеки держави є забезпечення умов для вільного проходження інформаційних потоків і захист українського інформаційного простору від інформації, здатної зашкодити інтересам держави, з кола основних функцій суб'єктів забезпечення національної безпеки, визначених у ст.10 вказаного Закону, доцільно виокремити такі, що безпосередньо стосуються забезпечення інформаційної безпеки, а саме:

- вироблення й періодичне уточнення Стратегії національної безпеки України і Воєнної доктрини України, доктрин, концепцій, стратегій і програм у сфері національної безпеки, планування і здійснення конкретних заходів щодо протидії та нейтралізації загроз національним інтересам України;

- створення нормативно-правової бази, необхідної для ефективного функціонування системи національної безпеки;

- постійний моніторинг впливу на національну безпеку процесів, що проходять у соціальній, науково-технологічній, інформаційній сферах; прогнозування змін, що відбуваються в них, та потенційних загроз національній безпеці;

- прогнозування, виявлення та оцінка можливих загроз, дестабілізуючих чинників, причин їх виникнення та наслідків прояву;

- розроблення науково обґрунтованих пропозицій і рекомендацій щодо прийняття управлінських рішень з метою захисту національних інтересів України; запобігання та усунення впливу загроз і дестабілізуючих чинників на національні інтереси;

- оцінка результативності дій щодо забезпечення національної безпеки та визначення витрат на виконання цих завдань.

Специфіка реалізації функцій забезпечення інформаційної безпеки держави полягає у тому, що кожен державний орган здійснює власну діяльність з використанням інформаційної інфраструктури суспільства, виробляє і споживає інформаційні ресурси, має певні відносини із громадянами і як власник інформаційних ресурсів та інформаційної

інфраструктури має вживати певних заходів, спрямованих на забезпечення збереження ресурсів і безпеки функціонування інформаційних і телекомунікаційних систем, мереж зв'язку, систем управління [223, с. 83].

В.Ліпкан зазначає, що система забезпечення інформаційної безпеки, з погляду функціональності її суб'єктів, включає в себе стратегічний, тактичний та оперативний рівні управління інформаційною безпекою. До суб'єктів стратегічного рівня вчений відносить Раду національної безпеки і оборони України та Кабінет Міністрів України, тоді як до суб'єктів тактичного рівня - центральні органи виконавчої влади, а до суб'єктів оперативного рівня - місцеві органи виконавчої влади [223, с. 85].

О.Олійник ранжує суб'єктний склад забезпечення інформаційної безпеки за рівнями організаційно-функціонального забезпечення інформаційної безпеки «відповідно до порядку їх розташування в Конституції України»:

суб'єкти першого - загальнодержавного - рівня (Верховна Рада України, Президент України, Рада національної безпеки і оборони України, Кабінет Міністрів України);

суб'єкти другого рівня (центральні й місцеві органи виконавчої влади та інші державні органи, що виконують спеціальні повноваження, в тому числі органи прокуратури та судової влади);

суб'єкти третього рівня (підприємства, установи й організації критично важливих інфраструктур, які функціонують на основі використання електронних, телекомунікаційних засобів та інформаційних технологій, виведення яких з ладу може призвести до тяжких наслідків для особи, суспільства, держави);

суб'єкти четвертого рівня (громадян та їх об'єднання, а також державні та приватні засоби масової інформації) [270].

М.Левицька так класифікує суб'єктів забезпечення національної, зокрема, інформаційної безпеки:

суб'єкти, діяльність котрих безпосередньо підпорядкована завданням

забезпечення національної безпеки, як у комплексі, так і окремим із них (Рада національної безпеки і оборони України, правоохоронні та інші державні виконавчі органи спеціальної компетенції);

суб'єкти, для яких така діяльність є одним з основних, але не єдиним напрямом (вищі органи законодавчої, виконавчої та державної влади);

суб'єкти, для яких участь у забезпеченні національної безпеки не є основною діяльністю (всі інші державні та громадські організації) [271, с. 66].

На думку О.Тихомирова, серед суб'єктів забезпечення інформаційної безпеки можна узагальнено виділити три групи: міжнародні організації; держава в особі державних структур; недержавні організації, громадяни та їх об'єднання. При цьому кожна державна організація в межах своєї діяльності, реалізуючи функції держави, тією чи іншою мірою виступає суб'єктом державного забезпечення інформаційної безпеки. Існує також система державних органів, для яких окремі напрями забезпечення інформаційної безпеки є безпосередньою функцією. До таких структур в Україні О.Тихомиров пропонує відносити: Службу безпеки України, Службу зовнішньої розвідки України, Міністерство оборони України, Міністерство закордонних справ України, Державну службу спеціального зв'язку та захисту інформації України, Національну комісію з питань регулювання зв'язку України, Національну експертну комісію України з питань захисту суспільної моралі, Державну адміністрацію зв'язку Міністерства транспорту та зв'язку України, Державну службу України з питань захисту персональних даних, Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України, Національну раду України з питань телебачення і радіомовлення, а також Головне управління з питань безпекової та оборонної політики, Головне управління забезпечення доступу до публічної інформації, Управління з питань комунікацій Адміністрації Президента України та інші. З-поміж міжнародних

організацій, рішення яких відіграють важливу роль у формуванні системи забезпечення інформаційної безпеки як регіонального та світового масштабу, так і окремих держав, виділяють:

1) Європейський Союз (ЄС);
2) Організацію Об'єднаних Націй (ООН);
3) Організацію Об'єднаних Націй з питань освіти, науки і культури (ЮНЕСКО);
4) Шанхайську організацію співробітництва (ШОС);
5) Євразійське економічне співтовариство (ЄврАзЕС);
6) Організація Північноатлантичного договору (НАТО).

Недержавне забезпечення інформаційної безпеки при цьому може здійснюватися численними недержавними інституціями: засобами масової інформації; провайдерами телекомунікаційних послуг; комерційними підприємствами, які надають послуги з технічного захисту інформації; різноманітними об'єднаннями громадян, що здійснюють громадський контроль державного забезпечення інформаційної безпеки і сприяння йому та іншими [143, с. 84].

В.Гусаров, вибудовуючи матрицю інформаційної безпеки, підкреслює, що функціонально система забезпечення інформаційної безпеки України має складатися з: органів управління, на які покладалися б завдання з виявлення інформаційних загроз та планування інформаційних заходів; центрів аналізу розвитку інформаційної ситуації; сил і засобів для проведення інформаційних заходів; спеціальних методик і технологій виявлення, розпізнавання інформаційних загроз, а також їх нейтралізації (або іншої відповідної реакції). При цьому дослідник вважає, що ядро сил проведення заходів з інформаційної безпеки України мають складати державні органи, до завдань яких (або до завдань їх структурних підрозділів) входить діяльність щодо забезпечення інформаційної безпеки, а саме:

Служба безпеки України;

Служба зовнішньої розвідки України;

Міністерство оборони України;

Міністерство внутрішніх справ України;

Міністерство транспорту та зв'язку України;

Міністерство закордонних справ України;

Державна прикордонна служба України;

Державний комітет України по стандартизації, метрології та сертифікації;

Державний комітет з питань телебачення і радіомовлення України;

Служба спеціального зв'язку та захисту інформації України та інші державні органи [272].

Доктрина інформаційної безпеки України (п.6), затверджена Указом Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України», покладає функції щодо забезпечення інформаційної безпеки на такі органи:

- Рада національної безпеки і оборони України;
- Кабінет Міністрів України; Міністерство інформаційної політики України;
- Міністерство закордонних справ України;
- Міністерство оборони України;
- Служба безпеки України;
- Державна служба спеціального зв'язку та захисту інформації України;
- розвідувальні органи України.

Доктрина також передбачає, що Національний інститут стратегічних досліджень забезпечує науково-аналітичне та експертне супроводження процесу формування й реалізації державної інформаційної політики. Крім того, участь у забезпеченні інформаційної безпеки держави беруть Міністерство культури України, Державне агентство України з питань

кіно, Національна рада України з питань телебачення і радіомовлення, Державний комітет телебачення і радіомовлення України [190].

Таким чином, зважаючи на комплексний характер загроз національній безпеці України в інформаційній сфері та специфіку функціональних завдань, у складі системи суб'єктів, уповноважених на забезпечення інформаційної безпеки, можуть бути виділені спеціально уповноважені суб'єкти, для яких забезпечення національної безпеки, в тому числі й інформаційної (як у цілому, так і в її окремих аспектах), виступає основним завданням, та суб'єкти, які беруть участь у її забезпеченні.

Відповідно до мети цього дослідження нас передусім цікавитимуть державні органи, на які чинним законодавством покладаються специфічні завдання щодо забезпечення інформаційної безпеки при виконанні їх основних функцій. До таких органів належать:

по-перше, окрім визначених Доктриною інформаційної безпеки РНБО та Кабінету Міністрів України, також Президент України та Верховна Рада України, які здійснюють загальне керівництво, координацію та контроль за реалізацією заходів у сфері національної, в тому числі інформаційної, безпеки;

по-друге, – державні органи, на які безпосередньо покладається виконання заходів у сфері забезпечення інформаційної безпеки.

Проаналізуємо спочатку функції суб'єктів, які здійснюють загальне керівництво, координацію та контроль за реалізацією заходів у сфері забезпечення інформаційної безпеки.

Отже, *Президент України* як глава держави, гарант державного суверенітету, територіальної цілісності України, додержання Конституції, прав та свобод людини і громадянина виконує такі функції у сфері забезпечення інформаційної безпеки:

- *здійснює* загальне керівництво з питань забезпечення інформаційної безпеки як важливої складової національної безпеки та системоутворювального чинника інших видів

безпеки;

- *визначає* напрями й заходи забезпечення реалізації внутрішньої та зовнішньої державної політики інформаційної безпеки відповідно до змін внутрішньої ситуації в Україні та міжнародної обстановки;
- *утворює* за поданням прем'єр-міністра організаційно-функціональну систему центральних і місцевих органів виконавчої влади та визначає їх повноваження з питань забезпечення інформаційної безпеки;
- *затверджує* стратегію і тактику забезпечення інформаційної безпеки, інформаційного протиборства, ведення оборонних і наступальних інформаційних воєн, протидії й нейтралізації кібератак та інших спецоперацій проти України;
- *затверджує* порядок і правила забезпечення безпеки об'єктів критично важливих інфраструктур, управління яких здійснюється на основі електронних, телекомунікаційних засобів та інформаційних технологій;
- *санкціонує* застосування спеціальних заходів і засобів щодо попередження й нейтралізації широкомасштабних внутрішніх і зовнішніх загроз інформаційній безпеці України;
- *приймає* у разі необхідності рішення про введення в Україні або окремих її місцевостях надзвичайного стану у зв'язку з розв'язуванням проти України системної (гібридної) війни із подальшим затвердженням цих рішень Верховною Радою України;
- *визначає* напрями, завдання та здійснює керівництво зовнішньополітичною діяльністю держави щодо забезпечення інформаційної безпеки, веде перемови й укладає двосторонні та багатосторонні міжнародні угоди з цих питань;
- у посланнях до народу України та щорічних і позачергових

посланнях до Верховної Ради України *визначає* пріоритетні напрями забезпечення інформаційної безпеки [23].

Функції *Верховної Ради України* як єдиного органу законодавчої влади випливають із її конституційних повноважень. Тож, Верховна Рада України:

- *визначає* засади внутрішньої та зовнішньої політики інформаційної безпеки України;
- *формує* законодавчу базу з питань забезпечення інформаційної безпеки, спрямованої на: захист конституційних прав і свобод людини й громадянина, забезпечення єдності їх прав та обов'язків; розвиток духовних, морально-етичних, культурних, історичних, інтелектуальних і матеріальних цінностей, інформаційного і природного середовища; суверенітету, конституційного ладу, територіальної цілісності; політичної, економічної, соціокультурної, науково-технологічної, оборонної та державної безпеки, екологічної тощо складових національної безпеки;
- *затверджує* загальнодержавні програми забезпечення інформаційної безпеки; перелік об'єктів критично важливих інфраструктур зв'язку, транспорту, промислового виробництва, соціальної сфери, управління якими здійснюється на основі електронних, телекомунікаційних засобів та інформаційних технологій;
- *надає* в установленому законом порядку згоду на обов'язковість та денонсацію міжнародних угод із питань інформаційної безпеки;
- *затверджує* в установленому Конституцією України порядку звернення Президента України про введення надзвичайного стану в Україні або в окремих її місцевостях у зв'язку з розв'язанням проти України системної (гібридної) війни тощо

[23].

Рада національної безпеки і оборони України як координаційний і консультативно-дорадчий орган при Президентові України:

- *здійснює* оцінку потенційних і реальних загроз національним інтересам;
- *розробляє й доповідає* Президентові України пропозиції щодо їх попередження й нейтралізації;
- *розглядає* на своїх засіданнях найбільш актуальні питання забезпечення інформаційної безпеки й ухвалює відповідні рішення;
- *здійснює* координацію діяльності органів виконавчої влади щодо забезпечення національної безпеки в інформаційній сфері.

Так, ст. 3 Закону України «Про Раду національної безпеки і оборони України» [273] наділяє РНБО функціями координації та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони у мирний час. Ст. 4 цього ж закону покладає на Раду національної безпеки і оборони України, розгляд на своїх засіданнях питань, які відповідно до Конституції та законів України, Концепції (основ державної політики) національної безпеки України, Воєнної доктрини України належать до сфери національної безпеки і оборони, зокрема: визначення стратегічних національних інтересів України, концептуальних підходів та напрямів забезпечення національної безпеки й оборони у науково-технологічній, інформаційній сферах; заходів політичного, соціального, науково-технологічного, інформаційного та іншого характеру відповідно до масштабу потенційних та реальних загроз національним інтересам України; забезпечення і контроль надходження та опрацювання необхідної інформації, її збереження, конфіденційності та використання в інтересах національної безпеки України, аналіз на її основі стану й тенденцій розвитку подій, що відбуваються в Україні та світі, визначення потенційних та реальних загроз національним інтересам України.

Кабінет Міністрів України як вищий орган у системі виконавчої влади, відповідальний перед Президентом України та підконтрольний і підзвітний Верховній Раді України у межах, передбачених статтями 85, 87 Конституції України, відповідно до ст. 116 Конституції України, а також ст. 7 Закону України «Про національну безпеку України»:

- *забезпечує* інформаційний суверенітет України, здійснення внутрішньої та зовнішньої інформаційної політики держави, виконання Конституції та законів України, актів Президента України, що стосуються інформаційної безпеки;
- *вживає* заходів щодо забезпечення прав і свобод людини і громадянина в інформаційній сфері;
- *забезпечує* проведення державної політики інформаційної безпеки;
- *спрямовує і координує* роботу всієї системи органів державного управління з питань, що стосуються інформаційної безпеки.

Серед завдань Кабінету Міністрів України у сфері забезпечення інформаційної безпеки можна також виділити: визначення потреб у витратах на забезпечення інформаційної безпеки, забезпечення виконання затвердженого Верховною Радою України Державного бюджету України щодо фінансування заходів у сфері інформаційної безпеки у визначених обсягах; організація розроблення й виконання державних програм з розвитку інформаційної інфраструктури органів державного управління; здійснення передбачених законодавством заходів щодо формування, розміщення, фінансування та виконання державного оборонного замовлення на поставку (закупівлю) продукції, виконання робіт, надання послуг для потреб органів, що забезпечують інформаційну безпеку; встановлення порядку надання суб’єктам забезпечення інформаційної безпеки у користування державного майна, засобів зв’язку й радіочастотного ресурсу, комунікацій, інших об’єктів інфраструктури держави, навігаційної, топогеодезичної, метеорологічної, гідрографічної та

іншої інформації; здійснення загальнодержавних заходів щодо забезпечення «життєздатності» об'єктів інформаційної інфраструктури; забезпечення комплектування особовим складом сил забезпечення інформаційної безпеки; утворення, реорганізація, ліквідація науково-дослідних установ, навчальних закладів та структурних підрозділів суб'єктів забезпечення інформаційної безпеки; забезпечення реалізації права на соціально-економічний захист відповідно до законодавства України, що регламентує діяльність окремих суб'єктів забезпечення інформаційної безпеки; здійснення у визначених законом випадках регулювання господарської діяльності суб'єктів забезпечення інформаційної безпеки; встановлення відповідно до закону порядку реалізації та утилізації об'єктів інформаційної інфраструктури, інформаційних ресурсів; здійснення заходів щодо забезпечення обороноздатності України [274].

До кола державних органів, на які безпосередньо покладається виконання заходів у сфері забезпечення інформаційної безпеки, з урахуванням положень п. 6 Доктрини інформаційної безпеки, належать: Служба безпеки України; Державна служба спеціального зв'язку та захисту інформації України; Служба зовнішньої розвідки України; Міністерство оборони України; Міністерство інформаційної політики України; Міністерство закордонних справ України [190]. Крім того, за своїми функціональними завданнями до цього переліку слід включити Державну службу України з питань захисту персональних даних, Національну комісію, що здійснює державне регулювання у сфері зв'язку та інформатизації [275-277], а також Міністерство культури України, Державне агентство України з питань кіно, Національну раду України з питань телебачення і радіомовлення, Державний комітет телебачення і радіомовлення України, які відповідно до компетенції відіграють важливу роль у забезпеченні інформаційно-психологічної безпеки населення [190; 140].

Необхідно зазначити, що п.3 Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», визначає також перелік та функціональні завдання основних суб'єктів забезпечення кібербезпеки. Так, Рада національної безпеки і оборони України відповідно до Конституції України та у встановленому законом порядку має здійснювати координацію та контроль діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку України, тоді як основу національної системи кібербезпеки становитимуть Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи, на які покладаються специфічні завдання у сфері забезпечення кібербезпеки [165].

Водночас слід констатувати, що таке відокремлення інформаційної безпеки та кібербезпеки, яке знайшло відображення у Доктрині інформаційної безпеки України та Стратегії кібербезпеки України, є штучним, що призводить до розбалансованості зусиль суб'єктів забезпечення національної безпеки й інституціональної невизначеності. Зокрема, Т. Попова наголошує на необхідності розгляду національного сегмента кіберпростору як складової частини інформаційного простору держави, з чого випливає й логічність розгляду питань кібербезпеки в контексті інформаційної безпеки. Відтак, дослідження інформаційного середовища та кіберсередовища (і, відповідно, інформаційної безпеки та кібербезпеки) як окремих паралельних інституцій (напрямів діяльності) є методологічною помилкою [278].

Отже, доцільно вибудувати єдину систему суб'єктів забезпечення інформаційної безпеки, на які безпосередньо покладається виконання заходів у сфері забезпечення інформаційної безпеки, ранжувавши їх за основними сферами відповідальності:

- *Міністерство інформаційної політики України* (здійснює організацію та забезпечення моніторингу засобів масової інформації та загальнодоступних ресурсів вітчизняного сегмента мережі Інтернет з метою виявлення інформації, поширення якої заборонено в Україні, а також моніторингу загроз національним інтересам і національній безпеці в інформаційній сфері; сприяє Міністерству закордонних справ України щодо донесення офіційної позиції України до іноземних засобів масової інформації; формує поточні пріоритети державної інформаційної політики, контролює їх реалізацію; координує діяльність центральних та місцевих органів виконавчої влади у сфері забезпечення інформаційного суверенітету України, урядових комунікацій, кризових комунікацій, зокрема під час проведення антитерористичної операції та в особливий період; вживає заходів в інформаційній сфері, пов'язаних із запровадженням правових режимів надзвичайного чи воєнного стану; здійснює розробку стратегічного наративу та його імплементацію; виробляє і впроваджує стратегію інформаційного забезпечення процесу звільнення та реінтеграції тимчасово окупованих територій; розробляє та впроваджує єдині стандарти підготовки фахівців у сфері урядових комунікацій для потреб державних органів) [190; 279];

- *Міністерство закордонних справ України* (здійснює формування та реалізацію стратегії публічної та культурної дипломатії України; координує інформаційну діяльність державних органів у зовнішньополітичній сфері; забезпечує просування інтересів України за кордоном інформаційними засобами; забезпечує донесення позиції України до керівництва іноземних держав, парламентів та урядів, зовнішньополітичних відомств, представників бізнесу та експертних кіл, широкої громадськості, сприяння просуванню позитивного іміджу України; сприяє просуванню українських телеканалів у кабельні та супутникові мережі за кордоном; забезпечує налагодження взаємодії з міжнародними партнерами як на двосторонній, так і на багатосторонній

основі з метою застосування міжнародного досвіду та найкращих практик у контексті протидії інформаційним загрозам) [190];

- *Міністерство оборони України та Генеральний штаб Збройних сил України* відповідно до компетенції (забезпечують функціонування системи військово-цивільних зв'язків у місцях постійної дислокації та розгортання підрозділів Збройних сил України, інших військових формувань, а також організовують і забезпечують зв'язки з українськими та іноземними засобами масової інформації щодо висвітлення ситуації в районі проведення антитерористичної операції (нині – Операція об'єднаних сил) у Донецькій та Луганській областях, протидію спеціальним інформаційним операціям, спрямованим проти Збройних сил України та інших військових формувань, супроводження інформаційними засобами виконання завдань оборони України, донесення достовірної інформації до військовослужбовців Збройних Сил України, інших військових формувань, зокрема через засоби масової інформації Збройних Сил України; забезпечують здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснюють військову співпрацю з НАТО, пов'язану з безпекою кіберпростору та спільним захистом від кіберзагроз; забезпечують у взаємодії з Державною службою спеціального зв'язку та захисту інформації України і Службою безпеки України кіберзахист власної інформаційної інфраструктури) [190; 165; 280; 281];

- *Служба безпеки України* (здійснює моніторинг спеціальними методами і способами вітчизняних та іноземних засобів масової інформації та мережі Інтернет з метою виявлення загроз національній безпеці України в інформаційній сфері; протидіє проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуацій; здійснює попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі, контррозвідувальні та

оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, а також щодо готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, можливі наслідки якої безпосередньо створюють загрозу життєво важливим інтересам України; здійснює розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на комп'ютерні інциденти у сфері державної безпеки) [190; 165; 282];

- *Державна служба спеціального зв'язку та захисту інформації України* (забезпечує в межах компетенції формування і реалізацію державної політики у сферах організації спеціального зв'язку, захисту інформації, телекомунікацій та користування радіочастотним ресурсом України; здійснює формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури, державний контроль у цих сферах; координацію діяльності інших суб'єктів кібербезпеки щодо кіберзахисту; здійснення організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти й кібератаки та усунення їх наслідків, інформування про кіберзагрози та відповідні методи захисту від них; забезпечення функціонування державного центру кіберзахисту; проведення аудиту захищеності об'єктів критичної інформаційної інфраструктури на уразливість) [190; 165; 283];

- *розвідувальні органи України* - Служба зовнішньої розвідки України та розвідувальний орган Міністерства оборони України [165; 190; 284-285] (здійснюють добування, аналітичну обробку та надання розвідувальної інформації споживачам; реалізують спеціальні заходи впливу, спрямовані на підтримку національних інтересів і державної політики України в інформаційній сфері; здійснюють розвідувальну діяльність щодо загроз

національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки; сприяють у процесі здійснення розвідувальної діяльності реалізації та захисту національних інтересів України в інформаційній сфері за кордоном, протидії зовнішнім загрозам інформаційній безпеці держави);

- *Національна поліція України* (забезпечує захист прав і свобод людини та громадянина, інтересів суспільства й держави від злочинних посягань у кіберпросторі; здійснює запобігання, виявлення, припинення та розкриття кіберзлочинів, а також підвищення поінформованості громадян про безпеку в кіберпросторі) [190; 286];

- *Національний банк України* (забезпечує формування вимог щодо кіберзахисту критичної інформаційної інфраструктури у банківській сфері) [190; 287];

- *Державна служба України з питань захисту персональних даних* (забезпечує реалізацію державної політики у сфері захисту персональних даних; вносить пропозиції щодо формування державної політики у сфері захисту персональних даних; здійснює контроль за додержанням вимог законодавства про захист персональних даних; здійснює міжнародно-правове співробітництво у сфері захисту персональних даних) [288].

- *Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації* (забезпечує проведення єдиної державної політики з питань державного регулювання у сфері телекомунікацій, інформатизації та розвитку інформаційного суспільства, користування радіочастотним ресурсом, надання послуг поштового зв'язку; здійснює державне регулювання та нагляд у сфері телекомунікацій, інформатизації, користування радіочастотним ресурсом, надання послуг поштового зв'язку, використання інфраструктури з метою максимального задоволення попиту споживачів на послуги зв'язку та інформаційні послуги, створення сприятливих умов для залучення інвестицій, збільшення обсягів послуг та підвищення їх якості, розвитку та модернізації телекомунікаційних та

інформаційно-телекомунікаційних мереж з урахуванням інтересів національної безпеки; забезпечує ефективне користування радіочастотним ресурсом і функціонування ринку телекомунікаційних, інформаційно-телекомунікаційних, інформаційних послуг та послуг поштового зв'язку на основі збалансування інтересів суспільства, суб'єктів господарювання та споживачів цих послуг; сприяє розвитку конкуренції та підприємництва, забезпечення рівних умов діяльності суб'єктів господарювання всіх форм власності, вдосконалення механізму регулювання ринкових відносин у сфері телекомунікацій, інформатизації, користування радіочастотним ресурсом та надання послуг поштового зв'язку; забезпечує системність, комплексність і узгодженість розвитку інформатизації та інформаційного суспільства в державі) [289];

- *Міністерство культури України [290]*, *Державне агентство України з питань кіно [291]*, Н*аціональна рада України з питань телебачення і радіомовлення [292]*, *Державний комітет телебачення і радіомовлення України* [293] (відповідно до компетенції беруть участь у забезпеченні захисту українського інформаційного простору від пропагандистської аудіовізуальної та друкованої продукції держави-агресора; розробляють пріоритети і стимули розвитку українського кіно, телевізійного контенту, книгодрукування, зокрема висвітлення героїчного спротиву Українського народу російській агресії) [294].

Таким чином, можна вести мову про те, що, з погляду функціональних завдань суб'єктів, система забезпечення інформаційної безпеки держави складається з таких підсистем:

- *підсистема інформаційної розвідки* (основні суб'єкти: розвідувальні органи, Міністерство оборони України, Служба безпеки України, Міністерство закордонних справ України, Міністерство інформаційної політики України та ін.);

- *підсистема інформаційного захисту*, яка включає в себе підсистему захисту інформації та підсистему захисту від інформаційних впливів, в т.ч.

інформаційно-психологічного захисту й захисту суспільної моралі (основні суб'єкти: Міністерство оборони України, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації України, Міністерство інформаційної політики України, Державна служба України з питань захисту персональних даних, Національна поліція України, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, Національна рада України з питань телебачення і радіомовлення, Державний комітет телебачення і радіомовлення України та ін.);

- *підсистема інформаційного впливу* (основні суб'єкти: Міністерство оборони України, Служба безпеки України, розвідувальні органи України, Міністерство інформаційної політики України та ін.).

Зазначені підсистеми включають у себе також кібернетичний аспект забезпечення інформаційної безпеки, і внаслідок їх функціонування здійснюється забезпечення державної, військової, економічної та інших складових національної безпеки у внутрішній та зовнішній сферах. Слід зазначити, що міжвідомча взаємодія та координація діяльності в галузі забезпечення інформаційної безпеки держави суттєво ускладнюється внаслідок того, що ті чи інші суб'єкти забезпечення інформаційної безпеки відіграють різні за значенням ролі при забезпеченні інших складових національної безпеки, а тому їх повноваження у сфері забезпечення інформаційної безпеки можуть частково дублюватися.

Ми підтримуємо думку М.Зайцева, який зауважує, що сьогодні існує нагальна потреба створення системи забезпечення інформаційної безпеки, при цьому необхідно врахувати таке: по-перше, кількість елементів системи забезпечення інформаційної безпеки не повинна бути надмірною, оскільки їх збільшення призводитиме до ускладнення функціонування і, як наслідок, зменшення її ефективності; по-друге, має існувати єдиний суб'єкт управління забезпеченням інформаційної безпеки, наділений владними повноваженнями стосовно інших елементів забезпечення

інформаційної безпеки, а також запроваджені ефективні механізми їх взаємодії; по-третє, повноваження та функції суб'єктів забезпечення інформаційної безпеки мають чітко розмежовуватися, не допускати дублювань з метою уникнення конкуренції в діяльності цих суб'єктів та водночас охоплювати всі сфери та аспекти забезпечення інформаційної безпеки, що дозволить досягти прийнятної ефективності функціонування системи; по-четверте, до складу системи забезпечення інформаційної безпеки мають входити не тільки органи публічної влади, а й інституції громадянського суспільства, що дозволить однаково ефективно захищати в інформаційних відносинах інтереси не лише держави, а й суспільства та громадян [295, с. 237].

Відповідно, лишається відкритим питання щодо необхідності створення спеціально уповноваженого органу державної влади з питань забезпечення інформаційної безпеки. Проте не виключено, що така «надструктура» не зможе монополізувати та ефективно виконувати функції щодо забезпечення інформаційної безпеки внаслідок специфічного інтегруючого характеру останньої та її здатності «проникати» до інших сфер життєдіяльності суспільства внаслідок їх інформаційного обслуговування. Тому одним із найбільш вдалих варіантів забезпечення вироблення узгоджених рішень щодо напрямів і заходів забезпечення реалізації державної політики інформаційної безпеки вбачається створення при Раді національної безпеки і оборони України міжвідомчої комісії (або ж координаційної ради) у складі представників профільного Комітету Верховної Ради України, Кабінету Міністрів України, Міністерства інформаційної політики, Міністерства оборони, Служби безпеки України, Міністерства внутрішніх справ, Міністерства закордонних справ та інших державних органів, які спеціально уповноважені на виконання завдань щодо забезпечення інформаційної безпеки або беруть участь у її забезпеченні в рамках визначеної законодавством компетенції. Також звертає на себе увагу визначена ст.10 Закону України «Про Службу

безпеки України» наявність у структурі Центрального управління Служби безпеки України підрозділу контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, котрий, зважаючи на визначені ст.2 того ж закону завдання Служби безпеки України, може виконувати координуючу функцію у сфері забезпечення інформаційної безпеки держави, що, на нашу думку, потребуватиме внесення відповідних змін до Закону України «Про національну безпеку України», а також до Доктрини інформаційної безпеки України та Стратегії кібербезпеки України.

Висновки до розділу 3

Загрози інформаційній безпеці здебільшого супроводжують виникнення та реалізацію загроз в економічний та політичній сферах, у сфері виконання функцій держави тощо, і заподіяння шкоди в інформаційні сфері виступає передусім засобом досягнення інших цілей. Поряд із суто корисливою метою (наприклад, отримання коштів із банківських установ унаслідок вчинення корупційних злочинів), у сучасних умовах інформаційні загрози пов’язані з розпалюванням міжнаціональної, міжконфесійної та іншої ворожнечі, дискредитацією правоохоронної системи та органів державної влади в цілому, заподіянням шкоди честі, гідності та діловій репутації фізичних осіб, у тому числі публічних, формуванням «образу ворога», «зомбуванням» населення задля створення умов для управління масовою свідомістю. При цьому потенціал інформаційної сфери через її інтегруючий характер та здатність проникнення до інших сфер життєдіяльності суспільства поки що недостатньо усвідомлюється політиками та правоохоронцями (за винятком проявів кіберзлочинності), однак успішно використовується представниками організованих злочинних співтовариств та політичними противниками нашої держави.

Головною загрозою інформаційній безпеці України наразі лишається загроза впливу зовнішнього ворога на інформаційну інфраструктуру, інформаційні ресурси, на суспільство, свідомість та підсвідомість людей з метою нав'язати власну систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної й державної діяльності, керувати їхньою поведінкою і розвитком у бажаному для іншої сторони руслі. Стратегічне інформаційне протистояння являє собою як самостійний феномен, здатний вирішувати конфлікт без застосування традиційних збройних сил, так і небезпечний компонент гібридної війни, розгорнутої Росією проти України.

Механізми протидії інформаційним загрозам від зовнішніх джерел – це сукупність різноманітних видів діяльності органів державного й військового управління, громадських організацій і політичних інститутів та інших суб'єктів, а також способів їх взаємин, які дозволяють оперативно впливати на зовнішні загрози інформаційній безпеці або управляти зумовленими ними ризиками з метою їх локалізації й нейтралізації. Конкретні механізми протидії інформаційним загрозам від зовнішніх джерел вибудовуються на підставі системи потенційних і реальних небезпек, імовірності їх настання, з урахуванням циклу розвитку системи (зародження, становлення, зрілість, трансформація) та її конкретного стану (криза, депресія, піднесення), виходячи з наявних фінансових, матеріальних, кадрових можливостей країни, на основі балансу інтересів суспільства, держави, груп, окремих осіб. Оцінка відповідних механізмів базується на:

- інформаційній політиці держави, її впливі на параметри безпеки;
- виявленні ступеня ризику відхилень параметрів для стійкості системи інформаційної безпеки;
- визначенні зовнішніх обставин, у яких відбуваються відхилення: збільшення (за несприятливого зовнішнього середовища) або зниження (за сприятливого зовнішнього середовища) ризиків.

Таким чином, механізми протидії інформаційним загрозам від зовнішніх джерел є передусім такими, що базуються на принципах управління ризиками, дозволяють блокувати деструктивні елементи, властивості, процеси, що руйнують систему інформаційної безпеки та національної безпеки в цілому, і стимулювати конструктивні елементи, властивості, процеси, що сприяють її функціонуванню й розвитку.

У складі визначених компонентів безпеки інформації, безпеки «від інформації» й належного порядку реалізації прав та інтересів суб'єктів інформаційної сфери, щодо яких триває постійний процес протидії інформаційним загрозам та створення інформаційних загроз супротивнику, поняттям інформаційної безпеки охоплюється не лише захищеність інформаційної сфери, що є передумовою її належного функціонування, а й можливість учинення суб'єктами інформаційної сфери необхідних впливів на інші сфери життєдіяльності суспільства, взаємодії з останніми.

Нормативне закріплення системного характеру та змісту складових інформаційної безпеки сприятиме не лише більш коректному усвідомленню її сутності суб'єктами інформаційної сфери, але й забезпечить гармонійний розвиток законодавства у відповідній галузі та підвищить ефективність правового забезпечення інформаційної безпеки України. За відсутності такого концептуального визначення не можна адекватно сформулювати визначення безпеки інформації, кібербезпеки тощо. Однак, як уже зазначалося, в теперішній час поняття інформаційної безпеки закріплено у Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», який фактично передбачає тимчасову стратегію, котру доцільно затверджувати та періодично оновлювати на рівні підзаконних нормативно-правових актів. Тож убачається доцільним закріпити поняття інформаційної безпеки як складової національної безпеки та системного феномена у нормах Закону України «Про національну безпеку України», виклавши його таким чином: «Інформаційна складова національної безпеки (інформаційна безпека) –

постійний процес діяльності компетентних органів, спрямований на своєчасне запобігання, виявлення та протидію загрозам в інформаційній сфері, застосування активних заходів інформаційного впливу, а також сукупність умов такої діяльності, що реалізуються й здатні контролюватися тривалий час, за яких забезпечується формування, використання та розвиток інформаційної сфери в інтересах її суб'єктів та сталий розвиток суспільства шляхом розвитку власного інформаційного простору, зведення до мінімуму заподіяння шкоди через неповноту, несвоєчасність і недостовірність інформації, негативні інформаційні впливи (в тому числі - інформаційну експансію з боку інших держав), негативні наслідки функціонування інформаційних технологій, а також через несанкціоновані дії з інформацією».

Аналіз визначеної чинним законодавством України компетенції державних органів, на які покладаються завдання щодо забезпечення інформаційної безпеки, дозволяє дійти висновку, що, з погляду функціональних завдань суб'єктів, система забезпечення інформаційної безпеки держави складається з таких підсистем:

- *підсистема інформаційної розвідки* (основні суб'єкти: розвідувальні органи, Міністерство оборони України, Служба безпеки України, Міністерство закордонних справ України, Міністерство інформаційної політики України та ін.);

- *підсистема інформаційного захисту*, яка включає в себе підсистему захисту інформації та підсистему захисту від інформаційних впливів, в тому числі інформаційно-психологічного захисту й захисту суспільної моралі (основні суб'єкти: Міністерство оборони України, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації України, Міністерство інформаційної політики України, Державна служба України з питань захисту персональних даних, Національна поліція України, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, Національна рада України з питань телебачення

і радіомовлення, Державний комітет телебачення і радіомовлення України та ін.);

- *підсистема інформаційного впливу* (основні суб'єкти: Міністерство оборони України, Служба безпеки України, розвідувальні органи України, Міністерство інформаційної політики України та ін.).

Задля ефективної реалізації державної політики забезпечення інформаційної безпеки потрібні вдосконалення організаційно-функціонального забезпечення інформаційної безпеки, суттєва оптимізація системи державних органів, що виконують функції забезпечення інформаційної безпеки, чітке визначення й розмежування їх повноважень, налагодження ефективної взаємодії, координації діяльності всіх суб'єктів забезпечення інформаційної безпеки та контролю за дотриманням чинного законодавства. Запорукою вироблення узгоджених рішень щодо напрямів і заходів забезпечення реалізації державної політики інформаційної безпеки може слугувати створення при Раді національної безпеки і оборони України міжвідомчої структури за представництва основних суб'єктів забезпечення інформаційної безпеки або ж наділення додатковими координуючими повноваженнями Служби безпеки України.

Основні результати даного розділу висвітлено у працях [296-307].

РОЗДІЛ IV

МІЖНАРОДНИЙ ДОСВІД ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ, СУСПІЛЬСТВА, ДЕРЖАВИ

4.1. Правові засади політики інформаційної безпеки Північноатлантичного альянсу

8 червня 2017 року було прийнято Закон України «Про внесення змін до деяких законів України щодо зовнішньополітичного курсу України» [308], яким внесено зміни до законів України «Про національну безпеку України» [203] та «Про засади внутрішньої і зовнішньої політики» [309] у частині євроатлантичної інтеграції. Одним із пріоритетів національних інтересів України цим законом визначено інтеграцію у євроатлантичний безпековий простір з метою набуття членства в Організації Північноатлантичного договору. Остаточно обравши євроінтеграційний курс, Україна має орієнтуватися на стратегію розвитку країн Європи в інформаційній сфері [310, с. 20]. Найбільш успішним прикладом втілення в життя оптимальної моделі інформаційного суспільства є країни Європи, що входять до НАТО [311, с. 35].

Зазначені зміни в законодавстві свідчать про поглиблення співпраці України з НАТО задля набуття членства в цій організації. За таких умов набуває все більшого значення координація діяльності органів виконавчої влади, ЗМІ тощо з питань співробітництва з НАТО в інформаційній сфері. Цей вектор розвитку зовнішньої політики України впливає й на правове регулювання системи безпеки інформації як складової частини євроатлантичного безпекового простору [312, с. 110], що, у свою чергу,

потребує глибокого розуміння сутності політики інформаційної безпеки НАТО та інформаційної політики Альянсу в цілому.

Досліджуючи питання політики інформаційної безпеки НАТО в сучасних умовах, слід передусім з'ясувати сутність інформаційної політики цієї організації в цілому, а також питання забезпечення безпеки інформації та кібербезпеки у системі Альянсу.

Наразі регулювання інформаційної сфери у країнах НАТО здійснюється за такими напрямами:

1) заохочення конкуренції, боротьба з монополізмом та концентрацією ЗМІ;
2) забезпечення права і технічних можливостей для доступу до інформації та інформаційних ресурсів усього населення;
3) дотримання свободи слова;
4) захист інтересів національних меншин, національної культурної спадщини, мови, протистояння культурній експансії інших країн; захист молоді в інформаційній сфері;
5) охорона інтелектуальної власності, боротьба з піратством;
6) протидія кіберзлочинності; впровадження електронного урядування;
7) правове регулювання мережі Інтернет;
8) забезпечення інформаційної безпеки тощо [313, с. 22-23].

Система інформаційної політики НАТО є похідною від реалізації демократичного принципу цивільного контролю над військово-політичною сферою в умовах участі громадськості в міжнародному військово-політичному процесі. З підвищенням суспільного інтересу до діяльності Альянсу на початку 1990-х років основна роль у провадженні інформаційної діяльності відводиться власним інститутам НАТО. Основним органом проведення інформаційної політики організації є Атлантична рада, яка оприлюднює свої рішення й заяви для преси та широкого загалу. Крім Атлантичної ради, інформуванням громадськості

опікуються установи країн-членів НАТО.

Одну із провідних ролей у реалізації інформаційної політики Альянсу відіграє Бюро інформації та преси. Воно входить до числа структур відділу Генерального секретаря (після празького саміту 2002 року його функції виконує Департамент публічної дипломатії, який забезпечує інформаційну діяльність). У ході реалізації різних програм і заходів Бюро інформації та преси сприяє урядам країн-членів і держав-партнерів у розширенні розуміння громадськістю ролі й напрямків політики НАТО. Бюро підтримує тісні зв'язки з національними інформаційними органами й неурядовими організаціями та здійснює заходи, спрямовані на роз'яснення громадськості цілей, завдань і досягнень НАТО [314].

Якщо вести мову про забезпечення безпеки інформації, то слід зазначити, що при створенні НАТО в 1949 році системи безпеки країн-учасниць істотно різнилися. Перша натівська система засекречування містила вісім рівнів таємності, була розроблена для документів у вигляді «твердих копій», а також передбачала створення в кожній країні двох центральних режимних органів і певну кількість підпорядкованих їм структур. На початку 1990-х років НАТО розпочала політичну та військову трансформацію структур безпеки, відчувши не тільки позитивні (скорочення часу обміну, збільшення місткості носіїв, швидкість пошуку, класифікацію, створення баз даних), а й негативні (втрата конфіденційності, цілісності змісту інформації або цілісності системи, втрата доступу) наслідки інформатизації. Виникнення нових загроз у сфері інформаційної безпеки зумовило необхідність осучаснення підходів до забезпечення безпеки інформації [315].

Засади політики НАТО щодо забезпечення безпеки так званої класифікованої інформації викладені у Документі СМ (2002)49 «Безпека в організації Північноатлантичного договору (НАТО)» [316]. Класифікована інформація - термін, який використовується у законодавстві країн−членів НАТО стосовно частини «уразливої» (sensitive) інформації, тобто

інформації, чутливої до загроз, що виникають у зв'язку з несанкціонованим доступом до неї, а тому потребує захисту або принаймні обмеження доступу до неї. НАТО має п'ять рівнів захисту інформації з обмеженим доступом: Cosmic TOP Secret (CTS), NATO Secret (NS), NATO Confidential (NC), NATO Restricted (NR), Unclassified but Sensitive [317; 318]. При цьому, у внутрішньодержавному законодавстві застосовують не більше трьох рівнів класифікації для інформації з обмеженим доступом, враховуючи інформацію з грифом, що відповідає рівню RESTRICTED і належить до офіційної, службової та громадської публічної таємниці. Певні термінологічні та сутнісні розбіжності у визначенні та класифікації інформації з обмеженим доступом в національному законодавстві країн НАТО компенсуються уніфікацією підходів до такої інформації у базових сферах діяльності держав-членів – військовій, економічній, правоохоронній та ін.

Документ СМ (2002)49 [316] встановлює основні вимоги до системи забезпечення фізичної, організаційної, процедурної та технічної безпеки, зокрема й безпеки інформації. Дотримуючись спільних зобов'язань, кожна країна-член НАТО надає інформації з обмеженим доступом власну оцінку, і, залежно від того, як інші члени виконують прийняті на себе зобов'язання, визначає, яку саме інформацію зробити доступною Альянсу. Відтак, будь-яке відхилення одного чи декількох членів Альянсу від виконання їхніх зобов'язань може призвести до скорочення обсягу та якості переданої їм інформації. Зазначений документ проголошує п'ять основних принципів політики безпеки НАТО:

1) широти;
2) глибини;
3) централізації;
4) управління доступом;
5) персонального контролю [319].

Засадничим принципом безпеки інформації в системі НАТО є при

цьому те, що інформація має зберігати свій ступінь захисту протягом усього циклу її обігу, починаючи від джерела. При цьому контроль за розподілом і поширенням інформації має унеможливити її витік.

Завдання, які пов'язані із забезпеченням захисту інформації входять до компетенції Комітету внутрішньої безпеки НАТО (NSC). Даний Комітет є дорадчим органом при Північноатлантичній Раді з питань, що стосуються безпеки НАТО. Усередині НАТО національний уповноважений орган з безпеки інформації виконує функції керівництва створенням органу правління та режимних відділів, забезпечення безпеки таємної інформації НАТО в усіх установах, що перебувають під її юрисдикцією, як усередині країни, так і за її межами, забезпечення розробки планів захисту інформації в разі виникнення надзвичайних обставин з метою запобігання втрати конфіденційності інформації НАТО. Представники національного уповноваженого органа із забезпечення безпеки інформації беруть участь у нарадах Комітету безпеки НАТО, де виробляються політика й інструкції у безпековій сфері. На обсяг функцій відповідального уповноваженого впливають розмір і кількість населення країни, географія місць обробки таємної інформації й не в останню чергу розподіл повноважень між органами у сфері національної безпеки. В окремих країнах НАТО уповноважений орган з безпеки інформації входить до структури міністерств закордонних справ, оборони та юстиції, в інших країнах - його керівником є прем'єр-міністр або міністр внутрішніх справ.

Співробітництво між НАТО та країнами-партнерами, в тому числі з Україною, в рамках Ради євроатлантичного партнерства (РЄАП) та Програми «Партнерство заради миру» (ПЗМ) [320] також передбачає певні зобов'язання сторін щодо обміну інформацією та забезпечення її безпеки. Зокрема, перед обміном будь-якою таємною інформацією між країною-учасницею ПЗМ і НАТО, органи, на які покладається забезпечення безпеки інформації, мають бути взаємно впевненими, що сторона, яка приймає

інформацію, готова забезпечити її захист відповідно до вимог сторони, котра її передає.

Приєднання країни до програми ПЗМ передбачає ратифікацію Угоди про безпеку між НАТО та країнами, які беруть участь у РЄАП та/або ПЗМ. Згідно з положеннями цієї Угоди сторони погоджуються консультуватися з політичних і безпекових питань, розширювати й інтенсифікувати політичне та військове співробітництво в Європі, усвідомлюючи, що ефективність співробітництва в цих сферах передбачає обмін учасників секретною інформацією або іншою інформацією з обмеженим доступом. Відповідальним органом при захисті інформації, якою обмінюються сторони при співробітництві в рамках РЄАП/ПЗМ, є NOS. Крім того, між НАТО та країною-партнером укладається окрема адміністративна угода щодо стандартів взаємного забезпечення безпеки інформації, якою обмінюються сторони, а також призначається офіцер зв'язку між NOS і національним органом з безпеки інформації. Всі дані, якими обмінюються сторони в рамках РЄАП/ПЗМ, є інформацією з обмеженим доступом і призначена тільки для урядового використання. На відміну від стандартів щодо захисту інформації, прийнятих в системі НАТО, в мінімальних стандартах з обробки і захисту таємної інформації, якою обмінюються сторони в рамках програм РЄАП/ПЗМ, немає рівня «цілком таємно», адже кількість такої інформації в системі НАТО вкрай обмежена, а додаткові вимоги із забезпечення безпеки інформації такого рівня таємності невиправдано ускладнили би процедуру взаємного обміну.

Україна також активне співробітничає в галузі безпеки інформації в рамках програми НАТО «Наука заради миру і безпеки» [321]. Щорічно затверджується й Річна національна програма під егідою Комісії Україна – НАТО [322; 323]. В умовах тимчасової окупації Росією Автономної Республіки Крим та м. Севастополя, проведення в окремих районах Донецької та Луганської областей антитерористичної операції та загальної ситуації, що склалася внаслідок збройної агресії Росії проти України, Річна

національна програма під егідою Комісії Україна – НАТО на 2017 рік мала особливе значення для забезпечення захисту національних інтересів і безпеки України, передусім у контексті використання потенціалу та практичної допомоги НАТО та держав – членів Альянсу у підвищенні обороноздатності України для протидії агресії Росії та реформування за стандартами НАТО сектору безпеки й оборони та оборонно-промислового комплексу.

Важливим завданням НАТО є недопущення актів агресії у кіберпросторі [324], адже кібератаки частішають та стають усе більш організованими та збитковими для державних установ, підприємств, об'єктів критичної інфраструктури, а також можуть сягнути критичного рівня, який загрожує національному та євроатлантичному процвітанню, безпеці та стабільності всього світового співтовариства. Джерелом таких атак можуть бути іноземні військові та розвідувальні служби, організовані злочинні угруповання, терористичні та/або екстремістські групи [325]. Так, П.Корніш з лондонського Королівського інституту іноземних справ пропонує таку класифікацію інформаційних загроз: діяльність хакерів-одинаків; організована злочинність у глобальних мережах; ідеологічний і політичний екстремізм; інформаційна агресія держав [326]. При цьому, в системі НАТО під кібербезпекою розуміється підтримка стану готовності до протидії потенційним загрозам високої інтенсивності та вжиття наступальних контрзаходів.

Незважаючи на те, що НАТО з часів створення постійно захищає свої інформаційні системи, на Празькому саміті 2002 року це питання було винесене до кола політичних. Беручи до уваги технічний прогрес, досягнутий після Празького саміту, лідери країн Альянсу на Ризькому саміті у 2006 році ще раз визнали необхідність забезпечення кібернетичної безпеки. Водночас, перед кібернападами на Естонію в 2007 році діяльність НАТО в галузі кіберзахисту зосереджувалася переважно на захисті комунікаційних систем, які належали Альянсу та використовувалися його

членами. Кібернапади 2007 року змусили НАТО серйозніше замислитися над проблемами забезпечення безпеки кіберпростору, зокрема, сприймати загрози, що походять з Інтернет-простору, як стратегічно важливі. Надалі НАТО провела ретельну оцінку свого підходу до кіберзахисту, за результатами якої в жовтні 2007 року була підготовлена доповідь міністрам оборони країн-членів з рекомендаціями щодо конкретних завдань НАТО, а також нових заходів з удосконалення захисту від кібернападів. Офіційна політика НАТО у сфері кіберзахисту (NATO Cyber Defence Policy) була схвалена міністрами оборони держав-членів і представлена учасникам організації у квітні 2008 р. на саміті в Бухаресті. Її мета – «забезпечити можливості для надання підтримки країні-союзниці, на її вимогу, у протидії кібератаці» [327].

Кількість та складність кібернападів швидко збільшувалася після нападів на Естонію в 2007 році, а вже влітку 2008 року війна РФ проти Грузії продемонструвала, що кібернапади стали основною складовою воєнних дій із застосуванням традиційної зброї. Тож у 2010 році на Лісабонському саміті НАТО було вирішено розробити нову політику організації з питань кіберзахисту, а також конкретний план дій, який набув чинності з червня 2011 року. В рамках їх реалізації НАТО використовує процеси оборонного планування з метою сприяння розвитку захисту союзників від кіберзлочинності, а також для оптимізації взаємодії, співробітництва та обміну інформацією. З питань протидії небезпекам, що виникають у кіберпросторі, НАТО тісно співпрацює за країнами ЄС та з ООН [328].

У цьому контексті слушно зауважує В. Пилипчук про те, що Латвія, Литва та Естонія змогли протистояти спробам втручання РФ у внутрішні справи завдяки набуттю членства у ЄС і НАТО [329, с. 257].

У Стратегічний концепції та Декларації Лісабонського саміту зазначається, що швидкий розвиток та постійне ускладнення кібернападів роблять захист інформаційно-комунікаційних систем країн-членів НАТО

таким, від якого залежить майбутня безпека організації, а інформаційні атаки фігурують серед найнебезпечніших викликів і загроз безпеці та процвітанню держав-членів Альянсу [330]. В ієрархії викликів, перелічених у вказаній концепції, загрози, які походять з інформаційного простору, розташовані одразу ж після поширення зброї масового знищення й тероризму. Така увага зумовлена, зокрема, феноменом секьюритизації, завдяки якому кібербезпека «еволюціонувала з технічної дисципліни у стратегічний концепт» [331, с. 29]. Сьогодні НАТО забезпечує розвиток засобів запобігання, виявлення, реагування й відновлення після атак за допомогою створених Органу з управління кібернетичною безпекою, Спільного Центру передового досвіду з кіберзахисту і Сил реагування на комп'ютерні інциденти [332, с. 198].

Орган з управління кібернетичною безпекою (ОУКБ) відповідає виключно за узгодження діяльності в галузі кіберзахисту в межах організації. ОУКБ НАТО керує Комісія з управління діяльністю в галузі кіберзахисту, до складу якої входять керівники політичних, військових, оперативних і технічних органів НАТО, які відповідають за питання кіберзахисту. Вона є основним консультативним органом Північноатлантичної ради з питань кіберзахисту та надає поради країнам-членам організації з усіх аспектів кіберзахисту. ОУКБ НАТО входить до складу Управління нових викликів безпеці Штаб-квартири НАТО. Центр передового досвіду в галузі кіберзахисту (м. Таллінн), який одержав у жовтні 2008 року акредитацію при НАТО, не наділений оперативними функціями і виступає в ролі дослідницького й навчального центру, де розробляються доктринальні й концептуальні засади кібербезпеки. Він позиціонується як «головне джерело експертизи у сфері спільної кібероборони», яке «акумулює, створює й поширює знання з ключових питань кібербезпеки усередині НАТО, між державами Альянсу і його партнерами» [333]. Центр здійснює наукові дослідження та підготовку з питань ведення інформаційних операцій у віртуальному просторі. За

підтримки з боку Комітету з планування використання цивільних систем зв'язку, Центру передового досвіду в галузі боротьби з тероризмом (м. Анкара), а також програми НАТО «Наука заради миру і безпеки» Центр передового досвіду в галузі кіберзахисту проводить експертні перемови, навчальні семінари та обміни інформацією із зацікавленими партнерами й міжнародними організаціями (приміром, з ЄС та ОБСЄ) [334]. У 2015 році Центр опублікував книгу про кібервійну Росії проти України під назвою «Cyber War in Perspective: Russian Aggression against Ukraine», де проведено аналіз поточної діяльності у сфері захисту інформації та стратегічних і тактичних наслідків кібервійни. На сторінках цього видання експерти, зокрема, зазначають, що поняття «кібератака» включає наразі цифрову пропаганду, DDoS-кампанії, дефейси web-сайтів, витоки інформації внаслідок атак, використання шкідливого програмного забезпечення з метою шпигунства [335]. Британський експерт Р.Хьюз розглядає ОУКБ та талліннський Центр як елементи єдиної організаційної системи, де перший наділений «широкими можливостями щодо здійснення електронного моніторингу в «реальному часі» та діє на оперативно-тактичному рівні, тоді як Центр, розробляючи довгострокову доктрину НАТО, становить «інтелектуальну платформу» і є елементом стратегічного рівня [336]. У теперішній час експерти Центру розглядають мілітаризацію Інтернету як однин з найнебезпечніших трендів світового кіберпростору [337].

У заяві, оприлюдненій за результатами Варшавського саміту глав держав та урядів, які брали участь у засіданні Північноатлантичної ради у липні 2016 року, зазначається, що кібернапади становлять очевидний виклик безпеці Альянсу й можуть бути не менш згубними для сучасних суспільств, ніж напади із застосуванням звичайних видів зброї. Відтак, кіберзахист є частиною головного завдання НАТО – колективної оборони, а кіберпростір визнається сферою операцій, де НАТО має захищати себе так само ефективно, як робить це у повітрі, на землі та на морі. Це

підвищить спроможність НАТО щодо захисту та проведення операцій у цих сферах, збереже свободу дій та рішень у будь-яких умовах та сприятиме забезпеченню НАТО ширшими можливостями стримування та оборони [338].

НАТО розвиває співробітництво з кіберзахисту відповідно до Вказівок щодо співпраці з кіберзахисту з партнерами та міжнародними організаціями 2008 року та Рамкового документу щодо співпраці з кіберзахисту між НАТО та країнами-партнерами 2009 року, визнаючи необхідність визначення спільних підходів до використання сучасних систем захисту інформації з урахуванням вимог інформаційної безпеки. Забезпечення безпеки інформації в разі створення спільних інформаційних та телекомунікаційних систем, де циркулює інформація з обмеженим доступом, відбувається шляхом розроблення пропозицій щодо захисту конфіденційного зв'язку з використанням обладнання НАТО, необхідного для створення відокремлених інформаційно-комунікаційних систем в органах влади, а також підвищення кваліфікації їх фахівців з питань захисту інформації у рамках ПЗМ.

НАТО також усвідомлює необхідність посилення моніторингу критично важливих мереж у межах Альянсу та усунення виявлених недоліків. З цією метою талліннський Центр організує навчання та надає допомогу країнам-членам у поліпшенні програм кіберзахисту, а союзники мають розширювати свої засоби раннього попередження у формі загальної мережі моніторингових вузлів і сенсорів. НАТО застосовує процес оборонного планування задля сприяння розвитку можливостей кіберзахисту союзників, надання допомоги окремим країнам-членам та оптимізації обміну інформацією, співпраці та взаємосумісності [334]. У зв'язку з підвищенням небезпеки кібератак НАТО визначає вимоги для всіх країн, зацікавлених у збереженні цілісності, непорушності та конфіденційності їхнього інформаційного простору. Зокрема, інформаційна структура країн-членів Альянсу має постійно

вдосконалюватися, темпи розвитку новітніх інформаційних технологій та їх поширення мають прискорюватися. Потрібен також розвиток систем електронної сертифікації та криптографії, належна підготовка персоналу. Формування й реалізація єдиної державної політики в контексті забезпечення безпеки національних інтересів від загроз в інформаційній сфері має стати одним із пріоритетних напрямків розвитку кожної держави. Розвиток індустрії інформаційних та телекомунікаційних засобів, поширення їх на внутрішньому медіа-ринку, модернізація систем теле- і радіомовлення, оновлення технічної бази для забезпечення захисту інформації також є важливими заходами на шляху до забезпечення інформаційної безпеки.

Унаслідок нападів, спрямованих проти державних органів та здійснених за допомогою мережі Інтернет, увага НАТО поширилася на питання кіберзахисту окремих країн-членів. Альянс не виключає необхідності швидкого реагування на кібернетичні атаки шляхом надсилання групи експертів до будь-якої країни-члена, котра постраждала від кібернападу, або до країни, яка відчуває загрозу вторгнення у її інформаційний простір. Проте основну роль у захисті та безпеці власних комунікаційних систем продовжують відігравати самі союзники. Від них НАТО вимагає надійної та безпечної допоміжної інфраструктури, тому продовжуватиме працювати з національною владою над розробкою принципів і критеріїв забезпечення мінімального рівня кіберзахисту там, де національні мережі й мережі НАТО взаємопов’язані. З часом НАТО планує повністю забезпечити себе відповідним набором засобів кіберзахисту, включно з пасивними та активними елементами. З метою подолання ризиків безпеці, що виникають у кіберпросторі, НАТО також тісно співпрацює з іншими організаціями.

Проблема забезпечення інформаційної безпеки НАТО, крім питань технічного забезпечення й стратегічного планування, має також і політичний вимір. Передусім це стосується можливості застосування статті

5 Вашингтонського договору [339] до інформаційних атак. Основними протагоністами розширення дії принципу колективної відповідальності у сфері забезпечення інформаційної безпеки в системі НАТО виступають Естонія й, до певної міри, США. Зокрема, професор Дж. Голдгейєр відзначає, що за своїм визначенням кібератаки не є «збройним нападом», тобто не підпадають під дію ст. 5, однак робить висновок, що Альянс «має об'єднатися у протидії атакам, що загрожують безпеці будь-кого із членів НАТО» [340]. Варто зазначити, що питання протидії загрозам інформаційній безпеці, зокрема й кібербезпеці, відносять до сфери «м'якої безпеки» (soft security), тоді як головним завданням НАТО традиційно вважається протидія конвенційним викликам безпеки – забезпечення «жорсткої безпеки» (hard security) [341, с. 109]. Тому ще одним проблемним чинником, котрий проявляється на трансатлантичному рівні, є «поділ праці» між членами НАТО, внаслідок якого одні країни спеціалізуватися на темах «м'якої безпеки», а інші проводять «тверді» військові місії. Наслідком цього є розбіжність у підходах протидії: США, Франція, Велика Британія й Німеччина зіставляють інформаційну безпеку з військовою стратегією, натомість Естонія, котра не володіє потужним військовим потенціалом, наголошує на провідній ролі громадянського суспільства та приватного сектору [342].

4.2. Забезпечення інформаційної безпеки у нейтральних країнах Європи

Європейські держави, які умовно можна об'єднати під назвою «країни позаблокового статусу», належать до найрозвиненіших на континенті, в тому числі з точки зору темпів розвитку інформаційного суспільства, а також усвідомлення необхідності протидії кіберзагрозам, захист інформації та критичної інформаційної інфраструктури й інформаційно-

психологічної безпеки громадян та забезпечення інформаційної безпеки в цілому як складової національної безпеки. Тож, обравши євроінтеграційний курс, Україна має орієнтуватися на стратегію розвитку провідних європейських країн в інформаційній сфері [343, с. 18], критично оцінюючи та адаптуючи до власних реалій їх позитивний досвід у сфері забезпечення інформаційної безпеки. У цьому контексті корисним та цікавим убачається досвід таких країн, як Австрія, Швейцарія, Фінляндія та Ірландія, адже вони є успішним прикладом втілення в життя оптимальної моделі інформаційного суспільства, створення розвиненої інфраструктури інформаційних технологій та забезпечення високого рівня доступу населення до них [344, с. 35].

Із закінченням холодної війни біполярний світ став набагато складнішим, відтак втратила самостійну цінність концепція неприєднання, неучасті у військово-політичних союзах і т.п. Зокрема, позбулося свого безпосереднього змісту поняття нейтралітету, пов’язане з неучастю у війнах, тому такий статус ряду країн Європи залишається значною мірою даниною історичним традиціям. На сьогодні такі держави позначають як постнейтральні або позаблокові (буквально - неприєднані, non-aligned). Кожна із цих держав має власну історію нейтралітету, однак протягом останніх 20 років усі вони зіштовхнулися з проблемою доцільності збереження нейтрального статусу та з необхідністю запровадження тих або інших обмежень щодо нього. Аналогічна тенденція продовжує діяти й нині, оскільки міжнародні процеси й змістовне наповнення нових загроз, серед яких це і регіональні конфлікти, і міжнародний тероризм, і поширення зброї масового знищення, а також кіберзлочинність – вимагають від міжнародної спільноти узгоджених дій та масштабного співробітництва.

Особливе місце з-поміж країн позаблокового статусу посідає Швейцарія, котра не є ані членом НАТО, ані ЄС.

З 1992 року у Швейцарії діє Федеральний акт про захист даних, який

втілює загальноєвропейські принципи захисту інформації, в тому числі так званих «чутливих» відомостей та, зокрема, персональних даних [345]. У 2010 році Верховний суд Швейцарії надав додаткові гарантії конфіденційності персональних даних, підтримавши місцевого уповноваженого із захисту таких даних та ухваливши порядок, відповідно до якого збір інформації про IP-адреси користувачів файлообмінних мереж без їхньої згоди (в тому числі в контексті боротьби з порушеннями авторських прав) є незаконним [346].

У цілому забезпечення інформаційної безпеки електронних даних та інформаційних мереж здійснюється у Швейцарії відповідно до затвердженої у 2012 році Національної стратегії захисту від кіберризиків, метою якої визначено:

- раннє виявлення кіберзагроз і небезпек;
- підвищення стійкості критичної інфраструктури;
- ефективне зниження кіберризиків, зокрема кіберзлочинності, кібершпигунства й кіберсаботажу.

Передумовами для зниження кіберризиків при цьому вважається індивідуальна відповідальність та національне співробітництво між приватним сектором і органами влади, а також співпраця з іншими країнами. Держава має втручатися у процеси забезпечення кібербезпеки тільки тоді, коли суспільні інтереси перебувають під загрозою або якщо це відповідає принципу субсидіарності. Обробка кіберризиків має розглядатися як елемент процесів бізнесу, виробництва або управління, до яких мають бути інтегровані всі суб'єкти – від адміністративних і технічних рівнів до найвищого керівництва. Ефективний підхід до управління кіберризиками, заснований на принципі розподілу обов'язків між владою, приватним сектором і населенням, передбачає, що кожна організаційна одиниця (політична, економічна або соціальна) відповідає за те, щоб знати про кібер-аспекти та усувати інформаційні ризики, пов'язані з конкретними процесами, або по можливості зменшувати їх [347].

На початку 2018 року Швейцарія розпочала розробку закону про інформаційну безпеку, позаяк визнано, що незаконне використання інформації та втручання в роботу інформаційних систем може серйозно вплинути на істотні інтереси держави та права її громадян. Ґрунтуючись на загальновизнаних міжнародних стандартах, закон про інформаційну безпеку має забезпечити єдину формально-правову основу для контролю й упровадження інформаційної безпеки у сфері компетенції Федерального уряду Швейцарії. Закон стосується насамперед федеральних органів державної влади – парламенту, федеральних судів, федеральної прокуратури, національного банку та ін. Приватні особи й бізнес підпадають під дію закону тільки у разі провадження інформаційно «чутливої» діяльності за дорученням федеральних органів. Федеральна рада прагне також поглибити співробітництво з кантонами, які мають бути представлені у відповідному координаційному органі та брати участь у стандартизації відповідних заходів. Серед іншого закон регулює питання управління ризиками, класифікує інформацію й установлює принципи безпеки у сфері використання інформаційно-технічних ресурсів. Передбачається, що закон про безпеку інформації матиме пріоритет над законодавством про свободу інформації [348].

Убачається доцільним розглянути далі досвід забезпечення інформаційної безпеки європейських країн, які не є членами НАТО, однак є членами ЄС, на прикладі Австрії, Фінляндії та Ірландії. Передусім зазначимо, що членство в ЄС накладає на ці країни обов’язки щодо дотримання стандартів цієї організації стосовно розвитку інформаційного суспільства та забезпечення інформаційної безпеки. Так, ще 1991 року було розроблено «Європейські критерії безпеки інформаційних технологій» [349], де, зокрема, визначено завдання забезпечення інформаційної безпеки:

- захист інформаційних ресурсів від несанкціонованого доступу з метою забезпечення конфіденційності;

- забезпечення цілісності інформаційних ресурсів шляхом їх захисту від несанкціонованої модифікації або знищення;
- забезпечення працездатності систем за допомогою протидії загрозам відмови в обслуговуванні.

У 1996 році стандарти європейської інформаційної безпеки було втілено у «Єдиних критеріях безпеки інформаційних технологій» [350].

2001 року Європейська Комісія оприлюднила документ під назвою «Мережева та інформаційна безпека: європейський політичний підхід», в якому окреслено сучасне бачення ЄС проблематики інформаційної безпеки [351] та, зокрема, визначено такі засади європейської політики інформаційної безпеки:

підвищення обізнаності користувачів щодо можливих загроз під час користування комунікаційними мережами;

створення європейської системи попередження та інформування про нові загрози;

забезпечення технологічної підтримки;

підтримка ринково орієнтованої стандартизації та сертифікації;

правове забезпечення, пріоритетами якого є захист персональних даних, регламентація телекомунікаційних послуг та протидія кіберзлочинності;

зміцнення інформаційної безпеки на державному рівні шляхом упровадження ефективних і сумісних засобів забезпечення інформаційної безпеки та заохочення використання країнами-членами електронних підписів під час надання державних онлайн послуг тощо;

розвиток міжнародного співробітництва з питань інформаційної безпеки.

В Австрії, Фінляндії та Ірландії, як і в інших країнах ЄС, значна увага приділяється проблемам кібербезпеки, окресленим у Документі Європейської комісії «На шляху до загальної політики у сфері боротьби з кіберзлочинністю», де остання визначається як кримінальні дії, вчинені з

використанням електронних комунікаційних мереж та інформаційних систем або проти таких мереж та систем, а саме:

- традиційні форми злочину (шахрайство та підробки в електронних комунікаційних мережах та інформаційних системах);
- публікації незаконного контенту в електронних медіа;
- специфічні злочини в електронних мережах (атаки на інформаційні системи, хакерство тощо) [352].

Основними викликами безпеці інформаційних інфраструктур зазначених країн, як і ЄС в цілому, є:

- некоординовані внутрішньодержавні підходи до безпеки інформаційних інфраструктур, що знижує ефективність національних заходів;
- відсутність на європейському рівні партнерства між державним та приватним секторами;
- обмежені можливості щодо раннього попередження та реагування на безпекові інциденти, зумовлені нерівномірністю розвитку систем моніторингу і сповіщення про інциденти у країнах-членах, нерозвиненістю міждержавного співробітництва та обміну інформацією щодо цих проблем;
- відсутність міжнародного консенсусу щодо пріоритетів у реалізації політики захисту критичної інформаційної інфраструктури [353].

Вагомим елементом інформаційної безпеки усіх без винятку країн ЄС є захист персональних даних, засади якого визначені директивою 95/46/ЄС «Про захист фізичних осіб у контексті обробки персональних даних і вільного обігу таких даних» [354]. Обов’язкові для країн-членів ЄС нові правила захисту персональних даних (GDPR), які схвалено 14 квітня 2016 року, для Австрії, Фінляндії та Ірландії набувають чинності у 2018 році. У документі переглянуто цивільні права користувачів, відповідальність за

схоронність даних, а також запроваджено деякі обмеження на переміщення даних між різними країнами. Важливим нововведенням убачається також запровадження більш суворого покарання за несвоєчасне повідомлення інформації про виток даних [355].

Одним із лідерів ЄС за показниками розвитку інформаційного суспільства справедливо вважають Фінляндію, адже в рейтингу країн Євросоюзу вона утримує першість за рівнем цифрової грамотності (понад 50 % населення) й посідає друге місце за показником поширення мережі широкосмугового зв'язку (34 % населення) [356].

Головними державними інституціями, відповідальними за розробку та реалізацію політики інформаційної безпеки, є Міністерство транспорту та комунікацій Фінляндії, Омбудсмен з питань захисту даних (Data Protection Ombudsman). До повноважень Міністерства транспорту та комунікацій належить розробка законодавства щодо комунікаційних мереж, безпеки даних, забезпечення доступу до комунікаційних послуг, а також розробка й реалізація національної політики у сфері інформаційної безпеки.

Структурним підрозділом Міністерства транспорту та комунікацій є Управління Фінляндії з регулювання комунікацій (Finnish Communications Regulatory Authority – FICORA), до компетенції якого входить контроль та державне регулювання у сфері інформаційно-комунікаційних технологій. До повноважень FICORA належить:

- контроль за функціонуванням електронних комунікаційних мереж;
- інформування про можливі загрози інформаційній безпеці;
- підвищення обізнаності громадян з питань інформаційної безпеки;
- планування й управління використанням радіочастот, мережевими адресами, а також контроль за змістом програм і реклами на телебаченні та радіо.

У структурі FICORA функціонує CERT-FI (Computer Emergency

Response Team of Finland) – фінська комп'ютерна група швидкого реагування, основним завданням якої є попередження, виявлення та реагування на кіберінциденти, а також поширення інформації про загрози інформаційній безпеці [357]. У забезпеченні інформаційної безпеки активну участь бере також громадянське суспільство. Серед неурядових організацій, що опікуються проблематикою інформаційної безпеки, провідна роль належить Фінській федерації комунікацій та телеінформатики (Finnish Federation for Communications and Teleinformatics – FiCom) та Фінській асоціації з питань інформаційної безпеки (Finnish Information Security Association - FiSA). FiCom здійснює планування і координацію заходів щодо розвитку інформаційно-комунікаційних технологій, моніторинг ситуації в ІКТ-секторі, бере участь у регулюванні ринку інформаційно-комунікаційних технологій тощо. Натомість метою FiSA є розвиток професіоналізму й обізнаності у сфері інформаційної безпеки. Діяльність асоціації включає організацію дискусій, конференцій, участь у різних програмах з інформаційної безпеки [358]. У 2015 році компанія CGI відкрила у Фінляндії центр інформаційної безпеки, завданням якого є відстеження кібератак [359].

Стратегія національної безпеки Фінляндії, зазначаючи, що критична інфраструктура країни все більше залежить від інформаційних систем та мереж, передбачає мінімізацію відповідних ризиків важливим завданням забезпечення всеосяжної безпеки. Концепція всеосяжної безпеки, окрім традиційного сценарію протидії військовим загрозам, охоплює також інші проблеми на кшталт зміни клімату, дефіциту енергетичних та водних ресурсів, міграції, тероризму, торгівлі наркотиками, кібератак тощо [360].

Стратегія кібербезпеки Фінляндії, затверджена у 2013 році, наголошує на тому, що загрози, які виходять з кіберпростору, стають усе більш серйозними, адже кібератаки можуть використовуватися як інструмент політичного й економічного тиску, в тому числі в комплексі із традиційними військовими засобами. При цьому кіберпростір – це джерело

величезного потенціалу та ресурсів, позаяк збільшує можливості розвитку бізнесу, працевлаштування та залучення іноземних інвесторів. Стратегія також визначає, що Фінляндія як невелика й відкрита до співробітництва країна має «відмінні шанси піднятися до авангарду кібербезпеки». Бачення кібербезпеки полягало в такому:

- країна спроможна забезпечити свої життєво важливі функції і протистояти кіберзагрозам у всіх ситуаціях;
- громадяни, органи влади та юридичні особи можуть ефективно використовувати безпечний кіберпростір, що виникає завдяки заходам кібербезпеки, здійснюваних на національному й міжнародному рівнях;
- до 2016 року Фінляндія має стати провісником повної готовності до протидії кіберзагрозам та управління порушеннями, що викликані цими загрозами.

Якщо розслідування кіберінцидентів здійснює поліція, то організація всеосяжного кіберзахисту покладається на Сили оборони Фінляндії під проводом Міністерства оборони. Потенції військового кіберзахисту включають розвідку, кібератаки та ведення кібервійн, однак головним вектор військової потуги в кіберпросторі спрямований на інтелектуальне попередження загроз [361]. Зауважимо, що 2015 року Міністерство внутрішніх справ Фінляндії ініціювало оновлення закону про розвідувальну діяльність з метою надання поліції та військовим права на розвідку в інформаційних мережах [362].

Фінська модель інформаційного суспільства має яскраво виражену соціальну спрямованість з поєднанням динамічної взаємодії бізнесу й суспільством за активної посередницької ролі держави. При цьому держава залишає за собою дві функції: управління розвитком та дерегулювання [363]. До переліку її основних завдань входить створення національної інформаційної інфраструктури з метою сприяння підвищенню рівня поінформованості населення країни. Саме тому ще з 2003 року уряд

Фінляндії в рамках Стратегії кібербезпеки здійснює заходи з інформування громадян країни про методи і способи захисту від негативного інформаційного впливу.

Варто також відзначити, що в 2013 році уряд Фінляндії затвердив національну Стратегію інформаційної безпеки, яка окреслила такі пріоритети [364]:

– створення національного центру інформаційної безпеки для комплексного збору та аналізу даних, загальної ситуаційної обізнаності, а також національного та міжнародного співробітництва;

– удосконалення управління загрозами та ефективністю обслуговування стратегічно важливих інформаційних систем;

– підвищення базових знань населення та бізнесу у сфері інформаційної безпеки шляхом надання конфіденційних і безпечних мережевих сервісів та послуг;

– розробка і здійснення професійної підготовки на всіх рівнях з метою зміцнення інформаційної безпеки;

– інвестування в міжнародне співробітництво та участь у міжнародній науково-дослідній діяльності, орієнтованій на інформаційну безпеку.

Як бачимо зі змісту основних пріоритетів Стратегії інформаційної безпеки Фінляндії, усі вони розроблені відповідно до принципів, за якими побудована модель національного інформаційного суспільства [365, с. 35].

Що стосується Австрійської Республіки, то програми становлення інформаційного суспільства в цій країні втілюють політичну стратегію об’єднання Європи на базі новітніх технологій, інформаційно-комунікаційної інфраструктури та інтелектуального потенціалу регіону. На інформаційну політику Австрії значний вплив чинять міжнародні організації, що мають резиденції у Відні, складовою програм діяльності яких є розвиток інформаційного суспільства. У Плані дій Уряду Австрії передбачено такі напрями інформаційної інтеграції країни, як:

- координація трансформації інформаційного сектору;
- створення відповідних державних інституцій з регулювання ринку інформаційних технологій;
- стимулювання виробництва інформаційних продуктів та послуг;
- підтримка лідерства Австрії в галузі електронних технологій, зокрема виробництва мікрочипів та інтегрованих електронних схем;
- лібералізація торгівлі інформаційними продуктами й послугами; розвиток електронної комерції;
- сприяння торгівлі інноваційними технологіями з третіми країнами;
- створення об'єднаних мереж австрійських та європейських центрів прикладних досліджень інформаційного суспільства;
- використання потенціалу міжнародних організацій;
- наукова кооперація (на паритетних засадах);
- розробка проектів для соціальної сфери, освіти, охорони здоров'я, екології;
- міжнародне співробітництво за гуманітарними напрямами.

Стратегія кібербезпеки Австрії зазначає, що звичайні військові напади на країну в найближчій перспективі малоймовірні, натомість для Австрійської Республіки та ЄС в цілому все більшої актуальності набувають нові проблеми, ризики й загрози. Це, насамперед:

- міжнародний тероризм;
- поширення зброї масового знищення;
- внутрішні й регіональні конфлікти або заворушення, які стосуються Європи або мають глобальні наслідки;
- «відмова держави»; природні або техногенні катастрофи;
- кібератаки;
- загрози для стратегічної інфраструктури;

- транснаціональна організована злочинність;
- торгівля наркотиками, корупція, незаконна міграція;
- безуспішна інтеграція;
- брак ресурсів (енергія, продовольство, вода тощо), зміна клімату, екологічна шкода й пандемії;
- піратство й загрози транспортним маршрутам, а також наслідки міжнародної фінансово-економічної кризи у сфері безпеки [363].

Напади з кіберпростору становлять безпосередню загрозу безпеці й належному функціонуванню державного апарату, економіки, науки й суспільства. Недержавні суб'єкти (приміром, злочинці, учасники організованих злочинних угруповань або терористи), а також державні суб'єкти (скажімо, секретні служби й військові) можуть зловживати можливостями кіберпростору у своїх власних цілях і перешкоджати його належному функціонуванню. Як загрози в кіберпросторі, так і його продуктивне використання практично не лімітовані. Тому головним пріоритетом Австрії є забезпечення безпеки й кібербезпеки на національному й міжнародному рівнях. Всеосяжна політика кібербезпеки означає, що зовнішня й внутрішня безпека, а також усі аспекти цивільної й військової безпеки тісно пов'язані та взаємозалежні. Забезпечення кібербезпеки виходить за межі компетенції традиційних органів безпеки й потребує залучення інструментів багатьох інших сфер безпекової політики. Інтегрована політика кібербезпеки має наголошувати на поділі завдань між державою, економікою, науковими колами й громадянським суспільством, включаючи заходи у таких напрямах:

- політико-стратегічне управління;
- оцінювання ризиків;
- запобігання загрозам та забезпечення готовності;
- визнання й реагування, обмеження наслідків і відновлення;
- розвиток урядових і неурядових можливостей.

Політика кібербезпеки має бути проактивною, що означає роботу із

запобігання загрозам кіберпростору й людні в кіберпросторі або пом'якшення їх впливу («налаштування безпеки»). Політика кібербезпеки також має бути заснована на принципі солідарності, позаяк через глобальний характер кіберпростору кібербезпека Австрії, ЄС і всього світового співтовариства дуже взаємозалежна. Тому для забезпечення кібербезпеки потрібне інтенсивне співробітництво на спільній основі на європейському й міжнародному рівні [364].

Стратегієя кібербезпеки Австрії національним координатором і центральним органом у сфері кібербезпеки визначила Центр боротьби з кіберзлочинністю Федерального міністерства внутрішніх справ (Cyber Crime Competence Center (C4) of the Federal Ministry of the Interior). Крім того, на нього покладено головні функції щодо здійснення правоохоронної діяльності у сфері кібербезпеки та боротьби з кіберзлочинністю [366, с. 79]. Федеральне міністерство внутрішніх справ Австрії, до складу якого входить вказаний Центр, є органом з контррозвідувальними функціями, що виконує завдання із забезпечення державної безпеки. Це, зокрема, – боротьба з тероризмом, політичним екстремізмом, незаконною міграцією, протидія злочинам проти конституційного ладу та основ державної безпеки [367].

Ірландію, де розташовані великі європейські офіси таких компаній, як Google і Facebook, часто називають європейською Силіконовою долиною, оскільки ця країна докладає багато зусиль для підготовки та працевлаштування IT-фахівців. У 2013 році компанія Microsoft проінвестувала 170 мільйонів євро у створення та розвиток європейського дата-центру в Ірландії. Ця ініціатива була підтримана місцевою владою, адже Ірландія прагне стати європейським лідером у сфері обробки big data, а її кліматичні умови підходять для підтримки необхідної температури роботи серверів [368]. Кім того у Дубліні створюється тренінговий центр, котрий, як планується, у щільній співпраці з урядом та навчальними

закладами країни проводитиме навчання в таких перспективних галузях, як захист критичної інфраструктури й кібербезпека транспорту [369].

Національна стратегія кібербезпеки Ірландії на 2015-2017 роки передбачала, що уряд всіляко сприятиме стійкій та безпечній експлуатації комп'ютерних мереж і відповідної інфраструктури ірландськими громадянами й підприємствами. Розвиток і поширення інформаційно-комунікаційних технологій посприяв вагомому поліпшенню якості життя, появі інноваційних послуг та радикальним змінам в організації бізнесу. Відтак, держава, критична інфраструктура, юридичні особи й громадяни залежать від надійного функціонування інформаційно-комунікаційних технологій та Інтернету. Порушення роботи цих систем, яким би джерелом воно не було спричинене, створює безпосередню загрозу функціонуванню державного механізму й економіки, може відчутно вплинути на повсякденне життя мільйонів громадян. Тому на будь-яку загрозу безпеці кіберпростору потрібне своєчасне, надійне й послідовне реагування як на національному, так і на міжнародному рівні. З цією метою уряд Ірландії намітив виконання відповідними суб'єктами країни таких завдань:

підвищити стійкість і надійність критично важливої інформаційної інфраструктури в найважливіших секторах економіки, особливо в державному;

продовжувати взаємодію з міжнародними партнерами, аби кіберпростір залишався відкритим, безпечним, цілісним і безкоштовним, а також здатним сприяти економічному та соціальному розвитку;

підвищувати обізнаність про відповідальність бізнесу та приватних осіб з питань забезпечення безпеки своїх інформаційних мереж, інфраструктури та даних, а також підтримувати таку обізнаність за допомогою інформації, навчання та узагальнення практики;

забезпечувати для державних органів всеосяжні та гнучкі нормативно-правові рамки для боротьби з кіберзлочинністю, які були би доречними й домірними із потребами захисту «чутливих» чи особистих даних;

створювати потенціал для органів влади і приватного сектору для функціонування та аварійного управління в умовах кіберінцидентів.

4.3. Досвід правового забезпечення інформаційної безпеки у країнах Європейського Союзу

Вивчення практики європейських країн у побудові влсних моделей правового забезпечення інформаційної безпеки, протидії кіберзагрозам, а також аналіз ряду міжнародних правових документів дає змогу нам резюмувати про відсутність єдиної моделі національної системи правового забезпечення інформаційної безпеки

Визначившись із зовнішньополітичним курсом, Україна має орієнтуватися першочергово на стратегію розвитку країн-учасниць Європейського Союзу в інформаційній сфері [343, с. 18]. При цьому, з огляду на геополітичне положення України, її провідним орієнтиром мають стати передусім країни Центральної Європи, адже саме вони є успішним прикладом втілення в життя оптимальної моделі інформаційного суспільства шляхом створення розвиненої інфраструктури інформаційних технологій з унікально високим рівнем доступу населення до них, випереджаючи за цим показником інші країни світу [344, с. 35].

Аналіз, оцінка та використання позитивних здобутків європейських країн мають важливе значення при розбудові системи забезпечення інформаційної безпеки в Україні, оскільки, як зазначають В.Шатун та О.Гладун [36, с. 179], події останніх років у нашій державі показали неспроможність влади адекватно протистояти інформаційним війнам, позаяк проблеми інформаційної політики досі не вирішені на належному рівні.

Питання щодо умовних кордонів Центральної Європи наразі лишається дискусійним. Традиційно до країн Центральної Європи

відносять Німеччину, Ліхтенштейн, Австрію, Швейцарію та деякі інші. Утім, де-факто до них належать й учасники Вишеградської групи – Угорщина, Польща, Чехія та Словаччина [370], а також частина країн Балканського півострова. Зважаючи на те, що питання інформаційної безпеки у країнах позаблокового статусу доцільно розглянути окремо, наразі зосередимося на забезпеченні інформаційної безпеки у Німеччині, Польщі, Угорщині та Хорватії [371].

Передусім зауважимо, що Федеративна Республіка Німеччини, Угорська Республіка, Республіка Польща та Республіка Хорватія є членами Організації Північноатлантичного договору та Європейського Союзу. Відповідно, на них поширюються стандарти цих міжнародних організацій щодо інформаційної політики та забезпечення інформаційної безпеки. Це, зокрема, стандарти НАТО щодо захисту інформації, викладені у Документі CM (2002)49 «Безпека в Організації Північноатлантичного договору (НАТО)» [316], офіційна політика НАТО у сфері кіберзахисту [372], стратегічна концепція кібербезпеки, сформульована на Лісабонському саміті [330] й уточнена за результатами Варшавського саміту [338], та ін.

Активну політику у сфері забезпечення інформаційної безпеки проводить не лише НАТО, але й ЄС, який сьогодні об’єднує розвинуті країни, котрі відчутно впливають на міжнародні відносини, встановлюючи норми і стандарти поведінки держав у політичній, економічній, соціальній, інформаційній та інших сферах. 1991 року було розроблено «Європейські критерії безпеки інформаційних технологій», де, зокрема, визначено завдання забезпечення інформаційної безпеки, а саме:

- захист інформаційних ресурсів від несанкціонованого доступу з метою забезпечення конфіденційності;
- забезпечення цілісності інформаційних ресурсів шляхом їх захисту від несанкціонованої модифікації або знищення;
- забезпечення працездатності систем за допомогою протидії загрозам відмови в обслуговуванні.

У 1996 році стандарти європейської інформаційної безпеки було втілено у «Єдиних критеріях безпеки інформаційних технологій» [373], де застосовано модель тріади CIA (CIA Triad), яка передбачає такі основні характеристики інформаційної безпеки:

1) конфіденційність;
2) цілісність;
3) доступність [103, с. 43].

У документі Європейської Комісії «Мережева та інформаційна безпека: європейський політичний підхід» (2001 р.), визначено базові засади Співтовариства до проблеми забезпечення інформаційної безпеки. Термінологічне сполучення «мережева та інформаційна безпека» трактується як здатність мережі або інформаційної системи чинити опір випадковим подіям або зловмисним діям, котрі становлять загрозу доступності, автентичності, цілісності та конфіденційності даних, що зберігаються або передаються, а також послуг, які надаються через ці мережі й системи [374]. Згаданий документ визначає такі пріоритетні напрями європейської політики забезпечення інформаційної безпеки:

- підвищення обізнаності користувачів щодо можливих загроз під час користування комунікаційними мережами;
- створення європейської системи попередження та інформування про нові загрози;
- забезпечення технологічної підтримки;
- підтримка ринково орієнтованої стандартизації та сертифікації;
- правове забезпечення, пріоритетами якого є захист персональних даних, регламентація телекомунікаційних послуг та протидія кіберзлочинності;
- зміцнення інформаційної безпеки на державному рівні шляхом упровадження ефективних і сумісних засобів забезпечення інформаційної безпеки та заохочення використання країнами-членами електронних підписів під час надання державних

онлайн послуг тощо;

- розвиток міжнародного співробітництва з питань інформаційної безпеки.

У всіх без винятку країнах ЄС питаням правового забезпечення інформаційної безпеки надається особлива увага. При цьому першочергового значення набувають питання протидії кіберзагрозам, які є складовими процесу забезпечення інформаційної безпеки. З 1999 року реалізуються програми «Безпечніший Інтернет» (Safer Internet), у рамках яких здійснюються заходи, спрямовані на боротьбу не лише зі шкідливим контентом, але й з небезпечною поведінкою в мережі [375].

Процес формування європеського глобальної системи правового забезпечення інформаційної безпеки має тривалий характер. Ще в 2007 році Європейська Комісія прийняла документ «На шляху до загальної політики в сфері боротьби з кіберзлочинністю». У даному документі, хоча й на рівні декларації, визначено кіберзлочини як кримінальні дії, вчинені з використанням електронних комунікаційних мереж та інформаційних систем або проти таких мереж та систем, котрі включають: традиційні форми злочину (шахрайство та підробки в електронних комунікаційних мережах та інформаційних системах); публікацію незаконного контенту в електронних медіа; специфічні злочини в електронних мережах (атаки на інформаційні системи, хакерство тощо) [377].

Дещо пізніше, у 2009 році у Повідомленні Європейської Комісії «Захист Європи від широкомасштабних кібератак та руйнувань: посилення рівня підготовленості, безпеки та стійкості» були визначені головні виклики тапроблеми, які потребують першочергового реагування зі сторони країн ЄС, а також окреслило основні заходи щодо посилення безпеки та здатності європейської критичної інформаційної інфраструктури протистояти зовнішнім впливам [378]. Відповідно до даного документу засадничними викликами безпеці інформаційної безпеки країн ЄС є:

- некоординовані національні підходи до безпеки інформаційних інфраструктур, що знижує ефективність національних заходів;
- відсутність на європейському рівні партнерства між державним та приватним секторами;
- обмежені можливості щодо раннього запобігання та реагування на безпекові інциденти, зумовлені нерівномірністю розвитку систем моніторингу і сповіщення про інциденти у країнах-членах, нерозвиненістю міждержавного співробітництва та обміну інформацією щодо цих проблем;
- відсутність міжнародного консенсусу стосовно пріоритетів у реалізації політики захисту критичної інформаційної інфраструктури.

Окрім зазначеного, важливим аспектом правового забезпечення інформаційної безпеки у рамках ЄС є питання інформаційної відкритості органів державної влади країн учасниць. Системоутворюючою тезою даного аспекту є: «…загальновизнано, що демократична система може функціонувати найбільш ефективно лише у разі, коли громадськість повністю поінформована» [312, с. 110]. У даному ракурсі слід також послатися і на рекомендації Ради Європи № R(81)19 «Про доступ до інформації, яка перебуває в розпорядженні державних органів». У даному документі відмічено, що для гарантування адекватної участі всіх у суспільному житті необхідно забезпечити, з урахуванням неминучих винятків та обмежень, доступ громадськості до інформації, що перебуває в розпорядженні державних органів усіх рівнів [379]. Першочергово значення тут набувають питання захисту персональних даних.

З цього приводу, у резолюції Генеральної Асамблеї ООН «Право на приватність у цифрову епоху» від 18 грудня 2013 року визначено глобальну й відкриту природу Інтернету і швидкий розвиток у сфері інформаційних та комунікаційних технологій як рушійної сили для прискорення прогресу на шляху до розвитку в різних формах. У документі

підтверджено, що «ті ж права, що люди мають в офф-лайн-режимі, мають також бути захищені онлайн, у тому числі право на приватність» [380]. Засади захисту персональних даних у правовій практиці країн ЄС можна звести до такого:

пріоритетність права особи розпоряджатися своїми персональними даними;

використання персональних даних без дозволу володільця тягне відповідальність згідно з законодавством;

для будь-кого, хто здійснює користування персональними даними фізичних осіб з їхнього дозволу, встановлено відповідальність у разі умисного розголошення цих даних третім особам (крім випадків, коли на це надано дозвіл) [381; 382, с. 5-6].

Попри згадані документи ЄС про захист персональних даних, основним серед них слід вважати директиву 95/46/ЄС «Про захист фізичних осіб у контексті обробки персональних даних і вільного обігу таких даних» [383]. У ньому декларується прагнення до вільного переміщення інформації між країнами-членами ЄС та одночасно надаються гарантії захисту основних прав громадян, до яких належить і право на недоторканність особистих даних та їх захист від третіх осіб. Директива ЄС зобов'язує кожну державу-члена прийняти свої національні закони про захист приватних відомостей, які відповідали б рекомендаціями OECD 1980 року. З-поміж цих рекомендацій варто відзначити «Принцип гарантованої безпеки N11» [384], який вимагає, аби «персональні дані були захищені розумними засобами безпеки від таких загроз, як утрата чи неавторизований доступ, руйнування, використання, модифікація або розголошення».

Обов'язкові для країн-членів ЄС нові правила захисту персональних даних (GDPR), які ухвалено 14 квітня 2016 року, набувають чинності у 2018 році. Ці правила поширюватимуться не лише на європейські компанії, але й на суб'єктів інших країн, які пропонують товари й послуги в ЄС. У

документі переглянуті цивільні права користувачів, відповідальність за схоронність даних, а також запроваджено деякі обмеження переміщення даних між країнами.

Слід констатувати, що країни ЄС сформували «в певному сенсі злагоджену систему захисту інформації» [385, с. 129], але водночас кожна країна має свої закони, положення, інструкції щодо врегулювання питань інформаційної безпеки.

Така, для Німеччини характерна детальна нормативно-правова розробка системи різних видів інформації з обмеженим доступом, чіткі формулювання їх визначень у федеральному законодавстві. Приміром, відповідно до закону «Про перевірку безпеки» [386] секретною інформацією вважаються факти, вироби та відомості, незалежно від форми їх представлення, які в державних інтересах мають зберігатися в таємниці та яким наданий державним органом чи за його дорученням ступінь секретності, котрий відповідає необхідному рівню захисту:

- «цілком таємно»;
- «таємно»;
- «конфіденційно»
- «для службового користування».

До системи секретної інформації належить державна таємниця (відомості з грифом «цілком таємно» і «таємно») та відомча таємниця (відомості з грифом «конфіденційно» і «для службового користування»), охорона яких, на відміну від інших видів таємниць, що стосуються конфіденційної сфери приватних осіб, зумовлена інтересами зовнішньої безпеки держави. Зокрема, особливо важливою та такою, що підлягає особливому захисту, вважається конфіденційна інформація про етнічне походження, політичні погляди, релігійні та філософські переконання, членство в об’єднаннях, здоров’я і статеве життя фізичних осіб.

У жовтні 1997 року в Німеччині ухвалено Акт захисту інформації в телекомунікаціях (TDPA) [387]. Відповідно до його загальних принципів

збирання, обробка та використання інформації допускається лише у випадках, коли це дозволено законом або здійснюється за згодою користувача. Інформація може бути зібрана, оброблена або використана лише окремо для різних послуг, яких потребує один і той самий користувач, причому згода останнього не є умовою для надання послуг.

Крім того, з 2005 року в Німеччині діє так званий «Акт про свободу інформації», який регламентує питання доступу до неї [388]. Нагляд за виконанням положень цього нормативного акта покладено на комісара із захисту інформації та персональних даних. У країні від 1990 року діє також закон про доступ приватних осіб і дослідників до архівів «Штазі» – служби безпеки колишньої НДР [389].

Федеральна служба інформаційної безпеки (BSI) є головним органом на який покладено обов'язки по забезпеченню інформаційної безпеки країни. BSI входить до Федерального міністерства внутрішніх справ, яке, серед інших функцій:

- забезпечує внутрішню безпеку і захист конституційного ладу Німеччини;
- здійснює боротьбу з тероризмом, екстремізмом, шпигунством і саботажем.

Відповідно до закону «Про Федеральне відомство безпеки інформаційних систем» BSI збирає та оцінює інформацію стосовно загроз кібербезпеці держави, виявляє нові типи кібератак, аналізує відповідні контрзаходи [390]. На BSI покладається також виконання таких функцій у взаємодії з НАТО та ЄС:

- оцінка ризику впровадження інформаційних технологій;
- розробка критеріїв, методів та випробних засобів для оцінки ступеня захищеності національних комунікаційних систем;
- перевірка ступеня захищеності інформаційних систем і видача відповідних сертифікатів;

- видача дозволів на впровадження інформаційних систем у важливі державні об’єкти;
- здійснення спеціальних заходів безпеки інформаційного обміну в державних органах, поліції тощо;
- консультування представників промисловості з питань інформаційної безпеки.

Крім того, відомство провадить заходи з пропаганди необхідності забезпечення інформаційної безпеки [391].

З метою оптимізації оперативного співробітництва між усіма державними установами та поліпшення координації заходів із протидії кібератакам у ФРН на базі Федерального відомства безпеки інформаційних систем створено національний центр кіберзахисту (NCAZ), який безпосередньо взаємодіє з іншими суб’єктами кібербезпеки країни, у тому числі з приватним сектором, країнами-партнерами з ЄС, НАТО, а також міжнародними організаціями [366, с. 78].

Питаннями забезпечення інформаційної безпеки Німеччини в межах своєї компетенції опікуються також Федеральне бюро захисту конституції (BFV) [392] та Управління інформаційних операцій, створене 2009 року у структурі бундесверу через масовані атаки на обчислювальні мережі державних структур ФРН у лютому 2009 року. Наприкінці 2010 року в рамках реалізації концепції кіберзахисту у структурі командування бундесверу остаточно завершене також формування підрозділу інформаційних і комп’ютерних мережевих операцій, який від 5 квітня 2017 року функціонує як «Сили кібернетичного та інформаційного простору Німеччини». До завдань зазначеного підрозділу входить, зокрема:

- розробка нових методів кібератак;
- проникнення в комп’ютерні мережі іноземних держав і організацій з метою отримання розвідувальних даних;
- проведення операцій деструктивного впливу на мережі й автоматизовані системи або блокування їх роботи [393].

Аналіз відкритих джерел щодо політки інформаційнох безпеки Німеччини здає змогу зробити нам висновок, що серед пріоритетів протидії кіберзагрозам, Німеччина обрала тактику так званої «активної оборони». Виділення наступальної складової інформаційного протиборства і створення відповідної окремої структури є, за оцінками німецьких експертів, адекватною відповіддю на сучасні загрози інформаційній безпеці Німеччини.

Подібна тактика забезпечення інформаційної безпеки успішно діє і у Франції, де 17 липня 2014 року на рівні законодавчого акту визначено глобальну політику безпеки інформаційних систем [394]. Даним правовиим актом вустановлено правила захисту державних інформаційних систем, та пріортетні механізм протидії кіберзагрозам на рівні держави. Дещо пізніше, а саме 27 березня 2015 року, вийшов Декрет № 2015-351, де уряд Франції сформулював нові положення безпеки інформаційних систем операторів галузей, роль яких має критичне значення для життєдіяльності нації [395].

Наведені вище законодавчі кроки яскраво підтверджують, що у країнах Центральної Європи питанням інформаційної безпеки приділяється особлива увага.

Що стосується подібної практики наших ближчих сусідів, зокрема Польщі, зазначимо, національна інформаційна політика Республіки Польща концептуально зорієнтована на розвиток вільного відкритого суспільства, забезпечення основоположних прав людини та громадянина, впровадження концепції вільного транскордонного обігу інформації, створення незалежних і плюралістичних мас-медіа. Правовим втілення польської концепції інформаційної безпеки є прийняті у 1990-х роках «Закон про пошту і телекомунікації», «Закон про телебачення і радіомовлення», «Закон про державні відносини з римською католицькою церквою в Республіці Польща», де визначено напрями інформаційної політики, встановлюються технологічні стандарти інформаційного зв’язку,

форми залучення іноземних інвестицій (33%-49% зарубіжного капіталу), ліцензування інформаційної діяльності. Окремо виписано права церкви на інформаційну діяльність, з огляду на значний вплив клерикальної інформації на політичні пріоритети та моральність польського суспільства [396; 397, с. 114].

Основні функціональні повноваження у забезпеченні кібернетичної безпеки Польщі покладено на Агентство внутрішньої безпеки (ABW). У 2013 році за участю даного органу розроблено Стратегію кібербезпеки Польщі та створено при Міністерстві національної оборони Центру криптології, на який покладено завдання із захисту інформації, кібероборони та проведення наступальних кібероперацій [398]. ABW також сформувало урядову команду реагування на комп'ютерні інциденти (CERT) [399], головним завданням якої є забезпечення і розвиток можливостей органів державного управління щодо захисту від кіберзагроз. Зокрема, це стосується захисту від атак на інфраструктуру, що складається з IT-систем та комп'ютерних мереж, порушення роботи або руйнація яких може значною мірою загрожувати життю і здоров'ю людей, національним багатствам та навколишньому середовищу або призвести до значних фінансових збитків і збоїв у функціонуванні органів державної влади [400]. Під керівництвом ABW у 2015 році розроблена й Доктрину кібербезпеки Польщі, яка оперує ключовими поняттями теорії безпеки на кшталт «загроз», «викликів», «ризиків» тощо [401].

У 2015 році у Польщі розпочато роботу над Доктриною інформаційної безпеки. З-поміж загроз інформаційній безпеці у Доктрині названі, наступні:

ескалація напруження у міжнародних стосунках;

дискредитація польської міжнародної політики і формування негативного іміджу країни на міжнародній арені, в тому числі й серед союзників по НАТО та ЄС;

формування образу Польщі як країни ксенофобів та антисемітів;

провокування польсько-литовського конфлікту на тлі польської меншини в Литві;

підбурювання польсько-українського конфлікту на складному історичному тлі з можливим застосуванням терористичних замахів, які буцімто могли би здійснити українці проти поляків чи навпаки.

Доктрина інформаційної безпеки Польщі розглядається як виконавчий документ до Стратегії національної безпеки [402; 403].

Важливим аспектом, який доречно й розвивати в українських реаліях, є залучення у Польщі до боротьби з інформаційними загрозами громадянське суспільство. Зокрема успішним прикладом такої діяльності є створена у 2018 році неурядова організація - Центр аналізу пропаганди і дезінформації. Даний Центр займається виявленням і протидією російській пропаганді. Вказана фундація є першою такого роду інституцією у Польщі, діяльність якої спрямовуватиметься на аналіз і пошук системного підходу до ідентифікації та протидії російській дезінформації в польському інформаційному просторі. Окрім науково-дослідної й аналітичної роботи, Центр співпрацюватиме з іншими суб'єктами, аби закласти фундамент розуміння у польському суспільстві загроз, позаяк інформаційна і психологічна війна проникає у різні сфери життєдіяльності суспільства й держави [403].

Іншою особливістю правовго забезпечення інформаційної безпеки у Польщіта й ряді інших країн Східної Європи, є безпосередній вплив на політику держави в інформаційній сфері вступ до НАТО. Це спонукало країни до приведення у відповідність до стандартів НАТО національне інформаційне закнодавство. Прикладом цього можна назвати прийнятий у січні 1999 року закон «Про захист конфіденційної інформації», ухвалення якого було однією з умов вступу Польщі до НАТО [396]. Іншим прикладом такого процесу є прийнятий у 1995 році закон Угорщини про державні та офіційні секрети у [404, с. 155].

У цілому ж угорська політика у сфері забезпечення інформаційної

безпеки налаштована переважно на обмеження. Так, закон про засоби масової інформації (2010) викликав критику з боку світових медіа та ЄС - Угорщину звинуватили в запровадженні тотального контролю за ЗМІ, включно з Інтернетом, у ліквідації свободи слова, ба навіть у прагненні встановити тоталітарний режим. Європейський парламент ухвалив резолюцію [405] (вперше стосовно країни – члена ЄС) із засудженням того, як угорський уряд ставиться до демократії, свободи слова, прав людини. Згодом парламент Угорщини вніс косметичні поправки до цього закону, які втім не торкнулися ключових питань (структури управління угорськими ЗМІ), але були сприйняті ЄС позитивно [406, с. 11-12].

Угорщина стала першою із постсоціалістичних країн, котра прийняла «Закон про захист інформації про особу та доступ до інформації, що становить суспільний інтерес» (1992), яким, зокрема, запроваджено інститут Парламентського комісара із захисту інформації та свободи інформації [407]. Відповідно до цього закону особу, чиї персональні дані обробляються, належить повністю поінформувати про мету цих дій. Допускається збір виключно тих даних, які необхідні для досягнення вказаної мети, а зберігатися вони можуть лише протягом терміну, допоки мета не буде досягнута. Кожному надається право діставати доступ до своєї персональної інформації та в разі потреби вимагати її виправлення або знищення. Особливий захист передбачено для так званих «чутливих» (sensitive) даних, які стосуються «расового походження, національності й етнічного статусу, політичних думок чи партійної приналежності, релігійних чи інших переконань» або «відомостей про хвороби, сексуальне життя чи судимості». Крім того, правове підґрунтя забезпечення інформаційної безпеки в частині захисту персональних даних в Угорщині становлять закони «Про право на інформаційне самовизначення та свободу інформації» (2011) та «Про обробку і захист медичної інформації та пов’язаних з нею персональних даних» (1997). З будь-яких питань, пов’язаних із захистом персональних даних, особа може звернутися до

Національного бюро із захисту даних та свободи інформації [408].

Правове забезпечення інформаційної безпеки Угорщини, в т.ч. кібербезпеки, втілено у законі «Про електронну інформаційну безпеку державних та муніципальних органів» (2013) [409] та п. 31 Стратегії національної безпеки Угорщини, затвердженої у 2012 році [410]. Стратегія національної безпеки, зокрема, передбачає, що держава має бути готова управляти ризиками й загрозами, пов'язаними з національною безпекою, обороною, боротьбою проти злочинності, а також запобігати нештатним ситуаціям у кіберпросторі, гарантувати адекватний рівень кібербезпеки й виконувати інші завдання, пов'язані із забезпеченням кібербезпеки. При цьому основним завданням визнається систематичне визначення пріоритетів у сфері потенційних загроз і ризиків у кіберпросторі, а також підвищення поінформованості суспільства щодо них. Відповідні положення дістали подальшого розвитку в Національній стратегії кібербезпеки Угорщини, затвердженій 2013 року [411].

Досить цікави є досвід правового забезпечення інформаційної безпеки держави у Хорватії. У цій країні ще з 2007 року діє Акт про інформаційну безпеку [412]. Цим законодавчим актом визначені поняття інформаційної безпеки, її елементи, заходи забезпечення і стандарти, а також функціональні компетентності органів для прийняття й реалізації рішень у сфері протидії загрозам та забезпеченні інформаційної безпеки держави, а також нагляду за дотриманням відповідних стандартів.

У 2015 році в Хорватії прийнято національну стратегію кібербезпеки [413], яка базується на таких основних принципах:

- усебічність підходу до кібербезпеки, що охоплює кіберпростір, інфраструктуру й користувачів відповідно до хорватської юрисдикції (громадянство, реєстрація, домен, адреса);
- інтеграція заходів у різних сферах забезпечення кібербезпеки;
- проактивність завдяки постійному коригуванню заходів та періодичному уточненню їх стратегічних кордонів;

- зміцнення стійкості, надійності й керованості шляхом застосування універсальних критеріїв конфіденційності, цілісності й доступності певних груп інформації та соціальних цінностей;
- захист прав і свобод людини у кіберпросторі, передусім – конфіденційності та власності;
- постійне вдосконалення правової бази;
- субсидіарність при розподілі повноважень; відповідність витрат на забезпечення кібербезпеки ступеню ризику тощо.

Стратегія кіберзахисту є частиною стратегії оборони, що є сферою відповідальності Міністерства оборони Хорватії. Кібертероризм, кіберзлочинність та деякі інші кібернетичні аспекти національної безпеки розглядаються також компетентними органами у системі безпеки й розвідки, як такі, що потребують спеціального підходу.

Слід зазначити, що забезпечення інформаційної безпеки, в тому числі шляхом активних інформаційних операцій, наприкінці минулого століття стало важливим компонентом боротьби Хорватії за свої тимчасово окуповані території, де понад чотири роки існувала сепаратистська «Республіка Сербська країна». При цьому, за оцінками експертів, якщо в мілітарному значенні боротьба за повернення вказаних територій закінчилася у серпні 1995 року під час операції «Буря», в дипломатичному – на початку 1998-го, водночас із мирною реінтеграцією хорватського Подунав’я, то в інформаційному сенсі війна закінчилася лише через 15 років після закінчення бойових дій [414].

Важливою складовою забезпечення інформаційної безпеки держави є міжнародна діяльність України у контексті широкого висвітлення подій, які гостро торкаються питань основних її складових. Аналіз міжнародного інформаційного простору дає підстави стверджувати, що Україна стала об’єктом інформаційних атак (інформаційно-психологічних акцій), спрямованих га встановлення контролю над усіма сферами існування

незалежної держави. Нерозуміння важливості проведення з боку України акцій інформаційного впливу задля підтримки наших національних інтересів і державної політики за кордоном, як засвідчують останні події, завдає державі величезних економічних, політичних, іміджевих та інших збитків.

Російська Федерація, наприклад, не обмежується проведенням інформаційних атак на українське населення. Через мережу російського мовлення за кордоном – потужну систему інформаційного впливу – вона проводить інформаційні операції для формування негативного іміджу нашої держави.

Прикладом успішності інформаційної експансії Росії можуть слугувати результати опитування «Як бачать в ЄС війну на сході України», яке американська компанія TNS проводила 3−8 вересня 2015 р. у восьми країнах – членах ЄС: Великобританії, Іспанії, Італії, Нідерландах, Німеччині, Польщі, Франції і Швеції. Зокрема, 53% опитаних європейців вважають, що в Україні відбувається громадянська війна. Серед тих, хто сприймає події в Україні як громадянську війну, найбільша частка німців (61%), італійців (59%) та голландців (58%). Менше підтримують це визначення британці та французи (42%). На жаль, навіть у Польщі більшість респондентів підтримала тезу про громадянську війну в Україні, хоч поляків найбільше і серед тих, хто не погоджується із цим твердженням (36%). З офіційною версією України, що в державі триває антитерористична операція, погоджується лише третина респондентів (з них лише 8% цілком згодні з цією думкою). 20−24% респондентів взагалі не знають, що відбувається на сході України [415].

Такі цифри засвідчують непідготовленість України до інформаційного протистояння зовнішньополітичним впливам. Однією з причин цього може бути те, що в нашій державі на інституційному рівні забезпеченням окремих напрямів інформаційної безпеки опікується низка органів державної влади, зокрема Міністерство інформаційної політики,

Національна рада України та Державний комітет з питань телебачення й радіомовлення, Національна комісія державного регулювання у сфері зв'язку та інформатизації, МЗС України, МВС України, СБ України, Державна служба спеціального зв'язку та захисту інформації, МО України, СЗР України тощо. Проте, всі вони виявилися неготовими з об'єктивних і суб'єктивних причин до протидії сучасним викликам і загрозам. Проблема в тому, що жоден із державних органів, які беруть участь у забезпеченні інформаційної безпеки України, не відповідає за незадовільний стан протидії інформаційній агресії через відсутність суб'єкта юридичної координації зусиль забезпечення національної безпеки в інформаційній сфері. Кожен виконує виключно свою функцію, не знаючи, що роблять інші відомства в цій сфері.

Британський тижневик The Economist розглядає тему збройного протистояння на сході України у статті під заголовком «Україна і Росія разом у пастці війни на Донбасі». Автор пояснює, що замість відкритої повномасштабної агресії проти України Кремль «створив образ громадянської війни, абсурдно зображуючи київський уряд «фашистським» режимом, а сепаратистів «борцями за свободу» [416].

Американський аналітичний центр The Atlantic Council у публікації під заголовком «Це суперечить здоровому глузду, але озброєння України насправді заощадить гроші платників податків США» пише про те, що існує п'ять основних причин, чому американці мають насправді бути зацікавлені у наданні Вашингтоном озброєння Україні.

По-перше, читаємо у статті, «ми захищаємо наші інтереси та союзників, допомагаючи Україні захистити себе». «Кожен український солдат, який бореться за свою країну, означає на одного американця менше, необхідного для захисту Європи», – пише автор допису.

По-друге, продовжує він, ця війна безпосередньо стосується США та Європи, адже «Москва, по суті, оголосила війну Європі та міжнародному порядку». «Наразі Росія веде інформаційну війну проти кожного

європейського уряду від країн Балтії до Іспанії. Москва відкрито субсидує політичні партії по всій Європі в спробі підірвати демократичні уряди», – зауважено у статті.

В ній пояснюється, що без надання України допомоги, щоб вона могла захистити себе, вплив Росії поширюватиметься, і «тоді Східна Європа буде жити в тіні війни, етнополітичної напруженості й всюдисущої реальності територіальних ампутацій». Цитуючи слова співробітника Фонду Карнеґі Шермана Ґарнетта, автор вказує, що «Україна є наріжним каменем у дузі європейської безпеки», а отже, якщо залишити Україну напризволяще, то «її поразка чи розпад потягне за собою розпад європейської безпеки».

По-третє, нагадав автор, у 1994 році США гарантували безпеку України в обмін на її відмову від ядерної зброї.

По-четверте, стверджується, що попередні нереалізовані спроби допомоги Україні заохотили Росію до ще більшої ескалації агресії з боку Росії, у той час як підтримка Києва з боку Заходу може врешті змусити Росію шукати політичного врегулювання чи повернутися до виконання своїх зобов'язань за Мінськими угодами.

По-п'яте, оскільки США є найсильнішою державою у світі, то Вашингтон не може просто заплющити очі на агресію, особливо ж агресію з участю ядерної держави. Залишення Києва віч-на-віч із агресором може призвести до вигідних фінансових оборудок із Росією чи риторичної підтримки боротьби з тероризмом, але це відчиняє двері до нового терору постійної війни, читаємо в публікації на сайті американської аналітичної установи [417].

За результатами проведених наукових досліджень [418], нині першочергової уваги потребують такі *ключові загрози національній та міжнародній безпеці в інформаційній сфері*:

– глобальні зміни і трансформації в інформаційній сфері формують новітні виклики і загрози, які становлять реальну загрозу безпеці людства та міжнародному правопорядку;

– в інформаційному просторі спостерігається тенденція до поширення інформаційної агресії і насилля, маніпуляції свідомістю людини та суспільства, періодично проводяться інформаційно-психологічні операції;

– більшість країн світу зіштовхнулася з проблемами кібершпигунства, кібертероризму, кіберзлочинності та кібератаками на об'єкти критичної інфраструктури;

– наслідки використання сучасної інформаційної зброї можуть призводити до реальної втрати державного суверенітету і територіальної цілісності країн світу.

Окрім проведеного аналізу, важливим убачається й досвід інших країн Європейського простору, які проходять аналогічний шлях євроінтеграції. Тож дослідження, оцінка та імплементація позитивних набутків цих країн мають неабияке значення при розбудові системи забезпечення інформаційної безпеки в Україні, оскільки події останніх років у нашій державі показали, що ми поки що не готові належним чином вести інформаційні війни, а політика у сфері забезпечення інформаційної безпеки та інформаційна політика загалом потребують удосконалення [36, с. 179].

Для нас, як країни яка заявила про свої наміри Євроінтеграції та членства в НАТО, цікави є досвід Румунії й Болгарії як членів НАТО та Європейського Союзу. Першочергово тому, що в цих країнах вже апробовані і діють стандарти ЄС та НАТО щодо інформаційної політики та правового забезпечення інформаційної безпеки. Зокрема, це стандарти НАТО щодо захисту інформації, викладені у Документі СМ (2002)49 «Безпека в організації Північноатлантичного договору (НАТО)» [316], офіційна політика НАТО у сфері кіберзахисту [327; 325], стратегічна концепція кібербезпеки, сформульована за результатами Лісабонського [330] й уточнена за результатами Варшавського самітів [338], та ін. Як члени ЄС ці країни втілюють також у національній політиці забезпечення інформаційної безпеки стандарти ЄС, в тому числі передбачені

«Європейськими критеріями безпеки інформаційних технологій» (1991) [349], «Єдиними критеріями безпеки інформаційних технологій» (1996) [350], документами «Мережева та інформаційна безпека: європейський політичний підхід» (2001) [351] і «На шляху до загальної політики у сфері боротьби з кіберзлочинністю» (2007) [352] та ін. Аналіз згаданих міжнародних документів дає змогу виокремити пріоритетні напрямами забезпечення інформаційної безпеки у цих країнах:

- підвищення обізнаності користувачів щодо можливих загроз під час користування комунікаційними мережами;
- створення європейської системи попередження та інформування про нові загрози;
- забезпечення технологічної підтримки;
- підтримка ринково орієнтованої стандартизації та сертифікації;
- правове забезпечення, пріоритетами якого є захист персональних даних, регламентація телекомунікаційних послуг та протидія кіберзлочинності;
- зміцнення інформаційної безпеки на державному рівні шляхом упровадження ефективних і сумісних засобів забезпечення інформаційної безпеки та заохочення використання країнами-членами електронних підписів під час надання державних онлайн послуг тощо;
- розвиток міжнародного співробітництва з питань інформаційної безпеки.

Основними викликами інформаційній безпеці Румунії та Болгарії як членів ЄС є:

- некоординовані національні підходи до безпеки інформаційних інфраструктур, що знижує ефективність національних заходів;
- відсутність на європейському рівні партнерства між державним та приватним секторами;
- обмежені можливості щодо раннього попередження та

реагування на безпекові інциденти, зумовлені нерівномірністю розвитку систем моніторингу і сповіщення про інциденти у країнах-членах, нерозвиненістю міждержавного співробітництва та обміну інформацією щодо цих проблем;

- відсутність міжнародного консенсусу щодо пріоритетів у реалізації політики захисту критичної інформаційної інфраструктури [353].

Попри зазначені пріоритети важливо значення на рівні законодавства надається захисту персональних даних. У Директиві 95/46/ЄС «Про захист фізичних осіб у контексті обробки персональних даних і вільного обігу таких даних» декларується прагнення до вільного переміщення інформації між країнами-членами ЄС та надаються гарантії захисту основних прав громадян, до яких належить право на недоторканність особистих даних та їх захист від третіх осіб [354; 384].

Важливим нововведенням є також запровадження більш суворого покарання за несвоєчасне повідомлення інформації про витік даних. Компаніям, що порушили положення нової директиви й не доповіли про факт витоку або злому протягом 72 годин з моменту виявлення інциденту, загрожує штраф до 4% річного доходу або до 20 млн. євро [419]. Крім того, відповідна Директива передбачає необхідність отримання згоди користувачів на обробку їхніх персональних даних, причому на обробку даних з різними цілями потрібні окремі згоди. Згода має бути вільною, свідомою і конкретною, а також може бути відкликана в будь-який момент. Згода не буде вважатися вільною, якщо користувач змушений її дати, щоб одержати доступ до сайту, програми або додатка. Винятком є випадки, коли персональні дані користувача потрібні для виконання угоди. У тому разі, коли персональні дані збираються й обробляються для маркетингових цілей, користувач повинен мати можливість не погоджуватися зі збором і обробкою його даних. Компанії, що працюють із персональними даними, мусять також вести облік операцій з

персональними даними (тип даних і мета їх обробки), мінімізувати використання персональних даних відповідно до принципу data protection by design, а також проводити внутрішній аудит [420].

У Румунії теж досить суворий підхід до даного питання. Так, у Румунії в теперішній час триває активний процес розбудови системи кібернетичної безпеки держави як на законодавчому, так і на організаційному рівнях. При цьому ключова роль у забезпеченні кібербезпеки Румунії відводиться її спеціальному контррозвідувальному органу – Румунській службі інформації, у структурі якої створено національний центр кібербезпеки [366, с. 79]. Головною функцією цього центру є поєднання систем технічного захисту із можливостями спецслужби з метою отримання інформації, необхідної для попередження, припинення та подолання наслідків кібератак на інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури держави [421]. Законопроект «Про кібербезпеку», який у грудні 2014 року був схвалений сенатом Румунії, передбачає також створення Національної системи кібернетичної безпеки Румунії, технічну координацію якої покладено на Румунську службу інформації як головного суб'єкта забезпечення кібербезпеки держави [422].

Особливу увагу Національна стратегія забезпечення кібербезпеки Румунії (2013) приділяє розвитку національних можливостей щодо управління ризиками у сфері кібернетичної безпеки [423].

Пункт 4.7.3 Стратегії передбачає створення механізмів і технічних ресурсів для постійного моніторингу можливих загроз кібербезпеці з точки зору масштабів, джерел і природи (кібер-, гібридні), тенденцій у геополітичному контексті й аналізу національної картини кібербезпеки, а також розвитку здатності застосовувати адекватні форми протидії, зокрема підтримувати створення джерел контр-інформаційних впливів [424].

Систему протидії кіберзлочинності Молдови, попри критику науковцями країни політики держави із забезпечення інформаційної

безпеки у [425], можна вважати відносно надійною. Так, ще 2009 року парламент цієї країни ратифікував Конвенцію Ради Європи про кіберзлочинність [426]. Крім того, у березні 2012 року Молдова підписала Другий додатковий Протокол до Європейської Конвенції про взаємну допомогу у кримінальних справах [427]. Ухвалено також закон «Про попередження та боротьбу зі злочинністю у сфері комп'ютерної інформації» (січень 2010 року) [428]. Згідно із цим законом генеральна прокуратура Молдови наділена повноваженнями координувати та здійснювати кримінальне переслідування осіб, що вчинили кіберзлочини. Метою закону є вдосконалення регламентації правовідносин за такими напрямами: запобігання та боротьба з кіберзлочинністю, сприяння провайдерам і користувачам інформаційних систем, співробітництво державних служб із неурядовими організаціями та іншими представниками громадянського суспільства, а також міжнародне співробітництво з організаціями та країнами, що мають досвід у відповідних питаннях. Генеральна прокуратура з метою сприяння розслідуванням відкрила Центр розслідування кіберзлочинів, один з відділів якого уповноважений реагувати на випадки загроз безпеці в урядових структурах, бізнесі та громадському секторі.

Окрім зазначеного у Молдові здійснено ряд важливих заходів на шляху зміцнення національної інформаційної безпеки. Зокрема, у результаті ратифікації Факультативного протоколу до Конвенції ООН про права дитини, що стосується торгівлі дітьми, дитячої проституції та порнографії [429], Конвенції Ради Європи про кіберзлочинність [430] і Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства [431] Молдова стала активним учасником процесу застосування загальної кримінальної політики у сфері боротьби з інформаційною злочинністю, у тому числі злочинами, пов'язаними із онлайн-експлуатацією дітей.

Іншим важливим заходом на національному рівні стало прийняття

закону «Про електронний підпис та електронний документ» (29 травня 2014 року), розробленого з метою підвищення рівня безпеки електронних підписів та приведення у відповідність із міжнародними стандартами й рекомендаціями щодо інфраструктури відкритих ключів [432]. Загалом слід зауважити, що у Молдові розпочато процес приведення чинного законодавства у відповідність до положень Директиви 2006/24/ЄС від 15 березня 2006 року про зберігання інформації, створеної або обробленої при наданні послуг зв'язку загального користування або мереж зв'язку загального користування, й унесення змін до директив ЄС про захист персональних даних 2002/58/ЄС [433] і 2008/114/ЄС від 8 грудня 2008 року про ідентифікацію й призначення європейських критичних інфраструктур та оцінку необхідності поліпшення їх захисту [434] та ін.

У Молдові в 2013 році прийнято Національну стратегію розвитку інформаційного суспільства «Moldova digitală 2020» («Цифрова Молдова 2020») і План дій з її впровадження, розроблений Міністерством інформаційних технологій та зв'язку [435]. У Стратегії вперше розглядається проблема створення умов для підвищення ступеня безпеки й довіри до кіберпростору, а ключові дії щодо створення цих умов становлять окрему главу вищезгаданого Плану дій. Стратегія визначає, що використання нових технологій породжує багато можливостей для розвитку, але й численні ризики й уразливості, що потребують підвищеної уваги держави й зацікавлених учасників. Ці ризики характеризуються асиметрією, вираженою динамікою та глобальним характером, що ускладнює їхнє виявлення і протидію за допомогою заходів, пропорційних ефектові їхньої матеріалізації. Таким чином, попередження кібератак і боротьба з ними, у тому числі зі злочинністю в цій сфері, є одним із пріоритетів міжнародних організацій, а бурхливий ріст числа кібератак на світовому рівні (на 600% з 2005 року) вказує на нагальну необхідність вжиття заходів щодо страхування інформаційної інфраструктури Республіки Молдова від можливих ризиків, пов'язаних із незаконною

діяльністю у цій сфері. Важливість цієї проблеми була підкреслена в Концепції національної безпеки та Стратегії національної безпеки Республіки Молдова, де визначено цілі системи забезпечення національної безпеки та загрози у інформаційній сфері [435].

На думку експертів, останні ініціативи щодо регламентації інформаційного простору містять цілу низку серйозних прогалин, які можуть призвести до зловживань. Зокрема, Концепцію інформаційної безпеки доцільно узгодити із новою Стратегією національної безпеки, однак останній проект Стратегії національної безпеки в червні 2017 року був відкликаний з парламенту президентом, а новий проект досі не розроблений. Крім того, проект Концепції передбачає надто суворий контроль Інтернету з боку деяких державних установ, зокрема Служби інформації та безпеки Республіки Молдова, які зможуть втручатися в діяльність провайдерів, а також контролювати інформаційний простір, включаючи соціальні мережі [436].

Цікавим є досвід Білорусії, де нагляд за інформаційним простором та система обмежень є наразі ключовими елементами державної інформаційної політики. З 2010 до 2015 року у країні діяла постанова Оперативно-аналітичного центру при президентові і Міністерства зв'язку та інформатизації Республіки Білорусь від 29.06.2010 №4/11 «Про затвердження Положення про порядок обмеження доступу користувачів інтернет-послуг до інформації, забороненої до поширення відповідно законодавчих актів». Постанова приписувала провайдерам фільтрувати інтернет-контент відповідно до двох чорних списків url-адрес, один із яких перебував у публічному доступі, а інший був доступний тільки провайдерам (закритий список містив приблизно 80 url-адрес, доступ до яких державних, культурних і урядових закладів обмежувався, і містив популярні опозиційні сайти на кшталт Charter97.org і Belaruspartisan.org) [437]. У теперішній час відповідні обмеження реалізуються відповідно до указу президента Білорусі від 1 лютого 2010 року № 60 «Про заходи щодо

вдосконалення використання національного сегменту мережі Інтернет», декрету президента від 28 грудня 2014 року «Про невідкладні заходи з протидії незаконному обігу наркотиків» та закону Республіки Білорусь від 17 липня 2008 року «Про засоби масової інформації» [438].

У березні 2010 року від білоруських провайдерів зажадали більш щільного співробітництва з державними системами спостереження (СОРМ), які здійснюють повний онлайн-нагляд по всій країні, що регламентується значною кількістю нормативно-правових актів. Як і в Росії та сусідніх країнах, СОРМ Білорусі з метою боротьби зі злочинністю дає виконавчим органам і органам національної безпеки можливість перехоплювати повідомлення з будь-яких комунікаційних каналів. Провайдери інтернет-послуг і оператори зв'язку зобов'язані встановлювати відповідне устаткування й надавати державним органам цілодобовий доступ до нього. Відповідно до указу «Про заходи щодо вдосконалення використання національного сегменту мережі Інтернет» № 60 [439] провайдери мусять вести облік Ір-адрес, а держава може витребувати інформацію щодо інтернет-діяльності будь-якого громадянина. З 2007 року до інтернет-кафе висувається вимога зберігати історію інтернет-активності користувачів протягом року й інформувати виконавчі органі про підозрілі дії [440]. СОРМ працює здебільшого відповідно до законів «Про оперативно-розшукову діяльність» [440], «Про органи державної безпеки Республіки Білорусь» [441] та указу № 129 «Про затвердження Положення про порядок взаємодії операторів електрозв'язку з органами, що здійснюють оперативно-розшукову діяльність» [442].

У Білорусі немає спеціальних законів, присвячених протидії кіберзлочинності, але деякі аспекти регулюються Кримінальним кодексом і законами, що стосуються регламентації діяльності глобальної інформаційної мережі Інтернет. Білорусь також подавала заявку на приєднання до Конвенції про кіберзлочинність, прийнятої в Будапешті в 2012 році [444], що й визначило необхідність дотримуватися відповідних

міжнародних стандартів. Такий крок Білорусі став вельми несподіваним, особливо в контексті їхніх тісних зв'язків з Росією, адже Китай і РФ виступили проти конвенції й висловилися на захист альтернативної концепції боротьби з кіберзлочинністю, за якою держава отримує значно більше повноважень, ніж це передбачається Будапештською конвенцією.

Розслідуванням комп'ютерних злочинів у Білорусі опікується спеціальне управління Міністерства внутрішніх справ, яке координує роботу з іншими виконавчими органами усередині країни й аналогічними міжнародними організаціями у США, Євросоюзі, країнах СНД та в інших державах. У суспільстві висловлюються непоодинокі підозри, що це управління займається переважно переслідуванням кримінальних правопорушників, а ніяк не розробкою законодавства з питань кібербезпеки, а також бере участь у переслідуванні та онлайн-відстеженні політичних активістів [442].

Що стосується участі Республіки Білорусь у забезпеченні кібербезпеки на регіональному рівні, то слід зауважити, що Рада голів держав Співдружності Незалежних Держав у 2013 році прийняла Концепцію співробітництва держав-членів СНД у боротьбі зі злочинами, що вчиняються з використанням інформаційних технологій [443]. Відповідно до цього документа країни-члени СНД обмінюються робочою, статистичною й методологічною інформацією та ведуть єдину базу даних щодо кіберзлочинців. На підставі цієї Концепції з 2015 року здійснюється розробка програми співробітництва між країнами СНД у боротьбі з кіберзлочинністю, яка підлягає затвердженню Радою міністрів країн СНД. Також у 2017 році розпочато підписання нової Угоди про співробітництво держав-членів СНД у боротьбі зі злочинами у сфері інформаційних технологій [444].

Висновки до розділу 4

У теперішній час одним із ключових чинників державної політики України чітко визначено вступ до НАТО. З метою набуття членства в Альянсі Україна активізує зусилля з усього комплексу реформ, у тому числі у безпековому та оборонному секторах. Ураховуючи, що саме інформаційна безпека є наразі одним із найважливіших аспектів забезпечення національної, регіональної та міжнародної безпеки в цілому, наша країна має запровадити достатньо заходів перестороги та процедур для її гарантування відповідно до положень політики НАТО у цій сфері, а також дотримати умов, зафіксованих у плані дій Україна – НАТО. Це, зокрема, передбачає:

- забезпечення реалізації гарантій доступу до інформації;
- імплементацію відповідного законодавства для усунення перешкод діяльності ЗМІ;
- поглиблення інформаційного виміру співпраці Україна-НАТО, включаючи парламентське співробітництво;
- створення прозорої та гнучкої структури електронного урядування;
- забезпечення розвитку спроможностей військових частин і підрозділів інформаційних операцій;
- підвищення рівня обізнаності громадськості щодо діяльності НАТО;
- підвищення рівня забезпечення інформаційної безпеки, кібербезпеки тощо.

Аналіз, оцінка та використання позитивних здобутків європейських країн мають важливе значення при розбудові системи забезпечення інформаційної безпеки України, адже нині наша країна стикається з новими викликами та загрозами в інформаційній сфері та перебуває на

стадії становлення інформаційного суспільства, яка супроводжується стрімким розвитком інформаційної інфраструктури.

Сьогодні нейтральні країни цілком усвідомлюють безпосередню залежність свого добробуту від інформаційної сфери, відтак, питання забезпечення інформаційної безпеки закономірно посідає одне з чільних місць у безпекових стратегіях відповідних держав. При цьому політика забезпечення інформаційної безпеки позаблокових країн має проактивний характер і спирається на засади управління ризиками інформаційної безпеки, передусім – кібербезпеки.

Досвід зміни парадигми забезпечення національної безпеки з реактивної на проактивну для України у контексті її євроінтеграційних спрямувань є надзвичайно важливим, адже дозволяє правильно визначати стратегічні пріоритети та оптимізувати зусилля щодо забезпечення інформаційної безпеки, а також сприятиме плідному співробітництву з усіма європейськими країнами у розбудові систем регіональної та міжнародної інформаційної безпеки. Не менш важливим є цей досвід і для подальшої розбудови теорії національної безпеки та наукових засад забезпечення інформаційної безпеки. Зокрема, до перспективних напрямів подальшого наукового пошуку належить передусім дослідження у сфері оцінювання загроз інформаційній безпеці України та методів управління ризиками в інформаційній сфері.

Проблеми забезпечення інформаційної безпеки особи, суспільства, держави, їх захисту від різного виду загроз, як зовнішніх, так і внутрішніх, посідають нині одне з чільних місць у пріоритетах державної політики та стратегіях забезпечення національної безпеки країн Центральної Європи, які у цьому питанні орієнтуються насамперед на стандарти ЄС та НАТО. Відповідні зразки мають становити орієнтир і для України на шляху нашої держави до реалізації своїх євроінтеграційних спрямувань.

Для України як держави, що зіштовхнулася із проблемами втягнення у гібридну війну та тимчасової окупації окремих територій, стане,

безперечно, у пригоді й досвід країн Центральної Європи у забезпеченні інформаційної безпеки. Це зокрема, стосується Хорватії, протидія сепаратизму в якій закінчилась успішною реінтеграцією самопроголошеної «республіки». Таким чином, нам слід брати на озброєння передові методи протидії російській інформаційній агресії, постійно подавати якісний інформаційний продукт на тимчасово окуповані території. Доцільним убачається також упровадження досвіду Німеччини щодо переходу в забезпеченні інформаційної безпеки до принципу «активної оборони», адже інформаційна безпека держави становить перманентний процес діяльності компетентних органів, спрямований на запобігання, протидію загрозам в інформаційній сфері, застосування активних заходів інформаційного впливу, а також сукупність умов такої діяльності, які реалізуються й здатні контролюватися тривалий час.

Крім того, Україна має приєднатися до інших європейських країн у розбудові системи міжнародної інформаційної безпеки з метою протидії загрозам стратегічній стабільності, таким як кібертероризм та кіберзлочинність. Співробітництво з країнами Центральної Європи у сфері формування системи міжнародної інформаційної безпеки відповідає національним інтересам України і сприяє зміцненню її національної безпеки.

Країни Східної Європи вважають вирішення проблем забезпечення інформаційної безпеки особи, суспільства, держави, їх захисту від внутрішніх та зовнішніх, у тому числі гібридних загроз, одним із найбільших стратегічних пріоритетів забезпечення національної безпеки.

Україна має співробітничати з іншими країнами Східної Європи у розбудові систем регіональної та міжнародної інформаційної безпеки з метою протидії загрозам стратегічній стабільності, таким як кібертероризм і кіберзлочинність, орієнтуючись при цьому на стандарти ЄС та НАТО.

У цьому контексті для України важливим є досвід країн Східної Європи щодо приведення національного законодавства у відповідність до

вимог вказаних міжнародних організацій, передусім – щодо забезпечення балансу між свободою та безпекою в інформаційній сфері на законодавчому рівні.

На сучасному етапі інформаційно-комунікаційні технології зазнають мілітарного впливу, що дедалі зростає. Зважаючи на реалії сьогодення, не складно спрогнозувати подальше вдосконалення методів ведення інформаційно-психологічної війни і розширення сфер застосування відповідних технологій, що на глобальному рівні може суттєво позначитися на стратегічному балансі сил і спричинити зміни в нинішніх критеріях його оцінки на основі співвідношення геополітичних, економічних і військових чинників. Складність ідентифікації джерел інцидентів в інформаційному просторі й неузгодженість поглядів щодо того, які заходи у зв'язку із цим є прийнятними, створюють ризик неадекватної оцінки загрози, а отже, підвищують імовірність виникнення конфлікту й завдання шкоди тій чи іншій сфері життєдіяльності держави (держав). З огляду на це актуальними загрозами у сфері інформаційної безпеки є наразі такі:

– зростання ймовірності застосування ІКТ у майбутніх конфліктах з огляду на нарощування ІКТ-потенціалу для військових, розвідувальних потреб і в політичних цілях, до якого вдається низка держав. При цьому різний рівень можливостей країн щодо забезпечення безпеки у сфері ІКТ, що нині має місце, в умовах взаємопов'язаного світу підвищує уразливість державних утворень з меншим ІКТ-потенціалом;

– можливість нападів з використанням ІКТ на критично важливі об'єкти інфраструктури та пов'язані з ними інформаційні системи держав;

– можливість застосування ІКТ зі злочинними намірами для здійснення терористичних атак на об'єкти ІКТ або пов'язану з ними інфраструктуру;

– імовірність глобальних загроз для миру й безпеки через використання ІКТ у терористичних цілях для вербування прихильників,

забезпечення фінансування терористичних атак, навчання членів терористичних угруповань та ін.;

– значна неоднорідність зловмисних недержавних суб'єктів (включно зі злочинними угрупованнями й терористами), їхніх мотивів тощо;

– швидкоплинність зловмисних нападів у сфері ІКТ і наявність значної кількості шкідливих інструментів і методів, якими послуговуються хакери, причому ІКТ-арсенал зловмисників невпинно вдосконалюється і стає ефективнішим;

– можливість використання ІКТ для пропаганди, підривної діяльності, обміну, збору, передачі інформації, в тому числі впровадження шкідливих програм для підриву довіри до певних державних, недержавних, комерційних структур, окремих програм, товарів, послуг і т. ін.

На міжнародному рівні занепокоєння державних суб'єктів викликають спроби встановити контроль над глобальним інформаційним простором за допомогою ІКТ. При цьому особливої ваги набуває питання поваги до прав людини й забезпечення основних свобод в інформаційній сфері. Водночас дотримання цих прав і свобод не має суперечити двом найважливішим принципам міжнародного права - невтручання у внутрішні справи держав і поваги до національного суверенітету.

Виходячи з вищевикладеного, можна визначити основні напрями міжнародної діяльності щодо забезпечення міжнародної інформаційної безпеки (МІБ):

- створення на національному і глобальному рівнях умов для розробки, виробництва і впровадження засобів забезпечення МІБ;
- організація ефективного міжнародного співробітництва у сфері ІКТ;

- спільна боротьба з кіберзлочинністю та інформаційним тероризмом;
- забезпечення захисту ІКТ від шкідливого впливу і зменшення потенційної шкоди від атак на інформаційні системи;
- удосконалення кадрового забезпечення та організаційних заходів, методик навчання фахівців і проведення наукових досліджень у галузі інформаційної та кібербезпеки;
- захист громадської безпеки, державних структур і бізнесу у сфері ІКТ;
- міжнародна діяльність щодо запобігання конфліктам в інформаційному просторі на противагу підходам, які передбачають їх легітимізацію;
- захист інформації та засобів її обробки для успішної реалізації складних сценаріїв на всіх рівнях;
- усебічне дослідження питань використання ІКТ у конфліктах і застосовуваності міжнародного права до дій держав в інформаційному просторі.

Відповідно до цього наступні кроки, спрямовані на зміцнення довіри та зниження ризику неадекватного сприйняття ситуації в разі дезорганізації або порушень, пов’язаних із застосуванням ІКТ, мають передбачати:

1. Продовження міждержавного діалогу щодо норм державного використання ІКТ для зменшення колективних ризиків і захисту критичної національної та міжнародної інфраструктури.
2. Розроблення і впровадження дієвих заходів для зміцнення довіри, підвищення рівня глобальної стабільності у сфері ІКТ, включно з обміном на державному рівні думками з приводу наслідків державного використання ІКТ і застосування їх у конфліктах.

3. Міждержавний обмін інформацією про національні закони, стратегії, технології, принципи й передові методи забезпечення інформаційної безпеки.
4. Визначення переліку заходів щодо сприяння створенню потенційних умов для забезпечення інформаційної безпеки у країнах з менш розвиненою сферою ІКТ.
5. Розроблення спільної понятійно-термінологічної бази з урахуванням положень Резолюції 64/25 Генеральної Асамблеї ООН «Досягнення у сфері інформатизації і телекомунікацій у контексті міжнародної безпеки».

Головною передумовою ефективного розв'язання проблем у сфері ІКТ є плідна співпраця між партнерами на світовій арені. У цьому сенсі особливого значення набуває діяльність зі створення міжнародної правової бази щодо захисту інформаційного простору, котра має юридично забезпечити можливість консолідованих дій і створення спільних механізмів у сфері ІКТ, а саме:

– установити правові зобов'язання держав сприяти розвиткові системи забезпечення інформаційної та кібербезпеки у країнах, що відстають у цьому;

– забезпечити правовий захист критично важливих інфраструктур;

– репрезентувати правові норми використання ІКТ у конфліктах;

– законодавчо закріпити загальні стандарти забезпечення кібербезпеки;

– створити єдине процесуальне законодавство з питань боротьби з кіберзлочинністю, інформаційним тероризмом і запобігання загрозі кібервійни;

– гарантувати правове забезпечення МІБ бізнес-структур.

Уважаємо, що міждержавні домовленості та міжнародне інформаційне право мають бути спрямовані на демілітаризацію міжнародного інформаційного простору. Необхідно доопрацювати й

адаптувати механізми міжнародного права щодо сфери інформаційно-комунікаційних технологій, а також створити нові норми, позаяк гонка озброєнь в інформаційному просторі здатна призвести до дестабілізації міжнародної безпеки через порушення наявних домовленостей про роззброєння та в інших сферах.

Основні результати даного розділу висвітлено у працях [445-460].

РОЗДІЛ 5.
НАПРЯМИ РОЗВИТКУ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ЄВРОІНТЕГРАЦІЇ

5.1. Концептуальні засади правового забезпечення інформаційної безпеки України в умовах євроінтеграції

Не викликає сумніву, що будь-яке законодавство має спиратися на чітку, науково обґрунтовану й об'єктивно зумовлену систему права. Тому систематизація інформаційного законодавства потребує створення стрункої комплексної галузі інформаційного права, формування положень, котрі втіляться в конкретні норми законів та підзаконних нормативно-правових актів. А отже розробка й удосконалення вітчизняного законодавства з безпекових питань інформаційної сфери мають відбуватися на міцному теоретичному фундаменті, науковому обґрунтуванні місця в загальній системі права підгалузі правового забезпечення інформаційної безпеки, а також її взаємодії з іншими правовими галузями та інститутами.

Слід зазначити, що теперішній стан захищеності прав і законних інтересів людини, суспільства й держави в інформаційній сфері України свідчить про недостатній рівень правового регулювання й забезпечення інформаційної безпеки. Так, непоодинокими є випадки порушення чи безпідставного обмеження вказаних прав та інтересів; у нормах, що регулюють інформаційні відносини, у правовому забезпеченні інформаційної безпеки існує чимало суперечностей, лакун і колізій, а деякі відносини у цій сфері взагалі не врегульовані. Убачається, що все це

зумовлене насамперед слабким теоретичним обґрунтуванням підгалузі правового забезпечення інформаційної безпеки та іншими системними прорахунками. Стосовно цієї підгалузі спостерігаємо також розсинхронізацію між системами права й законодавства, усунення якої потребує системного підходу до відповідної законотворчості. Саме такий підхід має стати головним методологічним інструментом забезпечення інформаційної безпеки, оскільки за його допомогою «можливе розв'язання проблем співвіднесення цілого й частини, організації та дезорганізації, порядку й безладу».

Ефективності інформаційного законодавства в цілому серйозно шкодить також відсутність у нормативно-правових актах з питань забезпечення інформаційної безпеки єдиних для всіх джерел правового регулювання відповідних засадничих нормативних умов.

Поряд із юридичними конструкціями, правилами та прийомами викладення законодавчих та інших нормативно-правових актів чи не найважливішим засобом юридичної техніки є відповідна термінологія. А між тим, термінологія, що застосовується у сфері забезпечення інформаційної безпеки, хибує на брак єдності, неоднозначні тлумачення, а то й узагалі відсутні визначення багатьох понять, у тому числі ключових. Усе це створює серйозні перешкоди як для правотворчої діяльності в інформаційній сфері, так і для правозастосовної, а також зайвий раз засвідчує відсутність системності у розв'язанні вказаних проблем.

Наприклад, до теперішнього часу немає законодавчого визначення такого базового терміна, як «інформаційна безпека», чи «безпека інформації», хоча самі ці термінологічні сполучення вживаються в деяких законах. Контекстний аналіз вживання законодавцем поняття «безпека інформації» дає підстави тлумачити його як стан захищеності інформації в системі. Відповідно, «захист інформації» – це діяльність із забезпечення вказаного стану захищеності. Захист інформації як складова діяльності із забезпечення безпеки інформації та інформаційної безпеки є одним із

засобів захисту прав і законних інтересів людини, суспільства, держави в інформаційній сфері.

Найбільш точно, на нашу думку, цей процес можна відобразити в категоріях «захист» і «охорона», які разом охоплюють діяльність із забезпечення інформаційної безпеки. Суть охорони інформації полягає у встановленні щодо окремих її видів певного правового режиму, скажімо, державної таємниці. Натомість захист інформації – це сукупність заходів із протидії загрозам та протиправним посяганням на права та законні інтереси суб'єктів в інформаційній сфері.

Важливою складовою інформаційної безпеки вбачається комплексний захист зазначених прав і законних інтересів від непередбачуваного й шкідливого впливу певного інформаційного техніко-технологічного середовища, створеного самим соціумом, тобто від побічних чинників впливу технологічних та організаційних процесів на особу, суспільство, державу. При цьому система інформаційної безпеки покликана нейтралізувати вказані негативні впливи на людину та сприяти підтриманню стабільності суспільства й держави, інститути котрої, у свою чергу, повинні цю нейтралізацію забезпечити. Іншими словами, головною ознакою стану захищеності в інформаційній сфері (інформаційної безпеки) є оптимальне співвідношення інтересів людини, суспільства й держави.

Чинниками забезпечення інформаційної безпеки держави є гарантування:

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

2) конфіденційності інформації з обмеженим доступом;

3) захищеності особи, суспільства й держави від шкідливого впливу певних видів інформації (в даному разі йдеться не про інформацію, віднесену до категорій з обмеженим доступом, а про такі її види, котрі здатні зашкодити вказаним суб'єктам інформаційних відносин).

За станом на сьогодні зазначені відносини, пов’язані із забезпеченням інформаційної безпеки, далеко не повно законодавчо врегульовані. Можна констатувати лиш загальну регламентацію діяльності щодо захисту інформації. Саме тлумачення змісту поняття «захист інформації» вважаємо не зовсім коректним, позаяк однією із цілей цієї діяльності називається фактично самозабезпечення – захист інформації спрямований на забезпечення захисту інформації, що утруднює не тільки розуміння змісту діяльності, а й оцінювання її результатів. Тому метою цієї діяльності, на наш погляд, слід визнати досягнення стану безпеки інформації як складової інформаційної безпеки.

Описане вище становище спричинене відсутністю сформульованих в одному законі концептуальних аспектів забезпечення інформаційної безпеки держави. При цьому зазначимо, що для розробки такого закону належить виокремити джерела права, котрі містять норми, які відповідають даному інституту, на основі створеної в системі права підгалузі правового захисту інформаційної безпеки. Ці норми, сьогодні розпорошені по багатьом галузевим законам і до того ж нерідко суперечать одна одній.

В умовах, у яких нині опинилася Україна через гібридну агресію Російської Федерації, особливої актуальності набуває протидія поширенню шкідливої для психіки людини інформації, яку без перебільшення можна вважати інформаційною зброєю, а також розвиток відповідного законодавства. У цьому контексті інформаційно-психологічну безпеку можна визначити як стан захищеності від окремих осіб та/або певних груп, а також відповідних життєво важливих інтересів людини, суспільства й держави в інформаційній сфері.

Під негативним інформаційно-психологічним впливом ми розуміємо 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.

Усю глибину загрози подібних постійних, цілеспрямованих, продуманих і щедро фінансованих впливів з боку РФ для національної безпеки Україна повною мірою відчула під час анексії Криму та воєнних дій на сході. Убачається, що всі питання, пов'язані із зазначеними впливами, слід передбачити в межах спеціального закону стосовно забезпечення інформаційної безпеки.

Інша проблема, яка потребує законодавчого визначення та врегулювання, – відсутність систематизації законодавства з питань протидії екстремізму в інформаційній сфері. Внаслідок цього матеріали подібного змісту часто розповсюджуються практично безперешкодно, позаяк діяльність із запобігання й припинення різних видів екстремізму здійснюється компетентними державними органами безсистемно й нерідко формально.

При цьому важливо пам'ятати, що реальна протидія екстремістським чи іншим негативним проявами в інформаційній сфері не повинна перетворюватися на зведення особистих рахунків з «незручними» журналістами, тиск на опозиційні засоби масової інформації та придушення свободи слова.

Масова інформатизація всіх сфер життєдіяльності суспільства не оминула й державні інституції. Тому вельми нагальним убачається забезпечення прозорості в діяльності всіх гілок державної влади, кожного держслужбовця. Це, своєю чергою, безпосередньо впливає на дієвість інституту відповідальності для кожного із суб'єктів цієї діяльності, на стан інформаційної безпеки, а також на загальний стан державної та національної безпеки.

Попри всі декларації й певні кроки української влади підвищити рівень доступу до офіційної інформації та ступінь довіри до електронного уряду, на даний момент до світових стандартів нам ще далеко. Такий висновок можна зробити на підставі дослідження, представленого

Департаментом економічного й соціального розвитку ООН (The United Nations Department of Economic and Social Affairs)[11], фахівці якого вважають, що електронний уряд є інструментом підвищення ефективності керування, трансформації процесів державного керування за рахунок підвищення ступені залучення до нього широкого кола громадськості на всіх рівнях – мікро, мезо, макро. Тож наразі стає актуальним і особливо затребуваним інститут доступу до офіційної інформації. Цьому сприяють швидкий розвиток інформаційних технологій, зростання добробуту й рівня освіченості населення. В 2009 році була відкрита для підписання Конвенція Ради Європи «Про доступ до офіційних документів» [461].

Електронне урядування протягом тривалого часу розглядається як один з найдійовіших інструментів максимального використання переваг інформаційного суспільства в Європі. Уряди й адміністрації на всіх рівнях одержують змогу пропонувати громадянам і установам більш високу якість послуг, підвищити швидкість і зручність доступу до них. Комісія ЄС визначає електронний уряд як «застосування інформаційних і телекомунікаційних технологій у роботі органів керування в комбінації з організаційними змінами й новими методами підвищення ефективності державної служби й демократичних процесів, а також формування й полегшення реалізації державної політики».

Для забезпечення участі європейських урядів, громадян і підприємств в інформаційному суспільстві ЄС послідовно працює над розвитком інформаційних і телекомунікаційних технологій. Після виходу білої книги «Зростання, конкурентоспроможність і зайнятість» в 1993 році сформовано єдину стратегію інформаційного суспільства, яка вже наступного року була закріплена у плані заходів «Шлях Європи до інформаційного суспільства» [462]. У 1999 році інформаційне суспільство стало реальністю, але залишалася необхідність подальшої координації між учасниками. Це було враховано в декларації «Eeurope – інформаційне

[11] https://www.un.org/development/desa/en/

суспільство для всіх» [463], а в 2000 році розроблено й ухвалено відповідний план заходів – «Eeurope».

Цей документ сконцентрований на виконанні трьох основних завдань: забезпечення дешевого, швидкого й безпечного доступу в Інтернет; інвестиції в трудові ресурси та їх кваліфікацію; заохочення до користування Інтернетом. План заходів eeurope грунтується на низці найважливіших концепцій, програм і дій, що стосуються таких сфер: e-research, e-security, e- working, e-accessibility, e-commerce, e-government, e-learning, e-health, e-transport, e-content. E-government є основним напрямком роботи майбутніх європейських концепцій у регіональному масштабі. Як констатується в документі BISER (Benchmarking for Information Society: eeurope Indicators for European Regions), основними рушійними силами для проникнення інформаційного суспільства в сферу держави й публічної адміністрації є e-government (в установах G2C, G2B, включаючи інтерактивну комунікацію із громадськістю), мережі/комунікації усередині й між адміністраціями, розміщення замовлень у режимі онлайн і менеджмент знань. Основною метою європейської політики в документі визначено створення Інтернет-порталів державних установ, запровадження інтерактивних комунікацій, послуг на основі транзакцій, нових інформаційних послуг, а також зниження рівня бюрократизму.

Від самого початку ініціатива eeurope отримала широкий політичний і громадський резонанс, що сприяло виникненню нових ініціатив у цій сфері в державах-учасниках і багатьох європейських регіонах. Для формування інформаційного суспільства, поширення якого має відбуватися як усередині суспільства, так і на рівні регіонів, потрібне не просто створення технічних потужностей ІКТ, хоча це і становить стрижень інформаційного суспільства й дає потужний імпульс для нових інвестицій. Інші чинники вбачаються не менш важливими: залучення уваги громадян до інформаційного суспільства, підвищення рівня професійної кваліфікації й освіти; роль публічного сектора при розвитку

інформаційного суспільства; організаційні ресурси підприємств тощо.

Усі автори єдині в думці, що світ вступає в епоху грандіозних соціальних змін, технологічних і культурних перетворень, їхні прогностичні позиції досить близькі. Потенціал техніки, незмінно нарощуваний, робить вирішальний вплив на всі сфери життя людського суспільства. Зростає продуктивність праці, змінюється в десятки, сотні разів його зміст. Вони змінюють лад культури і впливають на формування всієї цивілізації. Людський інтелект, його міць багаторазово збільшуються завдяки революції інформаційно-комунікаційних технологій. Соціальна структура суспільства опиняється під надмірним впливом технологічних нововведень. Ро́боти вже витіснили людей із багатьох галузей. Суть у тому, що відбуваються трансформації, бо народжується новий цивілізаційний устрій, в якому сфера праці, наука та освіта, державне управління, культура будуть носити принципово інший характер.

На відміну від індустріального суспільства, яке в основі має машинну технологію, специфіка постіндустріального суспільства криється в використанні інформаційно-інтелектуальної технології.

Сьогодні, на наш погляд, цю ідею необхідно розглядати в якості базисної при формуванні філософської концепції інформаційної безпеки. У її розрізі можна виокремити такі базові постулати типів суспільств (табл.. 5.1.)

Таблиця 5.1. Типи суспільств

Характеристика	**Доіндустріальне**	**Індустріальне**	**Постіндустріальне**	**Інформаційне**
Оновний виробничий ресурс	Сировина	Енергія	Інформація	Знання
Базовий тип діяльності	Добування	Виготовлення	Обробка	Перетворення
Характер базових технологій	Трудомісткі	Капіталомісткі	Наукомісткі	Технології спрямовані на покращення здоров’я людини та продовження її життя; робототехніка та інтрнет-речей,

				кіберзахист
Коротка характеристика	Підкорення природи	Перетворення природних ресурсів	Виникнення нових відносин між людьми	Взаємовідносини людей та роботів, розвиток інтернет-речей
Негативні впливи	Захоплення територій	Екологічні проблеми	Нерівномірний розподіл ресурсів. Маніпуляція суспільною думкою за допомогою інформації	Технологічна сингулярність, втрата людиною своїх основних ідентифікуючих цінностей, підміна базових цінностей
Можливості	Зародження інформаційного обміну	Розвиток інформаційних взаємовідносин	Обмін інформацією	Переоцінка базових цінностей на основі нового знання, розвиток взаємовідносини людини та роботів, поява нових видів правовідносин, пов'язаних з IT-сферою та штучним інтелектом. Перехід до відновлювальних джерел інформації та розвиток високих технологій. Диверсифікація інформаційних каналів.

Ми підтримуємо позицію тих учених, які виокремлюють наступний витóк розвитку суспільства після індустріального. Хоча й по-різному визначають даний етап, але сходяться до певних спільних його характеристик. Назва нового суспільства, наступного за індустріальним, не відображає головних характеристик майбутнього ладу, в якому інноваційним чинником стане інформація. Крім того, приставка «пост» виражає деяку обмеженість свідомості для нового суспільства (що будується на нових принципах). Тому, на наш погляд, основну суть суспільства, яке спирається на використання інформаційної технології, найбільш повно здатне передати поняття «інформаційне суспільство».

Теорії інформаційного суспільства, безсумнівно, розширюють знання про соціальний і науково-технічний прогрес, в той же час вони не дають цілісного уявлення про трансформації сучасного суспільства. Концептуальний аналіз основних теорій розвитку нового суспільства в контексті інформаційної безпеки дозволив нам виявити відносно

невисокий ступінь критичності дослідників до можливостей, що відкрилися на основі використання інформаційних технологій. Прийдешня цивілізація ставить суспільний розвиток у тісну залежність від прогресу науки і техніки, в результаті набуває політично небезпечного відтінку, їй притаманні економічні, соціальні і всі інші види проблем, посилені інформаційним фактором. Окрім того, відсутність в інформаційному суспільстві утвердження ідеалів справедливості поряд із проголошенням внутрішньої і зовнішньої свободи відображає в ньому «етичну неповноцінність», що свідчить про його нездатність протистояти виникненню антагоністичних протиріч.

Майбутні перспективи людства в теоріях інформаційного суспільства розглядаються без урахування етичних обмежень, в них затверджуються ідеї свободи, але, в більшій мірі, ігноруються принципи інформаційної безпеки як важливої умови, що визначає на сьогоднішній день стабільність суспільного ладу. Через цю обставину виявляються слабо врахованими виниклі в суспільстві нові види небезпек, загроз і негативні ефекти застосування інформаційних технологій.

У той же час, згідно з хронологією теоретичних поглядів на процеси інформатизації та проблеми безпеки, пов'язані з масштабним впровадженням інформаційних технологій, можна сказати, що властива першим концепціям суспільства, що формується високий ступінь науково-технічного фанатизму зменшується. Пізніші теорії інформаційного суспільства відрізняються вже більшою увагою до наслідків впровадження інформаційних технологій, до психологічних, духовно-моральних, гуманістичних аспектів розвитку інформаційної цивілізації, тим самим створюючи методологічну основу для вирішення проблем інформаційної безпеки.

Основні концепції нового суспільства зачіпають деякі актуальні проблеми інформаційної безпеки: інформаційне розшарування суспільства, контроль індивідуальної і суспільної свідомості, порушення

конфіденційності інформації, вторгнення в особисте життя індивіда і т. ін.

Таким чином, аналіз формування нового суспільства, усвідомлення його в цілісності, без відриву від інформаційних технологій, спонукає до пошуку шляхів безпечного розвитку, подолання негативних ефектів від застосування інформаційних технологій, перегляду ціннісних орієнтирів. На наш погляд, подальший напрямок безпечного розвитку і застосування інформаційних технологій, з метою забезпечення динамічної рівноваги громадської еволюції вимагає підтримки умов інформаційної безпеки.

Формування інформаційного суспільства є закономірним етапом еволюції сучасного соціуму, що характеризується, в першу чергу, масштабним впровадженням інформаційних технологій і розвитком глобального інформаційного простору. Процес становлення нового суспільства, обумовлений впровадженням інформаційних технологій, вимагає правильного усвідомлення його інформаційної специфіки і конструктивного розвитку закладеного в ньому потенціалу.

Проблема захисту від нових видів небезпек і загроз, породжених інформатизацією, що проявилися в третьому тисячолітті, турбує дослідників сучасного суспільства. Кількість робіт, присвячених проблемам інформаційної безпеки, стає дедалі більше. У той же час, аналіз наукової літератури доводить, що методологічні аспекти вивчення інформаційної безпеки вимагають подальшого опрацювання. Згідно з нашою точкою зору, перш за все, важливо досліджувати термінологію, оскільки автори численних робіт в галузі інформаційної безпеки сходяться на думці про те, що дати вичерпне визначення інформаційної безпеки надзвичайно складно.

Можна зробити висновок, що безпека визначається, як можливість системи протистояти небезпекам, а так само - здатність переходити в своєму розвитку до більш високого рівня. Процедура захисту безпечного стану необхідна для нормального функціонування і прогресивного розвитку системи. На наш погляд, безпека розглядається в якості однієї з

характеристик життєзабезпечення будь-якого об'єкта, а також - у якості іманентної здатності даного об'єкта реагувати на спотворення власних цінностей, цілей, інтересів, інакше - підстав існування даної системи.

Незважаючи на те, що технологічна революція може поглибити соціальні та географічні відмінності, життя людей за допомогою інформаційних технологій повинна бути покращена. Інформаційні технології, шляхом моментального доступу до інформації, розширюють права громадян, з'являється можливість не тільки споживати інформацію, але й виробляти її. Крім того, інформаційні технології збільшують можливості людей, це пов'язано з активною участю в процесі ухвалення політичних рішень, в результаті прозорості, що надається технологіями спостереження за діяльністю урядів.

Створення й постійне підвищення рівня відкритості та прозорості в діяльності органів державної влади є якісною ознакою демократичних перетворень суспільства в контексті концепції електронного урядування. Важливо, щоби відкритість стала дійовим інструментом забезпечення взаємодії суспільства й органів влади, залучення громадян і суспільних інститутів до вирішення державних питань, вироблення і прийняття політичних рішень, формування можливостей всебічного оцінювання якості їх реалізації, суспільного контролю.

Отже, транспарентність органів державного управління слід розглядати як багатогранну характеристику ефективного функціонування влади, що базується на трьох головних елементах: відкритості, прозорості й доступності, котрі у взаємозв'язку визначають інтегративний зміст досліджуваного поняття.

Гострим залишається питання співвідношення рівня транспарентності органів державної влади й забезпечення національної безпеки України. Як уже неодноразово зазначалося, національна безпека становить складну, багаторівневу, відкриту, динамічну систему, у центрі якої перебуває взаємодія базових соціальних суб'єктів – особи, суспільства

й держави. Формування й функціонування цієї системи відбувається під впливом безлічі чинників – історичних, географічних, етнічних, демографічних, соціально-політичних, економічних, культурних, релігійних та ін. Відтак, пріоритетні напрями стратегії національної безпеки, зумовлені життєво важливими інтересами особи, суспільства й держави, реалізуються через виявлення внутрішніх і зовнішніх загроз безпеці країни, розробку ефективних інструментів їх попередження і знешкодження з урахуванням ролі й місця України в системі глобальної та регіональної безпеки.

Зважаючи на виняткову важливість інформаційної сфери, у контексті дослідження взаємозв'язку і взаємовпливу інформаційного простору й національної безпеки можна зробити висновок про необхідність захисту національних інтересів передусім у контексті міжнародних відносин.

Оскільки рівень транспарентності органів влади залежить передусім від організації доступу до "особливої" (державної) інформації, слід відзначити таке:

- питання про співвідношення права на доступ до інформації й національної безпеки завжди було й лишається чутливим і спірним. Серйозна суперечність між потребою обмежень і доступу громадян до державної інформації ще більше загострюється через заборонний ухил і відсутність чітких законодавчо закріплених правових рамок, а також міжнародних стандартів;

- будь-яке обмеження права на доступ до інформаційних державних ресурсів слід закріпляти в законодавстві, причому відповідний закон та інші нормативно-правові акти мають бути загальнодоступними, чіткими та зрозумілими, не допускати двозначних тлумачень. Закон, що обмежує доступ до офіційних відомостей, повинен забезпечувати належні гарантії проти інформаційних зловживань;

- кожен державний орган, котрий уповноважений засекречувати інформацію, зобов'язаний надавати обґрунтування легітимності

запроваджених обмежень;

- система обмеження доступу до державної інформації має бути унікальною для кожної держави. Проблему кореляції свободи інформації (пошуку, одержання, поширення) та інтересів національної безпеки і, як наслідок, обмеження доступу до певної інформації не можна вирішити однозначно й на рівні усього світового співтовариства або ж в рамках ЄС чи будь-якої іншої регіональної спільноти, позаяк усі держави мають різний прийнятний рівень національної безпеки. Це, втім, не означає що Україна не повинна підвищувати власні безпекові стандарти, прагнучи наблизити їх до загальноєвропейського рівня.

При забезпеченні балансу безпеки й транспарентності дуже важливо, аби перелік правопорушень в інформаційній сфері, за які передбачена відповідальність, був чітко визначений, а інформація про подібні порушення з боку представників державної влади та місцевого самоврядування оприлюднювалася у доступних джерелах. Звісно, забезпечення державними органами принципу гласності та прозорості має сполучатися із забезпеченням вимог законодавства щодо охорони державної таємниці та іншої інформації з обмеженим доступом.

У контексті розглядуваного питання цікавою убачається практика Європейського суду з прав людини (ЄСПЛ), зокрема, справа «Ієрсилд проти Данії» [464]. У рішенні в цій справі від 23 вересня 1994 року ЄСПЛ зазначив, що «покарання журналіста за сприяння в розповсюдженні заяв, зроблених третіми особами під час інтерв'ю, могло би серйозно завадити засобам масової інформації робити свій внесок в обговорення проблем, що становлять суспільний інтерес, якщо тільки не йдеться про особливо серйозні ситуації». Тобто, при вирішенні подібних справ ЄСПЛ керується справедливим, на наш погляд, принципом, відповідно до якого журналіст (ЗМІ) не повинен відповідати за ретрансляцію достовірної інформації, навіть такої, яка містить екстремістські елементи, але не збігається з думкою журналіста (ЗМІ).

Таким чином, уважаємо за доцільне з метою чіткого системного врегулювання питань протидії інформаційному екстремізму, що забезпечило б захист законних інтересів людини від негативних інформаційних впливів, суспільної моралі та держави, а також задля усунення колізій і лакун законодавства регламентувати зазначену діяльність окремим законом з питань забезпечення інформаційної безпеки.

З цього приводу, наприклад, О. Ярема зазначає, що для інституційного розвитку правового забезпечення інформаційної безпеки необхідно прийняти закон «Про інформаційну безпеку» [465, с. 250].

Єдності щодо шляхів якісної трансформації інформаційного законодавства України дослідники цієї проблематики допоки не досягли, що не дивно з огляду на складність, динаміку та масштабність сучасних інформаційних процесів, які відбуваються в умовах становлення національної правової системи [465, с. 252].

Однією з основних причин невідповідності інформаційного законодавства України вимогам сучасності є те,, як слушно зазначає Г. Ситник, що у суспільній і науковій думці не сформувалося цілісне уявлення про інформаційну безпеку з позиції права та юридичної науки [38, с. 89].

Життєдіяльність інформаційного суспільства потребує чіткого законодавчого врегулювання багатоманітних відносин, що виникають у зв’язку зі створенням, функціонуванням, використанням інформаційних систем і ресурсів, каналів комунікацій, відповідних технологій тощо. Досліджене у попередніх параграфах формування в системі інформаційного права такої підгалузі, як правове забезпечення інформаційної безпеки, зумовлює потребу виокремлення законодавчих актів, положень, норм, котрі регламентують різні аспекти забезпечення інформаційної безпеки, їхнього аналізу на предмет наявності системних вад, а також систематизації, консолідації на цій основі загальних правових норм у єдиний базовий закон, позбавлений існуючих у теперішній час

суперечностей, колізій та прогалин. Це, у свою чергу, має створити передумови для якісної комплексної трансформації законодавства, яке регулює інформаційні відносини в різних сферах життєдіяльності суспільства. Ідеться передусім про прийняття закону «Про інформаційну безпеку».

Зауважимо, що ідея розробки такого закону не є новою, а найбільш результативні спроби її реалізації припадали на 2004 та 2014 роки.

Так, у 2004 році був розроблений проект Закону України «Про інформаційну безпеку України» (№5732 від 22 вересня 2004 року). Фактично зазначений законопроект становив лише словник визначень, що стосуються інформаційної безпеки (ст. 2); перераховував її об'єкти (ст. 3) та суб'єкти (ст. 4); зазначав підстави гарантування державою цілісності інформаційного простору (ст. 5); наводив перелік загроз інформаційному простору й інформаційній безпеці (не розрізняючи їх та не передбачаючи можливості виникнення нових загроз) (ст. 6); загальними фразами окреслював шляхи забезпечення інформаційної безпеки України (ст. 7); визначав основні напрями державної політики в інформаційній сфері (ст. 9). Відтак, за оцінками експертів, «законопроект справляє враження навчального посібника, присвяченого чи то теорії інформаційної безпеки, чи то інформаційному простору» [466].

Приміром, у ст. 10 «Система забезпечення інформаційної політики та інформаційної безпеки України» систематизовано й наведено повноваження Президента України, Верховної Ради України, Ради національної безпеки і оборони України, Кабінету Міністрів України, міністерств, Служби безпеки України, інших центральних органів виконавчої влади, місцевих державних адміністрацій, органів місцевого самоврядування, правоохоронних органів, судів загальної юрисдикції, Генеральної прокуратури України; окремі права громадян в інформаційній сфері. Вочевидь, закріплення таких норм, які відтворюють уже закріплені законодавчо положення лишень з наголосом на повноваженнях указаних

суб'єктів в інформаційній сфері, не тільки не врегульовує відповідні суспільні відносини, але й створює можливість обмеження діяльності у сфері інформаційної безпеки виключно наведеними повноваженнями. При цьому значна частина статей законопроекту має бланкетний характер і відсилає до норм чинного законодавства, що аж ніяк не сприяє визначеності правового регулювання.

Фактично законопроект спрямований на фіксацію рамкових засад інформаційної безпеки і має переважно декларативний характер. Відсутність конкретизації й орієнтація на загальні положення прийнятна, скажімо, для Концепції забезпечення інформаційної безпеки, але аж ніяк не для закону. Складність і багатоманітність інформаційних відносин зумовлюють необхідність систематизації нормативно-правових актів стосовно інформаційної сфери у вигляді, наприклад, Інформаційного кодексу (статті, присвячені правовому регулюванню інформаційної безпеки, могли би скласти окремий розділ чи книгу цього кодексу) або закону «Про інформацію», викладеного в новій редакції.

Окрім зауважень до законопроекту як такого, виникає й низка запитань щодо тексту конкретних статей. Зокрема, у ст. 2 передбачено, що «інформаційна безпека України – комплекс системних превентивних заходів із надання гарантій захисту життєво важливих інтересів особистості, суспільства й держави від негативних інформаційних впливів в економіці, внутрішній і зовнішній політиці, в науково-технологічній, соціокультурній і оборонній сферах, системі державного управління, самостійного й незалежного розвитку всіх елементів національного інформаційного простору та забезпечення інформаційного суверенітету країни, захисту від маніпулювання інформацією і дезінформування та впливів на свідомість, підсвідомість і психіку як індивіда, так і суспільства в цілому, спроможність держави нейтралізувати чи послабити дію внутрішніх і зовнішніх інформаційних загроз». Залишивши в дужках семантико-стилістичну незграбність наведеної дефініції, зауважимо, що,

попри певні позитивні зрушення стосовно нетрадиційного функціонального розуміння інформаційної безпеки (на відміну від «стану захищеності»), її визначення як процесу не може вичерпуватися суто превентивними заходами.

Варто також зазначити, що:

– тлумачення інформаційної інфраструктури у ст. 15 законопроекту відрізняється від її визначення, наведеного раніше у ст. 2;

– включення до системи засобів масової інформації не лише друкованих і електронних ЗМІ (телерадіокомпаній, інформаційних агентств), а й книговидавничих, кінематографічних, бібліотечних, архівних комплексів потребує, на нашу думку, певного обґрунтування, позаяк діяльність, скажімо, архівів урегульована окремим законодавством та ще й має принципово інший характер, а книговидавнича – Законом України «Про видавничу справу» і т.д.

Принципово помилковим убачається й визначення правопорушень у цифрових телекомунікаційних мережах саме цим законом, оскільки подібні делікти мають визначатися у відповідних кодексах – кримінальному, цивільному, про адміністративні правопорушення.

Так само вважаємо недоречним і запровадження вичерпних переліків, наприклад, загроз, напрямів державної політики чи об'єктів інформаційної безпеки, оскільки це створює передумови для можливих правопорушень (ст. 4, 6, 9, 18 законопроекту). Адже передбачити все у переліку неможливо, а будь-який об'єкт, котрий залишився за його межами, вже не підпадатиме під дію закону.

Виникають також цілком логічні сумніви щодо коректності визначення об’єктів інформаційної безпеки (ст 4). У законопроекті всі вони згруповані в чотири групи за відповідними сферами – економіки, оборони, духовності, політики. Така класифікація, безперечно, не охоплює всі об’єкти інформаційної безпеки, а визначення об’єктів у межах цих груп має вельми специфічний характер. Приміром, у духовній сфері об’єктами

інформаційної безпеки є культурні та естетичні позиції, соціальні й особистісні орієнтації, а в політичній – права політичних партій, організацій, громадських об'єднань. Поза увагою лишилися інформаційні ресурси з персональними даними, інформаційні ресурси, котрі забезпечують діяльність правоохоронних органів, тощо. Крім того, недержавні володільці інформаційних ресурсів мусять самостійно дбати про їх захищеність, і державне втручання тут неприпустиме, за винятком випадків, передбачених законом.

Ст. 5 законопроекту одним із засобів забезпечення цілісності національного інформаційного простору України передбачає збереження права власності держави на провідні його об'єкти, а у ч. 2 до таких об'єктів відносить: «інформаційну продукцію в усіх її різновидах, включаючи твори літератури і мистецтва, наукові праці, публічні виступи, використані в інформаційній діяльності, національні інформаційні ресурси, інформаційні послуги, організаційні та майнові функціональні елементи інформаційної інфраструктури». Водночас у ч. 4 ст. 1 зазначено, що «дія цього Закону не поширюється на регулювання інформаційних відносин у процесі побутового спілкування, літературно-мистецької та науково-творчої діяльності, на зміст інформації, що є продуктом художньої творчості, а також на проведення різного роду дискусій, симпозіумів, конференцій, з'їздів, семінарів, літературно-мистецьких заходів тощо, за виключенням публічної інформації про ці заходи, її поширення та використання». Відтак виникає закономірне питання, чи поширюється дія цього закону на згадані об'єкти інформаційного простору? Більше того, слід також зважати на відсутність процедури визначення цих провідних об'єктів. Тому спроби збереження права власності держави на те, що невідомо ким і в який спосіб визначатиметься, викликають серйозні побоювання щодо дотримання принципу передбачуваності як елемента доктрини верховенства права. Крім того, нагадаємо, що з набранням чинності новою редакцією Закону України «Про інформацію» дискусійним

лишається питання стосовно можливості існування права власності на інформацію, тож відповідні положення законопроекту не повною мірою відповідають сучасним правовим реаліям.

Не менше питань викликають і положення статей 12 і 13 законопроекту. Перша з них визначає, що таке національні інформаційні ресурси виняткового державного значення. Згідно з дефініцією такими є інформаційні ресурси, «які своїм змістом можуть істотно впливати на стан національної безпеки України». Що це означає, не зовсім зрозуміло, адже ч. 2 ст. 12 передбачає, що віднесення до складу таких ресурсів (або виключення) «здійснюється в порядку, встановленому законами України». Але таких законів фактично не існує. Таке регулювання, точніше, його відсутність дає підстави припустити наявність в цьому випадку законотворчості заради законотворчості. Одначе, позаяк ідеться про такий серйозний наслідок, як обмеження власника у праві розпоряджатися інформаційними ресурсами, що належать йому за правом власності, то, можливо, вартувало врахувати існуючий порядок регулювання права інтелектуальної власності Цивільним кодексом України (Книга четверта), чого, на жаль, не було зроблено. У свою чергу, у ст. 13 зазначено, що найбільш вагома, вартісна частина інформаційних ресурсів можуть оголошуватися національним надбанням України без позбавлення права власності на них, однак порядок такого оголошення також відсутній.

Далі. Ч .6 ст. 11 передбачає, що національні інформаційні ресурси, які є власністю держави, перебувають на обліку та у віданні органів державної влади й організацій відповідно до їхньої компетенції, що практично неможливо здійснити, зокрема через надмірну вартість такого обліку.

Практично ідентичними є значні частини ст. 7 і ст. 9 без видимої потреби в такому дублюванні.

Суперечливими є й такі положення законопроекту, як, наприклад: «Забезпечення інформаційної безпеки України здійснюється шляхом: забезпечення інформаційного суверенітету України» (ст. 7); «Основними

напрямами державної політики в інформаційній сфері України є: забезпечення інформаційного суверенітету України…» ст. 9. Як бачимо, інформаційний суверенітет із мети забезпечення інформаційної безпеки та здійснення державної політики в інформаційній сфері перетворюється на засіб їхньої реалізації. Тож у даному разі некоректним убачається використання такого поняття, як «інформаційний суверенітет держави», оскільки відповідно до Закону України «Про Національну програму інформатизації» [467], це – «здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою дотримання законів України, прав і свобод громадян, гарантування національної безпеки держави». Але в умовах свободи інформації виконання такого завдання є практично неможливим, тому поняття інформаційного суверенітету держави потребує осучаснення. Таким чином, розпливчастість визначення однієї з базових категорій законопроекту, а фактично – його відсутність ставить під сумнів доцільність самого цього документа в запропонованій редакції.

У ч. 1 ст. 9 законопроекту зазначено: «Основними напрямами державної політики в інформаційній сфері України є: забезпечення інформаційного суверенітету України; вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; активне залучення засобів масової інформації до боротьби з корупцією, зловживаннями службовим становищем, іншими явищами, які загрожують національній безпеці України; забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової

інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції; вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України». Своєю чергою, у ч. 4 цієї ж статті знов-таки перераховуються основні напрями державної інформаційної політики України з конкретизацією їх в організаційній сфері, у сфері інформаційної безпеки, у міжнародній та виробничій сферах, у сфері суспільних відносин та в галузях науки, культури, навчання та підвищення кваліфікації. Лишається незрозумілим, як же співвідносяться «основні напрями державної політики в інформаційній сфері України» та «основні напрями державної інформаційної політики України».

Низка статей законопроекту, як уже зазначалося, відсилає до інших нормативно-правових актів, не додаючи нічого нового у регулювання інформаційних правовідносин. Це, зокрема: ст. 8, яка перераховує нормативні акти, що становлять правову основу інформаційної безпеки; ст. 10, яка дає перелік повноважень органів державної влади та місцевого самоврядування, які фактично закріплені іншими нормативно-правовими актами; ст. 11, котра говорить, що національні інформаційні ресурси і право власності на них захищаються відповідно до чинного законодавства; ст. 14, де регламентується застосування мов у національному інформаційному просторі України, що, вочевидь, слід урегулювати в законодавстві з питань використання державної мови та мов національних меншин; ст. 24, що передбачає здійснення судочинства в інформаційній сфері, тощо.

Незрозумілим також, наприклад, залишився механізм реалізації положення ст. 19 про необхідність встановлення спеціальних символів у глобальних комп'ютерних мережах щодо інформації, небажаної для певних категорій населення.

Аналогічним хибує ч. 3 ст. 22, котра обмежує переміщення через кордон інформації, зібраної іноземними дослідниками, а прецінь

забезпечити реалізацію цієї норми у відкритому інформаційному суспільстві з новітніми комунікаційними технологіями, за допомогою яких будь-яку інформацію можна передавати за лічені секунди, причому незалежно від кордонів, практично неможливо.

Законопроект містить також низку термінів, значення яких вельми проблематично з'ясувати не лише зі змісту його статей, але й у рамках вітчизняної правової системи, наприклад, «спекуляція інформаційними ресурсами».

Отже, як бачимо, розглянутий вище законопроект не міг претендувати на статус закону, який має регулювати найбільш важливі суспільні відносини. Адже його запропонована редакція не могла забезпечити належного нормативного регулювання інформаційної безпеки держави. Більше того, законопроект ігнорував ту обставину, що інформація організується спонтанно, а не через упорядкування державою, а самі лиш обмеження на поширення інформації, навіть задля забезпечення національної безпеки, гальмують розвиток суспільства. Натомість інформаційна безпека в сучасних умовах має забезпечувати баланс між відкритістю (траспарентністю) та інтересами безпеки. Саме тому законодавчий акт з питань забезпечення інформаційної безпеки має, окрім іншого, усувати перешкоди для вільного обігу інформації, формувати умови для створення, поширення та отримання інформації з різних джерел, передбачати ефективні механізми забезпечення незалежної діяльності ЗМІ і журналістів, доступу до відкритої інформації органів державної влади й місцевого самоврядування тощо.

З огляду на зазначені вище та інші істотні вади проект закону «Про інформаційну безпеку України» було знято з розгляду.

Така ж сама доля спіткала і його більш сучасного «наступника» – проект закону «Про засади інформаційної безпеки України» (реєстр. № 4949 від 28 травня 2014 року) [468]. У цьому законопроекті пропонувалося визначити основні засади державної політики, спрямованої на захист

життєво важливих інтересів людини і громадянина, суспільства і держави в інформаційній сфері, порядок забезпечення інформаційної безпеки в умовах формування і розвитку інформаційного суспільства в Україні та глобального інформаційного простору, а також закріпити правові основи інформаційної безпеки України.

Метою законопроекту, як зазначили суб'єкти права законодавчої ініціативи, є встановлення: основних принципів забезпечення інформаційної безпеки України; життєво важливих інтересів України в інформаційній сфері; реальних та потенційних загроз інформаційній безпеці України; пріоритетів державної політики у сфері інформаційної безпеки; основних напрямів діяльності держави у сфері забезпечення інформаційної безпеки; об'єктів інформаційної безпеки і суб'єктів забезпечення інформаційної безпеки та їхніх основних функцій; статусу і порядку створення, засад діяльності та повноваження спеціально уповноваженого центрального органу виконавчої влади з питань інформаційної безпеки; засад міжнародного співробітництва у сфері інформаційної безпеки; відповідальності за правопорушення в інформаційній сфері.

Фахівці Головного науково-експертного управління Апарату Верховної Ради України в узагальнюючому висновку від 19 червня 2014 року, погоджуючись з необхідністю врегулювання порушених у законопроекті питань, зауважили, що чимало його положень потребують доопрацювання й уточнення для їх узгодження з іншими законодавчими актами з питань інформаційної безпеки і боротьби з комп'ютерною злочинністю та наповнення конкретним нормативним змістом.

Так, у законопроекті застосовувалася нова для вітчизняного законодавства термінологія. Це, зокрема, поняття "інформаційна безпека", "інформаційна сфера", "кібернетична безпека (кібербезпека)", "кібернетичний простір (кіберпростір)" та низка інших тематичних термінів. Однак при цьому лишилося незрозумілим, чому "інформаційна

безпека" тлумачиться як "стан захищеності…", а "кібернетична безпека" – як "здатність людини …". Адже визначення цих споріднених термінів, котрі, очевидно, співвідносяться між собою як загальне та спеціальне, має ґрунтуватися на одних і тих же вихідних поняттях.

Хоча поняття "кіберзлочинність" і пов’язана з ним термінологія, використовується досить широко, офіційного, закріпленого в міжнародних документах та національному законодавстві його визначення досі не існує. Навіть Конвенція про кіберзлочинність 2001 року і Додаткові протоколи до неї [469] оперують поняттями "комп'ютерна система", "комп'ютерні дані" та передбачають встановлення відповідальності за "правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; за навмисне перехоплення технічними засобами, без права на це передач комп'ютерних даних; за навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це; навмисне серйозне перешкоджання функціонуванню комп'ютерної системи" тощо. Тож запропоновані в законопроекті терміни, зокрема "кіберзлочинність" і "кібертероризм", не узгоджувалися з термінологією, що вже використовується в чинному законодавстві.

Зміст терміна "кібертероризм", крім того, охоплюється поняттям "технологічний тероризм", під яким, зокрема, розуміються "злочини, що вчиняються з терористичною метою із застосуванням… засобів електромагнітної дії, комп'ютерних систем та комунікаційних мереж, включаючи захоплення, виведення з ладу і руйнування потенційно небезпечних об'єктів, які прямо чи опосередковано створили або загрожують виникненням загрози надзвичайної ситуації внаслідок цих дій та становлять небезпеку для персоналу, населення та довкілля; створюють умови для аварій і катастроф техногенного характеру" (ст. 1 Закону України "Про боротьбу з тероризмом" [470]).

Деякі поняття, такі як "об'єкти критичної інформаційної інфраструктури держави", "кібервійська", "кіберпідрозділи" (ст. 5

законопроекту), взагалі не отримали визначень, хоча їхній зміст не є загальнозрозумілим.

До наведених у ст. 3 законопроекту принципів забезпечення інформаційної безпеки, які зведені здебільшого до конституційних гарантій права на інформацію, слід було би додати обов'язкове вжиття заходів щодо інформування про небезпеку та захисту журналістів, які працюють у місцях збройних конфліктів та вчинення терористичних актів, а також при ліквідації небезпечних злочинних груп.

Не можемо погодитися і з тим, що лише створення іншими державами кібервійськ чи кіберпідрозділів є підставою для віднесення цих подій до переліку загроз інформаційній безпеці України. Адже нести загрозу чи завдати державі величезної шкоди може навіть одна людина, котра володіє відповідними знаннями й технічними можливостями.

Зміст ст. 6 проекту, що визначає пріоритети державної політики у сфері інформаційної безпеки, мав би узгоджуватися зі ст. 4, де йдеться про життєво важливі інтереси в інформаційній сфері. На наш погляд, вказані поняття споріднені, а тому автори законопроекту оперують у цих статтях ідентичними положеннями. Зокрема, в обох випадках наголошується на необхідності забезпечення конституційних прав і свобод людини і громадянина в інформаційній сфері; забезпеченні (захисту) інформаційного суверенітету; недопущенні несанкціонованого втручання (забезпечення захисту) у зміст, процеси обробки, передачі та використання персональних даних; розвитку інформаційного суспільства в Україні; збереженні та примноженні духовних, культурних і моральних (національних) цінностей українського народу.

Ст. 7, яка визначає основні напрями діяльності держави у сфері забезпечення інформаційної безпеки, також перевантажена приписами декларативного змісту. Так, в ній відтворюються деякі положення попередніх статей проекту (4 і 6), зокрема, вже втретє вказується на необхідності "забезпечення неухильного додержання конституційних прав

і свобод людини в інформаційній сфері", "формування вітчизняної індустрії високотехнологічної інформаційної продукції (послуг)", "демократичного контролю за діяльністю суб'єктів забезпечення інформаційної безпеки" тощо. Крім того, дев'ять абзаців цієї статті починаються зі слів "удосконалення", "посилення", "поліпшення", "розширення", що свідчить про ненормативний характер відповідних положень, у результаті чого законопроект фактично перетворюється на своєрідну концепцію інформаційної безпеки України. Адже приписів про те, яким чином буде здійснюватися відповідне «удосконалення», «посилення» чи «розширення», документ не містить.

У ст. 8, де називаються об'єкти інформаційної безпеки, вкотре наголошується на необхідності забезпечення «конституційних прав і свобод людини і громадянина, на захищеності від негативного впливу інформаційних технологій та інформаційно-психологічного впливу» (статті 4, 6, 7). Уважаємо, що кількаразове відтворення одного й того ж положення, навіть дуже важливого, в одному законопроекті є очевидною техніко-юридичною помилкою.

Чимало питань виникає і щодо статусу запропонованого до створення аналізованим документом центрального органу виконавчої влади зі спеціальним статусом у сфері інформаційної безпеки – Національної комісії, що здійснює державне регулювання з питань інформаційної безпеки (далі – Нацкомісія інформбезпеки) (ст. 10). Це не повною мірою узгоджується з чинним законодавством, котре визначає порядок створення та формування персонального складу центральних органів виконавчої влади зі спеціальним статусом.

Так, під державними органами, які мають спеціальний статус, зазвичай розуміються прямо чи опосередковано названі в Конституції України органи, не віднесені до жодної з "гілок" єдиної державної влади (законодавчої, виконавчої або судової). До таких державних органів належать прокуратура, Служба безпеки України, Центральна виборча

комісія, Національна рада з питань телебачення і радіомовлення та ін. Спеціальний статус цих інституцій відображається насамперед у порядку їх формування та характері взаємозв'язків з іншими державними органами, передусім вищими – Верховною Радою, Президентом і Кабінетом Міністрів України. У сфері виконавчої влади до таких органів належать Антимонопольний комітет, Фонд державного майна та Державний комітет телебачення і радіомовлення України, створення яких також передбачено Конституцією. При цьому Основний закон України, як відомо, не передбачає створення центральних органів виконавчої влади зі спеціальним статусом за рішеннями парламенту, як це зафіксовано в законопроекті. Як випливає із відповідних положень Конституції (п. 9^1 ст. 106) та Закону України «Про центральні органи виконавчої влади» (ч. 2 ст. 24), такі органи можуть бути створені лише Кабінетом Міністрів України.

З огляду на це запропоновані у проекті приписи щодо надання Нацкомісії інформбезпеки спеціального статусу, порядку його формування, підзвітності та підконтрольності вбачаються не повною мірою узгодженими з відповідними положеннями Конституції України, а також законів «Про Кабінет Міністрів України» та «Про центральні органи виконавчої влади», які є базовим нормативно-правовими актами з питань утворення й функціонування центральних органів виконавчої влади.

Оскільки у ст. 10 законопроекту Нацкомісія інформбезпеки визначена центральним органом виконавчої влади, то на неї мають поширюватись організаційні, кадрові й контрольні повноваження Кабінету Міністрів України, визначені Конституцією та згаданими вище законами України. Це стосується, зокрема, п. 9 ст. 116 Конституції України, за яким спрямування і координація роботи міністерств та інших центральних органів виконавчої влади належить до компетенції Кабінету Міністрів України, а також п. 10 ст. 116 Основного закону, відповідно до якого Кабінет Міністрів України здійснює інші повноваження, визначені

Конституцією та законами України. Такі "інші повноваження" Уряду передбачені, зокрема, законами України "Про Кабінет Міністрів України" [274] та "Про центральні органи виконавчої влади" [471]. Приміром, згідно із ч. 4 ст. 21 закону "Про Кабінет Міністрів України", а також ст. 8 закону "Про центральні органи виконавчої влади" діяльність центральних органів виконавчої влади, керівники яких не входять до складу Кабінету Міністрів України (саме таким органом і пропонується визначити Нацкомісію інформбезпеки), спрямовується й координується міністрами.

Не зовсім коректним виглядає і запропонований у проекті термін, на який Кабінетом Міністрів України призначається керівник Нацкомісії інформбезпеки та його заступники, – 3 роки. Адже відповідно до ст. 19 Закону України "Про центральні органи виконавчої влади" призначення на посаду керівника такого органу та його заступників і звільнення з посади здійснюється Кабінетом Міністрів України за поданням Прем'єр-міністра України. Не узгоджується зі ст. 21 цього ж закону і запропонований у проекті порядок утворення територіальних органів Нацкомісії інформбезпеки та призначення їх керівників.

Крім того, суперечить вимогам Закону України "Про запобігання корупції" [472] надання членам Нацкомісії (крім Голови та його заступників) і членам міжрегіональних комісій з питань інформаційної безпеки дозволу працювати за сумісництвом. Адже закон забороняє посадовим особам державних органів займатися іншою оплачуваною або підприємницькою діяльністю (крім викладацької, наукової і творчої роботи, медичної практики, інструкторської та суддівської практики зі спорту).

У зв'язку із задекларованою потребою створення нових державних органів у сфері забезпечення інформаційної безпеки непереконливим виглядає твердження з Пояснювальної записки до проекту, що прийняття та реалізація Закону України "Про засади інформаційної безпеки" додаткових матеріальних витрат із державного бюджету не потребуватиме,

позаяк фінансування буде забезпечене за рахунок перегляду відповідних функцій інших центральних органів виконавчої влади та скорочення їх штатної чисельності. Але вбачається цілком очевидним, що реалізація даного законопроекту об’єктивно призведе до збільшень видатків з Державного бюджету, принаймні на створення й утримання Нацкомісії інформбезпеки. Крім того, зі змісту Пояснювальної записки незрозуміло, функції яких саме центральних органів державної влади переглядатимуться, яка кількість працівників має бути скорочена, на підставі яких нормативно-правових актів здійснюватимуться відповідні заходи, спрямовані на створення Нацкомісії інформбезпеки.

Далі. У ст. 11 законопроекту основні функції суб’єктів забезпечення інформаційної безпеки виписані надто узагальнено, без визначення повноважень суб’єктів інформаційної безпеки, які становлять зміст відповідних функцій. При цьому в тексті відсутній порядок і механізм здійснення деяких функцій. Приміром, лишається незрозумілим, які саме органи і в який спосіб мають визначати, яка саме інформація є спотвореною або забороненою для поширення і, зокрема, становить загрозу державному суверенітету, конституційному ладу і територіальній цілісності України, розпалює міжнаціональну, міжконфесійну та іншу ворожнечу, маніпулює свідомістю населення України.

Відтак, є підстави вважати, що відповідні положення цієї статті не справлять суттєвого впливу на стан забезпечення інформаційної безпеки. На нашу думку, кожна передбачена функція має супроводжуватися визначенням конкретних повноважень (прав та обов’язків) суб’єктів забезпечення інформаційної безпеки. До того ж низка повноважень суб’єктів інформаційної безпеки, визначених у загальній формі без жодної конкретизації, виглядає зайвою. Незрозуміло, зокрема, навіщо в нормативно-правовому акті найвищої юридичної сили встановлювати, що "наукові установи здійснюють наукову і науково-технічну діяльність…", "навчальні заклади здійснюють науково-педагогічну діяльність…",

"працівники підприємств, установ та організацій, які виконують роботи, пов'язані з експлуатацією інформаційних, телекомунікаційних та інформаційно-комунікаційних систем, зобов'язані дотримуватися норм, правил і стандартів…" (ч. 4–6 ст. 11 законопроекту) тощо.

Слід звернути увагу й на те, що з метою вирішення проблем забезпечення інформаційної безпеки РНБО ухвалила рішення «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» (введене в дію Указом Президента України від 1 травня 2014 року № 449/2014) [473], відповідно до якого Кабінету Міністрів України доручено розробити і внести на розгляд Верховної Ради України проект закону про кібернетичну безпеку України та законопроекти про внесення змін до деяких законів України, зокрема до законів "Про національну безпеку України", "Про інформацію", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про Службу безпеки України", "Про Державну службу спеціального зв'язку та захисту інформації України". Зміни спрямовувалися на приведення національного законодавства у відповідність із міжнародними стандартами з питань інформаційної та кібернетичної безпеки, вдосконалення системи формування та реалізації державної політики у сфері інформаційної безпеки України, а також протидії інформаційній агресії іноземних держав. При цьому у вказаних законопроектах слід було передбачити, зокрема: визначення механізму протидії негативному інформаційно-психологічному впливу (в тому числі шляхом заборони ретрансляції відповідних телевізійних каналів); запровадження для іноземних засобів масової інформації системи інформування та захисту журналістів, які працюють у місцях збройних конфліктів, вчинення терористичних актів, а також при ліквідації небезпечних злочинних груп, тощо. Натомість законопроект, що розглядається, спрямований на врегулювання проблем одночасно інформаційної безпеки та кібербезпеки. І хоча вказані поняття і є спорідненими, у документі вони чітко не відокремлені й не розмежовані,

що ускладнює їх розуміння.

Слід також зазначити, що Законом України ще від 7 вересня 2005 року № 2824-IV була ратифікована Конвенція Ради Європи про кіберзлочинність [426]. З метою імплементації її положень і Додаткових протоколів до неї були прийняті закони України «Про внесення змін до Кримінального та Кримінально-процесуального кодексів України» (щодо відповідальності за комп'ютерні злочини) від 23 грудня 2004 року [474] та «Про захист інформації в інформаційно-телекомунікаційних системах» [475]. На врегулювання відносин у цій сфері спрямовані також закони України «Про інформацію» [476], «Про науково-технічну інформацію» [477], «Про телекомунікації» [478], «Про доступ до публічної інформації» [479], «Про боротьбу з тероризмом» [480] та інші.

Тож законопроект з питань забезпечення інформаційної безпеки потребує узгодження із названими та іншими законодавчими актами. Тому при поданні його на розгляд Верховній Раді України належало виконати вимоги ч. 8 ст. 90 Регламенту Верховної Ради України, де зазначено: «…якщо для реалізації положень поданого законопроекту після його прийняття необхідні зміни до інших законів, такі зміни мають викладатися в розділі "Перехідні положення" цього законопроекту або в одночасно внесеному його ініціатором окремому законопроекті. До законопроекту додається перелік законів та інших нормативних актів, прийняття або перегляд яких необхідно здійснити для реалізації положень законопроекту в разі його прийняття» [481].

Таким чином, ретроспективний огляд спроб реалізації ідеї щодо розробки єдиного установчого нормативно-правового акту – закону з питань інформаційної безпеки дозволяє дійти висновку, що сьогодні такий закон має чітко визначати сферу правового регулювання, засадничі принципи забезпечення інформаційної безпеки, основні загрози правам та інтересам людини, суспільства й держави, котрі цим законом охороняються, зміст і пріоритетні напрями державної політики у цій сфері

та засоби її реалізації, перелік та компетенцію органів державної влади, що забезпечують різні складові інформаційної безпеки. Законом мають також передбачатися правові основи цих складових – захисту державної та іншої таємниці, інформації з різними правовими режимами, персональних даних, а також відповідальності за правопорушення в цій сфері. Нарешті, закон має уніфікувати й удосконалити понятійний апарат і термінологію регульованої сфери, оскільки в теперішній час із цим спостерігаються чималі проблеми.

Теоретичне обґрунтування вказаного закону має спиратися на сформовану у структурі вітчизняної системи права самостійну підгалузь – правове забезпечення інформаційної безпеки, а також відповідну законодавчу підгалузь, положення якої нині містяться в багатьох законодавчих актах різних галузей. Тому головним завданням законодавця вбачається, як уже зазначалося, саме систематизація й усунення наявних недоліків цих норм і положень з урахуванням комплексної природи вказаної підгалузі права та її взаємодії з іншими правовими галузями і структурними утвореннями. Тобто, належить виявляти правові джерела не лише забезпечення інформаційної безпеки, а й законодавчих актів, котрі взаємодіють з цією підгалуззю, з метою формування стрункої, позбавленої внутрішніх суперечностей системи відповідного законодавства.

Спробуємо змоделювати структурно-змістову схему пропонованого закону.

Розділ 1. Має розкривати найзагальніші питання, зокрема:

мета та сфера дії цього закону;

основні поняття (терміни), що в ньому вживаються;

принципи забезпечення інформаційної безпеки, його суб’єкти та об’єкти;

перелік актів законодавства, котрі цю сферу регулюють;

загальна структура законодавства про інформаційну безпеку.

Зрозуміло, що положення цієї глави (як і закону загалом) мають

відповідати Конституції України, Доктрині інформаційної безпеки України, а також міжнародно-правовим нормам і принципам.

Мета закону – правове регулювання діяльності із забезпечення інформаційної безпеки держави, тобто стану захищеності й балансу інтересів суб'єктів інформаційної сфери – людини, суспільства, держави.

Понятійний, термінологічний апарат цього системоутворювального закону має бути систематизованим й уніфікованим, містити коректно сформульовані визначення. Убачається за потрібне поряд з іншими визначити такі поняття, як: «інформаційна безпека держави», «захист інформації», «безпека інформації», «інформаційно-психологічна безпека», «стандарти інформаційної безпеки», «шкідливий (негативний) інформаційний вплив», «методи й засоби шкідливого інформаційного впливу» та інші. Чинником успішного виконання цього непростого наукового завдання є «проходження у професійній рефлексії юридичного явища від простого знакового заміщення до власне поняття як знаннєвої конструкції. Цей процес на початковому етапі збігається з юридичною діяльністю, юридичною практикою й відокремлюється від неї в результаті професійної рефлексії, дослідження права». Тому ретельний семантико-змістовий аналіз кожного терміна чи термінологічного сполучення, що включаються до понятійного апарату, специфіки їх уведення в науковий обіг та практики вживання в чинному законодавстві є обов'язковою умовою при розробці закону.

Об'єкт правового регулювання закону – відносини, які складаються у зв'язку з виникненням загроз і викликів правам і законним інтересам суб'єктів цих відносин в інформаційній сфері. Зокрема, це стосується й інформаційного впливу на психіку людини, людську й суспільну свідомість.

Суб'єкти правового регулювання закону – людина, суспільство, держава; органи державного управління, до компетенції яких входить забезпечення інформаційної безпеки; особа, права та/чи законні інтереси

котрої в інформаційній сфері були в будь-який неправомірний спосіб порушені.

Щодо загальної структури законодавства, котре регулює сферу інформаційної безпеки, закріплення якої в даному законі вбачається вельми важливим. Системоутворювальним, базовим законодавчим актом має бути власне сам закон про інформаційну безпеку. Позаяк решта законів не повинні суперечити базовому, його прийняття означатиме потребу ретельного вивчення чинного законодавства й приведення його у відповідність.

Уважаємо, що засадничими положеннями побудови вказаного закону, як і діяльності із забезпечення інформаційної безпеки, мають стати такі принципи:

примат прав і свобод людини і громадянина; цей закріплений у міжнародному праві принцип, що віддзеркалює сутність та межі діяльності із забезпечення інформаційної безпеки, є основоположним; у Доктрині інформаційної безпеки України дотримання прав і свобод людини в інформаційній сфері віднесене до першорядних національних інтересів нашої країни;

збалансованість інтересів особи, суспільства та держави; цей принцип також передбачений Доктриною інформаційної безпеки України й випливає із першого, позаяк законність інтересів кожної людини простягається до меж прав і свобод інших людей, а також інтересів суспільства й держави, якраз і зумовлених потребою захисту від посягань на ці права і свободи. Адже саме цим урешті-решт спричинені обмеження, пов’язані, приміром, з охороною державної таємниці, захистом персональних даних тощо;

відповідність безпекових заходів ступеню загроз; також випливає із попереднього принципу. Для запобігання загрозам в інформаційній сфері та їх усунення належить застосовувати заходи, адекватні їх реальному рівню, з мінімально необхідним обмеженням прав і свобод громадян;

монополія держави на розробку й виготовлення спеціальних засобів інформаційного, в тому числі інформаційно-психологічного, впливу; в умовах агресії РФ це означає заборону в Україні певної шкідливої інформації, певних антигуманних інформаційно-психологічних технологій, які цілком слушно багатьма правниками називаються інформаційною зброєю;

прозорість, гласність і контроль громадянського суспільства у сфері забезпечення інформаційної безпеки; тобто, відповідно до Закону України «Про доступ до публічної інформації» будь-які відомості про діяльність органів державного управління, місцевого самоврядування щодо забезпечення інформаційної безпеки мають бути відкритими й доступними для ознайомлення громадян, якщо тільки вони не становить державну чи іншу передбачену законом таємницю;

обов'язковість залучення до діяльності із забезпечення інформаційної безпеки громадських організацій; реалізація цього принципу, котрий випливає із попереднього та принципу збалансованості інтересів людини, суспільства й держави, дає змогу шляхом громадської оцінки законопроектів, пов'язаних з інформаційною сферою, значно повніше враховувати інтереси різних верств населення, підвищити якість відповідного законодавства.

Загрози інформаційній безпеці. Їх перелік наведено в Доктрині інформаційної безпеки України, й він цілком, на наш погляд, відповідає реаліям сьогодення. Якщо визначати їх у цілому, то це – сукупність чинників, котрі можуть призвести до порушення прав і свобод громадян, а також законних інтересів людини, суспільства й держави в інформаційній сфері.

Розділ 2. Загальні засади функціонування державної системи забезпечення інформаційної безпеки. Тут слід визначити пріоритетні завдання у цій сфері, головним із яких убачається створення й удосконалення відповідного законодавства. На його основі має бути

сформована вказана система задля неухильного втілення уповноваженими державними органами законодавчих вимог у цій сфері. Функції координації цієї діяльності доцільно покласти на Службу безпеки України.

Окрім виконання охоронних завдань, діяльність державних органів у цій сфері має бути спрямована на збереження й розширення єдиного інформаційного, духовного, мовного простору України, традицій українського народу й суспільної моралі, розвиток правової свідомості й культури населення стосовно інформаційної безпеки, просвіту громадян з питань безпечного користування інформаційними технологіями, захисту від шкідливих інформаційних впливів тощо.

Основні функції державних органів у досліджуваній сфері випливають із наведених вище завдань. Це насамперед: захист інформаційних систем і ресурсів держави, таємних відомостей та іншої інформації з обмеженим доступом; виявлення фактів шкідливих інформаційних впливів та суб'єктів, що їх здійснюють, нейтралізація та припинення їх протиправної діяльності; розробка нових і вдосконалення існуючих методів і засобів запобігання та протидії загрозам інформаційній безпеці людини, суспільства, держави; організація чіткого функціонування дозвільної, експертної та контрольної систем у вказаній сфері; стандартизація галузі; технічна, правова та інша підготовка висококваліфікованих фахівців з питань забезпечення інформаційної безпеки; розвиток продуктивного міжнародного співробітництва з питань інформаційної безпеки, приведення вітчизняного законодавства у відповідність до міжнародно-правових актів у цій сфері тощо.

Задля реалізації державної політики у сфері забезпечення інформаційної безпеки відповідно до наведених вище принципів, завдань і функцій має бути створена ефективна державна система. Крім уповноважених державних органів, її мають складати науково-дослідницькі, науково-технічні установи, проектні, конструкторські та інші організації, котрі провадять наукові дослідження й розробляють

технічні засоби, а також освітні заклади, які займаються підготовкою, перепідготовкою та підвищенням кваліфікації відповідних кадрів. Узгоджені дії вказаних суб'єктів забезпечуються шляхом ліцензійної, сертифікаційної, експертної та контрольної діяльності уповноважених на це органів у сфері забезпечення інформаційної безпеки, формування державних замовлень на відповідні наукові дослідження, освітні та інші послуги тощо.

Комплекс засобів, що їх застосовує державна система інформаційної безпеки, має гарантувати належний її рівень, у тому числі убезпечити суспільство від шкідливих інформаційно-психологічних впливів. Не останню роль у цьому має відіграти згадуване вище ліцензування, основні аспекти якого, зокрема умови отримання ліцензії, слід, на нашу думку, передбачити в базовому законі. Так, необхідною умовою отримання ліцензії вбачається сертифікація методів і засобів, які застосовуються під час проведення діяльності, пов'язаної з інформаційною безпекою.

Що стосується шкідливих інформаційних впливів, то достеменно виявити їх можна лише шляхом спеціальної експертизи. Остання проводиться для виявлення загроз інформаційній безпеці за державними стандартами й за дорученням відповідно уповноважених державних органів.

Допускається також заявний порядок проведення таких експертиз, тому варто, на нашу думку, закріпити окремий механізм розгляду вказаних запитів громадян. Зокрема, проведення подібної державної експертизи доцільно включити до необхідних заходів надання реабілітаційної допомоги людині, котра зазнала шкідливого інформаційно-психологічного впливу.

Необхідним елементом державної системи забезпечення інформаційної безпеки має також бути ефективний контроль за її достатністю та ефективністю, а також за дотриманням законності в усіх аспектах її функціонування.

***Розділ* 3**. Загальні питання забезпечення безпеки інформації з обмеженим доступом: підстави та принципи віднесення відомостей до категорії інформації з обмеженим доступом (таємна, конфіденційна), види інформації з обмеженим доступом (державна, комерційна, лікарська та ін. таємниця; для службового користування тощо); загальні засади захисту інформації з обмеженим доступом.

***Розділ* 4**. Загальні питання захисту відкритої (загальнодоступної) інформації від протиправних маніпуляцій з нею (викривлення, приховування, блокування тощо), зокрема: засади та вимоги до захисту інформації в загальнодоступних державних мережах; інформаційно-правові аспекти (на відміну від цивільно-правових) захисту об'єктів інтелектуальної власності (державна реєстрація, акредитація тощо) та ін.

***Розділ* 5.** Загальні засади захисту від недостовірної та шкідливої інформації, негативного інформаційно-психологічного впливу. Тут варто, на наш погляд, зазначити загрози суб'єктам інформаційних відносин, спричинені застосуванням спеціальних методів і засобів інформаційно-психологічного впливу, зокрема: маніпулювання особистісною та суспільною свідомістю, навіювання хибних думок і провокування неправильних дій, завдання шкоди здоров'ю та життю людини тощо.

Виходячи із принципу монополії держави на застосування методів і засобів інформаційно-психологічного впливу, треба передбачити вичерпний перелік підстав, коли воно може бути правомірним, а саме:

1) без відома об'єктів інформаційно-психологічного впливу:

у надзвичайних ситуаціях (стихійні лиха, катастрофи техногенного чи іншого характеру тощо) – для рятування людей, ліквідації наслідків та ін.;

під час воєнних дій проти зовнішнього агресора, проведення антитерористичних, миротворчих операцій;

2) за згодою об'єктів інформаційно-психологічного впливу:

з науковою метою (психічні, психологічні дослідження тощо);

під час підготовки фахівців:

які застосовують методи і засоби психологічного впливу;

чия діяльність пов’язана з екстремальними та надзвичайними ситуаціями;

які займаються антитерористичною діяльністю;

з інформаційної безпеки.

Крім того, вбачається доцільним врегулювати питання захисту громадян, суспільства й держави від розповсюдження недостовірної інформації на шкоду їхнім законним інтересам (наприклад, матеріали вітчизняних та зарубіжних засобів масової інформації, спрямовані на дискредитацію окремих осіб, підрив суспільної злагоди, дестабілізацію ситуації у країні і т.п.). Слід передбачити право постраждалого суб’єкта на компенсацію завданої шкоди (моральної та/чи матеріальної) та публічне спростування недостовірних відомостей, а також порядок його реалізації.

***Розділ* 6**. Загальні питання протидії інформаційному екстремізму. Необхідно визначити вичерпний перелік чітких критеріїв, за якими інформація визнається екстремістською (що загрожує конституційному ладу України), зокрема, умисел суб’єкта її розповсюдження, конкретні умови оприлюднення тощо. Підкреслимо важливість чіткого формулювання вказаних критеріїв, аби уникнути багатозначності їх тлумачення, що може призвести до фактичного запровадження цензури. Належність інформації до екстремістської має встановлюватися спеціальною експертизою, питання щодо організації та проведення якої теж мають бути врегульовані цим законом.

***Розділ* 7**. Види відповідальності за правопорушення, пов’язані зі сферою інформаційної безпеки. Слід передбачити випадки застосування кожного з видів відповідальності – дисциплінарної, цивільно-правової, адміністративної, кримінальної.

Джерела та порядок фінансування діяльності із забезпечення інформаційної безпеки. Додамо, що обсяги бюджетного фінансування

залежатимуть, зокрема, від того, чи буде створений спеціальний управлінський орган для керування державною системою забезпечення інформаційної безпеки або ж ці функції розподілятимуться між існуючими владними інститутами.

Підсумовуючи міркування стосовно запропонованої моделі закону, зазначимо, що прийняття базового Закону України «Про інформаційну безпеку України» вбачається необхідним задля консолідації, вдосконалення відповідного законодавства, чіткої структуризації системи нормативно-правових актів у цій галузі, усунення наявних суперечностей, лакун та інших вад.

Цей закон має, на наш погляд, закріпити найзагальніші положення, які поширюватимуться на решту нормативно-правових актів у цій галузі, а саме: принципи правового забезпечення, структуру відповідного законодавства, єдині параметри правового забезпечення інформаційної безпеки, єдину термінологію.

Крім того, вказаний закон, синтезувавши норми підгалузі правового забезпечення інформаційної безпеки, може стати одним із базових при кодифікації вітчизняного законодавства у сфері інформації та створенні Інформаційного кодексу України.

Зрозуміло, що подальша розробка вказаного закону потребує клопіткого теоретичного осягнення, вивчення великих масивів різногалузевих матеріалів, залучення до цієї роботи провідних правників, наукових установ, досвідчених практиків. На заключних етапах для створення якісного нормативно-правового акта законодавець має продемонструвати справжнє юридичне мистецтво, «завданням якого є відшліфування правового матеріалу» [482, с. 34]. Тому проведене вище дослідження правової природи феномену правового забезпечення інформаційної безпеки, місця у вітчизняній системі права цього утворення (підгалузі), норми котрого мають скласти основний зміст майбутнього закону про інформаційну безпеку, вбачається вельми актуальним і

корисним.

У свою чергу, такий закон має стати основою для інших нормативних актів у сфері забезпечення інформаційної безпеки, а також керівних документів державної політики в інформаційній сфері та процесу стратегічного планування забезпечення інформаційної безпеки України.

Ураховуючи викладене, передчасним видається прийняття Верховною Радою України Закону «Про основні засади забезпечення кібербезпеки України» [144], адже він має виступати спеціальним щодо засадничого закону про інформаційну безпеку в цілому.

Відповідно до закону «Про основні засади забезпечення кібербезпеки України» за цю сферу, в рамках своїх повноважень, відповідальні міністерства, місцеві держадміністрації, органи місцевого самоврядування, правоохоронні органи, розвідка і контррозвідка, суб'єкти оперативно-розшукової діяльності. Крім того, забезпечення кібербезпеки країни покладено також на Збройні сили України, Нацбанк, підприємства, котрі належать до об'єктів критичної інфраструктури, підприємства і громадян, які працюють у сфері національних інформаційних ресурсів, інформаційних електронних послуг.

Суб'єкти забезпечення кібербезпеки мають робити все, що належить до їх компетенції, щоб не допустити використання кіберпростору з воєнною, розвідувально-підривною, терористичною чи іншою незаконною метою.

Об'єктами кібербезпеки в документі названі конституційні права, суспільство, розвиток інформсуспільства, держава, національні інтереси та об'єкти критичної інфраструктури й комунікаційні системи. При цьому порядок формування переліку об'єктів критичної інфраструктури має бути затверджений Кабінетом Міністрів.

Законом передбачено, що до об'єктів критичної інфраструктури можуть бути віднесені підприємства й установи, які: ведуть діяльність і надають послуги в галузях хімічної промисловості, енергетики,

транспорту, ІКТ, електронних комунікацій, банківсько-фінансовому секторі; надають послуги у сфері життєзабезпечення населення; є комунальними, аварійними й рятувальними службами; включені до переліку підприємств, що мають стратегічне значення для економіки.

Закон також вводить поняття Національної системи кібербезпеки, яка є сукупністю суб'єктів забезпечення кібербезпеки і взаємопов'язаних заходів різного характеру.

Дія закону не поширюється на відносини та послуги, пов'язані зі змістом інформації, що обробляється в комунікаційних або в технологічних системах; на соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), якщо такі інформаційні ресурси не містять інформацію, необхідність захисту якої встановлена законом, відносини та послуги, пов'язані з функціонуванням таких мереж і ресурсів; на комунікаційні системи, які не взаємодіють з публічними мережами електронних комунікацій, не підключені до мережі Інтернет чи інших глобальних мереж передачі даних (крім технологічних систем).

Особи, винні в порушенні законодавства у сфері нацбезпеки, електронних комунікацій і захисту інформації, якщо кіберпростір є місцем або способом злочину, несуть відповідальність за цивільним, адміністративним і кримінальним законодавством.

Одним з істотних моментів у прийнятому законі є фактичне прирівнювання злочинів у кіберпросторі до звичайних. Так, закон вводить у правовий обіг саме поняття «кіберзлочини», котре визначається як суспільно небезпечне діяння, за яке передбачена кримінальна відповідальність.

Закон є новаторським документом, оскільки він запровадив у законодавство України багато визначень важливих термінів – кіберзагроза, кібершпіонаж, кіберзлочинність, кібератака. Крім того, держава отримала розуміння того, хто за що відповідає у цій сфері. Фактично розподілено

ролі й сектори відповідальності між спеціальними суб'єктами: за НБУ закріплюються питання кібрбезопасності банків, уряд відповідає за розробку державної політики у сфері державної безпеки тощо.

Закон визначає необхідність впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки і кіберзахисту. Які це можуть бути стандарти? Це – NIST Cybersecurity Framework – фреймворк з кібербезпеки, розроблений американським інститутом стандартів, а також серія міжнародних стандартів ISO-27XXX з інформаційної кібербезпеки. Закон також передбачає участь України в міжнародних і європейських системах забезпечення кібербезпеки, що дасть змогу поліпшити комунікації з багатьма фахівцями й підняти рівень знань вітчизняних фахівців.

У контексті перспектив міжнародного співробітництва України у сфері забезпечення кібербезпеки слід згадати, зокрема, той факт, що наприкінці травня поточного року Палата представників американського Конгресу підтримала виділення $250 млн на безпекову допомогу Україні в рамках законопроекту про оборонний бюджет США на 2019 рік. Так, до цього документа включено основні положення проекту «Закону про співпрацю з Україною з питань кібербезпеки», відтак він передбачає допомогу Україні в посиленні власних спроможностей щодо захисту від кібератак, забезпеченні безпеки комп'ютерних мереж органів державної влади, зменшенні залежності від російських інформаційних та комунікаційних технологій, сприянні участі у програмах обміну інформацією. У законопроекті також підтверджується відданість США Хартії про стратегічне партнерство між Україною та США, Будапештському меморандуму про гарантії безпеки, підтримці співробітництва України з НАТО [483].

Утім, на думку значної кількості вітчизняних правознавців, подальше вдосконалення правового забезпечення інформаційної безпеки держави та правового регулювання інформаційної сфери в цілому має

відбуватися шляхом кодифікації – розробки та прийняття Інформаційного кодексу України (Кодексу України про інформацію). Тут варто згадати, що необхідність розробки такого кодексу декларувалося ще в указі Президента України Л. Кучми «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». Крім того, необхідність прийняття Інформаційного кодексу України законодавчо закріплена в «Основних засадах розвитку інформаційного суспільства в Україні на 2007–2015 роки».

Таким чином, протягом більше десятиліття ведуться численні як наукові дискусії так і практичні дебати щодо необхідності розробки та прийняття Інформаційного кодексу України. У результаті такого творчого діалогу сформувалися три основні підходи.

Розробник першого підходу – Державний комітет телебачення і радіомовлення України в основу Інформаційного кодексу пропонував покласти «Концепцію національної інформаційної політики», а також змінений відповідно до сучасних вимог суспільного розвитку Закон України «Про інформацію». Проте, позаяк упродовж останніх 10 років зазнали фіаско всі спроби прийняти «Концепцію державної інформаційної політики», такий підхід убачається малоперспективним.

Другий підхід розроблено групою фахівців Інституту держави і права імені В. Корецького. На їхню думку, Інформаційний кодекс має складатися з чотирьох частин:

1) базова (загальна), яка містила би системоутворювальні норми, що регулюють базові відносини у сфері інформації та інформатизації;

2) галузева частина, яка має регулювати інформаційні відносини в окремих сферах життя особи, держави, суспільства;

3) видові норми й норми, що регулюють інформаційні відносини суб’єктів у сфері створення, пошуку, одержання, використання, зберігання та поширення окремих видів (категорій) інформаційної продукції або в

окремих складових інформаційного процесу;

4) спеціальні норми, які регулюють відносини стосовно створення й використання інформаційних технологій і телекомунікаційних систем.

Нарешті, третій варіант було запропоновано Урядовою комісією з питань інформаційно-аналітичного забезпечення діяльності органів виконавчої влади у проекті «Концепції реформування законодавства України у сфері суспільних інформаційних відносин». Цей підхід передбачав триетапну систематизацію інформаційного законодавства:

1) інкорпорація законодавства – визначення ієрархічної системи та структури інформаційного законодавства на рівні правової доктрини;

2) виокремлення в системі законодавства галузі та її закріплення у Зводі законів України як розділу «Інформаційне законодавство»;

3) кодифікація – розробка і прийняття Верховною Радою України такого нормативного акта, як Кодекс України про інформацію.

При цьому систематизація інформаційного законодавства мала, на думку розробників, проводитися методом агрегації – вдосконалення окремих правових норм чи створення нових міжгалузевих правових інститутів не повинно порушувати цілісність та призначення інформаційного законодавства, а поліпшувати його дієвість у цілому. Проте, попри відмінності в підходах, правознавці наполягають на необхідності розробки та прийняття Інформаційного кодексу України та вважають за необхідне об’єднати в ньому механізми регулювання провідних суспільних відносин, об’єктом яких є інформація незалежно від форми, способу, засобу чи технології її поширення. Такий кодекс, на їхню думку, має чітко визначити об’єкт, предмети інформаційного права, суб’єкти інформаційних правовідносин, правовий режим доступу до інформації, а також передбачити механізми забезпечення інформаційного суверенітету України та забезпечення інформаційної безпеки громадян, суспільства та держави як складових національної безпеки України [484].

Тож, хоча сьогодні інформаційна сфера України є лідером за кількості

законів, які її регулюють, аналіз чинного вітчизняного законодавства свідчить про низку прогалин у законодавстві, зокрема в питаннях балансу безпеки і транспарентності, унормування діяльності з поширення інформації в мережі Інтернет, удосконалення захисту інтелектуальної власності в умовах розширення застосування інтернет-технологій тощо.

Для вирішення цієї проблеми держава потребує передусім осмисленої та чіткої системи (а не просто масиву, механічної сукупності) нормативно-правових актів, що визначають державну політику та регламентують напрями діяльності органів державної влади в інформаційній сфері, в тому числі в галузі забезпечення інформаційної безпеки. Така системність зумовлюється не лише очевидною необхідністю стандартизації та систематизації нормативно-правового поля, а й ієрархічною моделлю законодавства, закріпленою Конституцією України, забезпеченням практичної реалізації тріади «національні цінності – національні інтереси – національні цілі» [97, с. 233], потребою формування нерозривного зв'язку між національними цілями та напрямками діяльності держави.

Тут слід згадати, що наразі на офіційному рівні лише Рада національної безпеки і оборони України запропонувала певне бачення ієрархії керівних документів державної політики [485], хоча аргументації на користь саме такого підходу наведено не було, – доктрина → концепція → стратегія → програма → план. Науковці пропонують й інші варіанти побудови такої ієрархії. Приміром: концепція → доктрина → стратегія → програма (Г. Ситник) [486]; стратегія → концепція → доктрина → програма (А. Кузьменко) [487].

Отже, оскільки загальновизнаного підпорядкування керівних документів державної політики немає, необхідне нормативно-правове врегулювання цього питання. Однак, хоча сьогодні в Україні існує низка відповідних нормативно-правових актів [488-490], у жодному з них не розглядаються доктрини та концепції.

Зауважимо, що з 2011 року тривала підготовка проекту Закону

України «Про державне стратегічне планування», котрий мав закріпити термінологію, систему та класифікацію подібних документів. Проте й цей законопроект не був позбавлений істотних недоліків. По-перше, у тексті не згадуються концепції та доктрини (що свідчить про виключення із процесу унормування так званих концептуально-доктринальних актів, котрі характеризуються вищим рівнем абстрагування, ширшим колом питань і є первинними щодо стратегій), а також національні проекти, які вельми широко застосовуються в сучасній вітчизняній практиці державного управління.

Крім того, законопроект пропонував такі терміни стратегічного планування: довгострокове – понад 5 років, середньострокове – від 3 до 5 років та короткострокове – 1 рік. Це суперечить усталеним, «класичним» підходам, адже як у теорії [491, с. 18], так і на практиці періодичність стратегічного планування визначається так: довгострокове – 10-20 років, середньострокове – 4(5)-10 років, короткострокове – 1-3(4) роки.

Законопроект передбачав також взаємозв’язок між плануванням і проведенням виборів народних депутатів. Пропонувалося нормативне закріплення положення про пріоритетне значення для соціально-економічного розвитку держави, плановість якого мав би забезпечити цей закон, політичного чинника, передбачуваність якого складно забезпечити. Крім того, ця норма суперечить сутності стратегічного управління – досягнення першочерговості перспективного розвитку порівняно з політичними циклами й відповідно кон’юнктурними механізмами управління. Зрештою, цей законопроект було відхилено і знято з розгляду [492].

Аналогічними недоліками хибував альтернативний законопроект, розміщений для обговорення на сайті Міністерства економічного розвитку і торгівлі України наприкінці 2017 року [492].

Певною мірою питання стратегічного планування намагається впорядкувати проект Закону України «Про національну безпеку України»,

однак стосовно інформаційної безпеки обмежується лишень вказівкою на потребу розробки Стратегії кібербезпеки, яка «є основою для підготовки державних програм та нормативно-правових актів, що стосуються забезпечення кібербезпеки України» (ст. 31).

Відтак, позаяк кібербезпека, що вже неодноразово підкреслювалося, не може розглядатися відокремлено від інформаційної безпеки в цілому, пропонуємо скоригувати зміст цієї статті вказаного законопроекту, виклавши її в такій редакції:

«Стаття 31. Стратегія інформаційної та кібернетичної безпеки України

1. Стратегія інформаційної та кібербезпеки України – документ, в якому визначаються пріоритети національних інтересів України у сфері інформаційної та кібернетичної безпеки, загрози життєво важливим інтересам людини і громадянина, суспільства та держави в інформаційному та кібернетичному просторі, пріоритетні напрями, концептуальні підходи до формування та реалізації державної політики щодо безпечного функціонування інформаційного та кібернетичного простору.

2. Організація підготовки Стратегії інформаційної та кібернетичної безпеки України здійснюється Службою безпеки України спільно з Національним координаційним центром кібербезпеки після затвердження Стратегії національної безпеки України.

Стратегія інформаційної та кібернетичної безпеки України схвалюється рішенням Ради національної безпеки і оборони України та затверджується указом Президента України.

3. Стратегія інформаційної та кібернетичної безпеки України визначає, зокрема:

безпекове середовище (глобальні, регіональні та національні аспекти) у контексті забезпечення інформаційної та кібернетичної безпеки;

пріоритети у сфері захисту національних цінностей, реалізації національних інтересів та досягнення національних цілей України у

контексті забезпечення інформаційної та кібернетичної безпеки;

актуальні виклики і загрози інформаційній та кібернетичній безпеці з урахуванням особливостей безпекового середовища, а також зумовлені ними ризики;

основні напрями державної політики у сфері інформаційної та кібернетичної безпеки;

напрями та завдання реформування й розвитку, підвищення ефективності діяльності основних суб'єктів забезпечення інформаційної та кібернетичної безпеки;

систему управління ризиками інформаційній та кібернетичній безпеці;

ресурси, необхідні для її реалізації.

4. Стратегія інформаційної та кібернетичної безпеки України є основою для підготовки державних програм та нормативно-правових актів, що стосуються забезпечення інформаційної та кібернетичної безпеки України.

Реалізація Стратегії інформаційної та кібернетичної безпеки України здійснюється на основі національного оборонного, безпекового, економічного, інтелектуального потенціалу з використанням механізмів державно-приватного партнерства, а також із залученням міжнародної консультативної, фінансової, матеріально-технічної допомоги».

У цілому з метою формування чіткої та не перевантаженої зайвими видами документів ієрархії вбачається за доцільне:

- прирівняти «основні засади» до концепцій або доктрин, оскільки на практиці предметний обсяг цих документів збігається;

- чітко визначити та обґрунтувати ієрархію керівних документів державної політики – доктрин, концепцій, стратегій, програм, національних проектів та планів;

- щодо кожного виду документа передбачити форму та механізм набуття ними чинності;

- визначити та законодавчо закріпити структуру кожного з видів документів.

Уважаємо також, що слід підтримати пропозиції стосовно ранжування керівних документів державної політики та стратегічного планування у такий спосіб:

- I рівень (доктринальний – норми-начала): ДОКТРИНА – основні положення (основні принципи), відповідно до яких вирішуються найважливіші питання існування й розвитку тієї чи іншої держави або міжнародних відносин;

- II рівень (концептуальний – норми-принципи): КОНЦЕПЦІЯ – сукупність правових норм, які утворюють підґрунтя стратегії тієї чи іншої діяльності;

- III рівень (стратегічний – визначально-установчі норми): СТРАТЕГІЯ – сукупність правових норм, що визначають систему офіційних поглядів на місце та роль держави в сучасному світі, її життєво важливі національні цінності, сили, засоби й методи протидії загрозам;

- IV рівень (програмний – норми-правила): ПРОГРАМА – сукупність правових норм, правил поведінки, що безпосередньо регулюють діяльність суб'єктів забезпечення національної безпеки в конкретних умовах;

- V рівень (плановий – норми-правила поведінки): ПЛАН – деталізація діяльності суб'єктів забезпечення національної безпеки в конкретній обстановці [495].

5.2. Пріоритети розвитку правових основ державної політики України у сфері інформаційної безпеки

В умовах радикальних суспільних трансформацій і становлення єдиного світового інформаційного простору інформаційна безпека стає ключовим компонентом усієї системи національної безпеки країни, адже,

як зазначає В. Шерстюк, інформаційно-комунікаційні технології «за своїм впливом на політику, господарсько-економічне життя, духовно-ідеологічну сферу й умонастрої людей стали вирішальними й всеохоплюючими» [496, с. 48]. Відтак, політика у сфері забезпечення інформаційної безпеки та інформаційна політика в цілому стає важливим елементом діяльності владних структур будь-якого рівня.

Відтак ефективне забезпечення національної безпеки України передбачає необхідність розробки науково обґрунтованої державної політики та стратегії в інформаційній сфері та постійного моніторингу актуальних загроз інформаційній безпеці держави, пошуку ефективних заходів для забезпечення безпеки в усіх її сферах, захисту від інформаційних загроз та реалізації права на отримання достовірної інформації.

Відомий вчений В. Пилипчук серед проблемних питань забезпечення інформаційної безпеки держави найбільш пріоритетною вважає ефективність державної інформаційної політики та політики національної безпеки в інформаційній сфері [181, с. 24].

Зростання залежності сучасного суспільства від стійкого функціонування інформаційної інфраструктури робить реалізацію національних інтересів України в інформаційній сфері важливим чинником національної безпеки. Тож для України сьогодні необхідним кроком на шляху до інформаційного майбутнього є розробка цілісної гнучкої динамічної державної політики у сфері забезпечення інформаційної безпеки, яка враховуватиме багатоаспектність цього явища, перспективні тенденції змін інформаційного простору, особливості геополітичного становища, економічного стану країни і знайде своє відображення у суспільній свідомості, а також на правовому концептуально-доктринальному рівні та в ефективному інформаційному законодавстві [497, с. 178].

Досліджуючи проблеми формування та реалізації державної

політики у сфері забезпечення інформаційної безпеки України на сучасному етапі, передусім слід з'ясувати, що ж таке «державна політика у сфері забезпечення інформаційної безпеки», і як зміст цього формулювання співвідноситься з поняттям «інформаційна політика держави».

Інформаційна політика держави в сучасному політичному процесі розглядається як окремий вид політичної діяльності. Основні підходи до проблеми становлення державної інформаційної політики сформувалися ще в XIX ст. і отримали новий імпульс до розвитку в 1960-х роках у зв'язку із входженням розвинених країн у стадію інформаційного суспільства [498, с. 44-45], коли ЗМІ з інструменту відображення реальності перетворилися на засіб її творення [499, с. 74].

За визначенням В. Попова, інформаційна політика – «це особлива сфера життєдіяльності, пов'язана з відтворенням і поширенням інформації, котра задовольняє інтереси держави й громадянського суспільства і спрямована на забезпечення конструктивного діалогу між ними та їхніми представниками» [500, с. 38]. Інакше тлумачить цей термін Ю. Нісневич, який вважає, що «інформаційна політика – це сукупність цілей, що відображають національні інтереси в інформаційній сфері, завдання державного управління, управлінських рішень і методів їх реалізації, розроблених і реалізованих державною владою для регулювання процесів інформаційної взаємодії» [501, с. 8]. Натомість А. Манойло визначає інформаційну політику як «діяльність системи державної влади й управління щодо створення умов для успішного, стійкого й безперервного розвитку системи соціально-політичних відносин суспільства в умовах інтенсивного впливу зовнішніх і внутрішніх чинників, котрі чинять на систему як стабілізуючий, так і деструктивний інформаційно-психологічний вплив» [502, с. 330]. На думку Г.Г. Почепцова, інформаційну політику слід розглядати як сукупність принципів, підходів, визначальних законів функціонування інформаційної сфери [503, с. 12].

Своєю чергою С. Бондаренко під державною інформаційною політикою розуміє цілеспрямовану діяльність центральних органів влади з формування політико-релевантного знання про державу, його поширення та управління в інформаційному просторі з метою досягнення політичних цілей і захисту національних інтересів [504, с. 113]. Інформаційну політику держави розглядають також як діяльність останньої в інформаційній сфері, спрямовану на задоволення інформаційних потреб людини і громадянина через формування відкритого інформаційного суспільства на основі розвитку єдиного інформаційного простору цілісної держави та його інтеграції у світовий інформаційний простір з урахуванням національних особливостей та інтересів при забезпеченні інформаційної безпеки на внутрішньодержавному та міжнародному рівнях [505, с. 6].

Виходячи із цього, основною метою державної інформаційної політики України є забезпечення: захисту інформаційного суверенітету держави (особливо захист національного інформаційного простору з інформаційним ресурсом і систем формування масового суспільної свідомості) в сучасних умовах глобалізації та інтернаціоналізації процесів в інформаційній сфері; рівня інформаційної достатності для прийняття рішень державними органами, підприємствами та громадянами; реалізації конституційних прав і свобод громадян, суспільства і держави на інформацію [506, с. 153]. Головною ж метою державної політики у сфері забезпечення інформаційної безпеки при цьому є управління реальними та потенційними загрозами, спрямоване на створення необхідних умов для задоволення інформаційних потреб людини та громадянина, а також реалізації національних інтересів. Відтак, як зазначають Р. Шаповал та В. Клочко, державна політика у сфері забезпечення інформаційної безпеки України – це діяльність державно-правових інституцій щодо управління реальними та потенційними загрозами й небезпеками з метою задоволення інформаційних потреб людини та громадянина, а також реалізації національних інтересів, тож державна інформаційна політика та державна

політика у сфері забезпечення інформаційної безпеки співвідносяться як ціле та частина [505, с. 6]. Я. Жарков також уважає, що державна політика у сфері забезпечення інформаційної безпеки України є невід'ємною складовою державної політики національної безпеки України і становить офіційно прийняту систему поглядів та практичну діяльність органів державної влади й управління, спрямовану на забезпечення такого стану соціальних суб'єктів, за якого дія будь-якої інформаційної загрози не призводить до зниження рівня їх інформаційної безпеки нижче мінімально припустимого [507, с. 187].

Отже, інформаційна безпека забезпечується проведенням єдиної державної політики в інформаційній сфері, системою заходів економічного, політичного й організаційного характеру, які є адекватними загрозам національній безпеці, а також можливостям держави щодо управління відповідними ризиками.

Система забезпечення інформаційної безпеки є інструментом реалізації державної політики у сфері забезпечення інформаційної безпеки. Її головне призначення полягає в досягненні мети національної безпеки в інформаційній сфері, а відтак її основною функцією є забезпечення збалансованого існування інтересів особи, суспільства й держави в інформаційній сфері.

Державна політика у сфері забезпечення інформаційної безпеки має три основних вектори:

1) захист інформаційних прав і свобод людини;

2) захист державної безпеки в інформаційній сфері та національного інформаційного ринку;

3) захист економічних інтересів держави в інформаційній сфері, національних виробників інформаційної продукції [142, с. 146].

Єдність і взаємозв'язок напрямків державної політики у сфері забезпечення інформаційної безпеки має забезпечуватися визначеними на законодавчому рівні правовими механізмами, з-поміж яких: чіткі цілі й

завдання державної політики; взаємодія державних і громадських інститутів з реалізації міжвідомчих напрямів державної політики; організація системи інформування суб'єктів, котрі функціонують у сфері забезпечення інформаційної безпеки, про актуальні проблеми, виявлення потенційних і реальних загроз та їх джерела, а також доцільні заходи й засоби щодо їх попередження, нейтралізації та ліквідації можливих наслідків; узгоджені й цілеспрямовані дії суб'єктів, що діють у різних сферах життєдіяльності суспільства й держави з питань адекватного реагування на виявлені потенційні та реальні загрози; загальнодержавне керівництво, координація та контроль у сфері забезпечення інформаційної безпеки [508, с. 170].

Сучасна державна політика у сфері забезпечення інформаційної безпеки ґрунтується на дотриманні Конституції й законів України «Про інформацію», «Про доступ до публічної інформації», «Про зв'язок», «Про авторське право та суміжні права», «Про державну таємницю», «Про друковані засоби масової інформації (пресу) в Україні», «Про телекомунікації», Кримінального та Цивільного кодексів України та ін. Проте в нашій державі досі не прийнятий закон, який би врегулював основні напрями державної інформаційної політики. Тому в Україні не вироблена чітка позиція (стратегія) розвитку інформаційної безпеки держави, хоча протягом 2002–2010 років спроби унормувати цю сферу здійснювалися. Лише після анексії Криму і початку війни на сході України, указом Президента було затверджене рішення Ради національної безпеки і оборони України «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України». Відповідно до цього указу розроблені та прийняті законодавчі акти щодо протидії інформаційній агресії іноземних держав, а також протидії негативному інформаційному впливу. Попри набуття цими законами чинності, повноцінна їх реалізація подекуди унеможливлюється браком технічних можливостей нашої держави.

У контексті потреби вдосконалення нормативно-правового забезпечення та попередження й нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері з початком гібридної війни проти України виникла необхідність кардинальних змін у системі забезпечення інформаційної безпеки нашої держави. Основний план відповідних дій запроваджено рішенням РНБО від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України», затвердженого Указом Президента України № 449/2014 від 01 травня 2014 року [191]. Цим рішенням Кабінету Міністрів України доручалося розробити і внести на розгляд парламенту законопроекти про зміни в законах України, які мають стосунок до протидії інформаційній агресії іноземних держав. Зокрема, слід було визначитися з механізмом протидії негативному інформаційно-психологічному впливу, в тому числі шляхом заборони ретрансляції телевізійних каналів, а також із системою інформування та захисту іноземних журналістів, які працюють у місцях збройних конфліктів, вчинення терористичних актів, при ліквідації небезпечних злочинних груп. Крім того, належало розробити проект стратегії розвитку інформаційного простору України, розробити і впровадити комплексні заходи організаційного, інформаційного і роз’яснювального характеру щодо всебічного висвітлення заходів з реалізації державної політики у сфері забезпечення інформаційної безпеки, а також посилити контроль за дотриманням законодавства з питань інформаційно-психологічної та кібернетичної безпеки. Відповідно до вказаного плану заходів було розроблено, зокрема, Стратегію кібербезпеки України, відповідно до якої розвиток та безпека кіберпростору, запровадження електронного урядування, гарантування безпеки і сталого функціонування електронних комунікацій та державних електронних інформаційних ресурсів мають бути складовими державної політики у сфері розвитку інформаційного простору та становлення інформаційного суспільства в Україні [165], а

також Доктрину інформаційної безпеки України [190].

В експертному середовищі й українському суспільстві взагалі публікація Доктрини інформаційної безпеки викликала неоднозначну реакцію. Амплітуда коливань оцінок змінювалася від визнання важливості й упевненості, що документа слід було прийняти ще кілька років тому, до звинувачень у його подібності з аналогічною російською доктриною інформаційної безпеки, прийнятою у грудні 2016 року. Пригадали експерти і так званий «пакет Ярової» – «антитерористичні» законопроекти, внесені депутатом російської Держдуми Росії І. Яровою і сенатором В. Озеровим, які передбачають жорстке обмеження прав і свобод громадян РФ. Деякі фахівці висловили також побоювання, що й наша доктрина може посприяти обмеженню свободи слова в Україні та інших прав її громадян.

Зокрема, з-поміж ключових аспектів Доктрини завідувач відділу досліджень інформаційного суспільства та інформаційних стратегій Національного інституту стратегічних досліджень Д. Дубов відзначив викладене державою бачення розвитку й функціонування національного інформаційного простору і визначення, що Російська Федерація є противником, який веде системну інформаційну війну. «У документі є пропозиції, як реагувати на агресію та забезпечувати інформацією громадян. Доктрина також визначає поняття “стратегічного наративу” і вказує, що медіа мають самі себе регулювати, але при цьому повинні нести соціальну відповідальність», – зазначає дослідник [509]. За його оцінкою, факт визначення цих понять і їх винесення на публічне обговорення є важливим. Щоправда, між доктриною та імплементацією її положень лежить тривалий законотворчий шлях.

Своєю чергою, експерт зі стратегічних комунікацій громадського об’єднання «Інформаційна безпека», екс-заступник міністра інформаційної політики Т. Попова вважає Доктрину інформаційної безпеки помітним кроком уперед у діяльності держави щодо протидії російській інформаційній агресії. На її думку, головним досягненням цього документа

є спроба визначити та гармонізувати повноваження органів влади, силових структур щодо їхньої діяльності із захисту інтересів суспільства й держави в інформаційній сфері, національного інформаційного простору [509]. До позитиву Т. Попова відносить і нормативне визначення низки термінів (передусім поняття «наратив»), розмежування питань урядових і стратегічних комунікацій, що, на її думку, дасть змогу позбутися певного дублювання і сконцентрувати проблематику стратегічних комунікацій переважно в контексті діяльності сектору безпеки та оборони держави.

Водночас, задекларована Доктриною мета – «уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни», з погляду Т. Попової, більше «личить» іншому документу, який має визначати основні засади державної інформаційної політики, особливо її структуру та зміст. (Сьогодні такого документа на державному рівні в Україні не існує. До питання стосовно документів стратегічного планування ми повернемося дещо нижче). Т.Попова вважає також, що Доктрина лишає відкритими питання стосовно методології підходів до проблематики забезпечення інформаційної безпеки, адже необхідним є передусім коректне визначення співвідношення понять «інформаційна безпека» та «кібербезпека». Вона констатує, що українська наука чітко обґрунтувала необхідність розгляду національного сегмента кіберпростору як складової частини інформаційного простору держави, з чого випливає й логічність розгляду питань кібербезпеки в контексті інформаційної безпеки. І хоча деякі країни вирішували це питання в інший спосіб, наразі вони також доходять висновку, що розгляд інформаційного середовища та кіберсередовища (і, відповідно, інформаційної безпеки та кібербезпеки) як окремих паралельних феноменів (напрямів діяльності) є необґрунтованим та штучним (тобто, такий підхід визнано методологічно помилковим). Так, в аналітичній доповіді «Information Warfare Boundaries for anArmy in a

Wireless World», підготовленій корпорацією RAND на замовлення сухопутних військ ЗС США у 2013 році зазначено, що у практичній діяльності органів військового управління, суб'єктів забезпечення інформаційної безпеки інформаційне середовище слід розглядати як єдине середовище у двох вимірах – людському й технічному. На жаль, констатує Т. Попова, в діяльності українських державних структур відбулося штучне відокремлення інформаційної безпеки та кібербезпеки, що відобразилося в низці нормативно-правових актів. Розбалансованість і розпорошеність діяльності, інституційна невизначеність за такого підходу є чинником зниження ефективності заходів інформаційного протиборства з боку України, вважає вона. З огляду на вказані проблеми Т. Попова вбачає низку ризиків щодо успіху реалізації положень Доктрини, а саме:

- невідповідність між рівнем нормативного регулювання того чи іншого напряму діяльності державних органів та реальними кроками щодо виконання ними положень правових актів. Щоб не допустити повторення цієї тенденції стосовно Доктрини, доведеться дуже ретельно попрацювати над новими нормативно-правовими актами, оскільки Доктрина не є нормативним актом прямої дії, яка регулює виключно всі аспекти діяльності щодо забезпечення інформаційної безпеки. Вона окреслює стратегічні питання, а центральні органи виконавчої влади, структури сектору безпеки та оборони мають деталізувати та конкретизувати її вимоги в інших нормативних документах;

- відсутність реально працюючих механізмів координації діяльності у сфері інформаційної безпеки. Деякі успішні приклади горизонтальної взаємодії органів влади, волонтерські акції, проекти у форматі «ручного управління» є винятком із правил, які лише підтверджують необхідність офіційної координації з боку держави. Безумовно, необхідність централізації діяльності, дієвих алгоритмів координації та контролю в тексті Доктрини задекларовані. Але, з іншого боку, механізми втілення зазначеного не прописані. Це є підставою говорити про певні ризики, бо

РНБО отримала завдання координації діяльності, не маючи при цьому необхідних повноважень і ресурсів, які притаманні центральним органам виконавчої влади. Мінінформполітики в існуючому вигляді також не зможе виконати певні завдання, не будучи до того ж офіційною складовою частиною сектору безпеки та оборони держави і суб'єктом боротьби з тероризмом. І якщо Мінінформполітики визнано фактично головним суб'єктом забезпечення інформаційної безпеки з-поміж інших міністерств і відомств виконавчої влади, то це накладає певні зобов'язання, особливо стосовно активних заходів інформаційного впливу, координації діяльності силових структур, які, між іншим, зобов'язані займатися такими чутливими заходами, як інформаційні та психологічні операції [509].

Відомий експерь Д. Дуцик у свою чергу зауважила, що в Доктрину не включено Міністерство з окупованих територій, хоча за урядовим планом дій воно також має залучатися до виконання завдань у сфері забезпечення інформаційної безпеки. Вона також підкреслила, що «розробники Доктрини, на жаль, не дослухалися до частини рекомендацій, які надавалися експертами від ОБСЄ та НАТО, коли Міністерство інформаційної політики представляло перший варіант документа. Цей варіант більш структурований. Проте залишається багато питань до того, як прописано національні інтереси України в інформаційній сфері, як визначаються загрози» тощо [510].

Координатор групи «Інформаційний опір» народний депутат Д. Тимчук, коментуючи прийняття Доктрини інформаційної безпеки, зазначив, що такий документ країні потрібен давно, тому дивно, що він з'явився лише в 2017 році. «Ще до початку російської агресії, а особливо під час неї ми бачили, що втримати "інформаційний фронт" для України не менш важливо, ніж військовий. І насторожувало, що три роки жодних концептуальних документів, які б стосувалися питання безпеки інформаційної галузі, по суті, запропоновано не було», – зауважив він. У Доктрині розписана відповідальність конкретних структур у сфері

інформаційного суверенітету, що є головним, уважає Д. Тимчук. При цьому Доктрина не позбавлена певних недоліків, передусім у частині дублювання повноважень, адже завдання, які ставить документ перед Міністерством інформаційної політики, перетинаються з обов'язками спецслужб у галузі захисту інформаційної безпеки. Тож, говорить Д. Тимчук, «є відповідні структури у складі СБУ, у них своя логіка роботи. Ці структури можуть не лише моніторити, а й у межах свого відомства проводити розслідування, починати карні справи, тобто здійснювати повний цикл заходів, аж до доведення до суду. МІП такими можливостями не оперує, не може займатися оперативно-розшуковою діяльністю і в певній частині просто дублює повноваження СБУ щодо моніторингу... Як на мене, доцільніше було б підсилити ті структури, які є у складі наших спецслужб. За моєю інформацію, там не вистачає робочих рук, ресурсів, замість цього передбачається дублювання функцій» [509].

Декларативним документом уважає Доктрину й голова Інституту масової інформації О. Романюк. Також, на її думку, поки зарано говорити, чи стане вона механізмом цензури. «Для того щоб Доктрина запрацювала на практиці, потрібні зміни в законодавстві, – констатує експерт. – І взагалі щось можна буде сказати тільки після практичного застосування Доктрини, трансформації її в конкретні механізми і закони. До цього оцінювати Доктрину сенсу немає – сама по собі вона цілком збалансована. Питання в тому, як її інтерпретують» [511].

За оцінкою медіа-експерта Н. Лігачової, Доктрина за своїм змістом є декларативною, і зрозуміти, в який спосіб реалізовуватимуться поставлені завдання, можна буде тільки з тієї законодавчо-нормативної бази, яка буде напрацьована далі. «Один з її недоліків, що положення Доктрини пов'язані перш за все з агресією Росії. Мені здається, що це свідчить про те, що Україна і автори Доктрини поки не мають уявлення, яким чином повинна забезпечуватися інформаційна безпека України, з урахуванням усіх загроз. Можна сказати, що це не стільки загальна Доктрина інформбезпеки,

скільки стратегія протидії загрозам з боку Росії нашій інформнебезпеці. Але те, що в нашій Доктрині згадується суспільне мовлення і розвиток медіа-грамотності населення і досить багато є про доступ до публічної інформації, великий плюс», – зазначає з цього приводу Н. Лігачова [512].

На думку політолога М. Спиридонова, небезпека Доктрини в тому, що у такий спосіб спробують контролювати не тільки ЗМІ, а й простих українців: «Моніторинг Інтернету, який здійснюватиме СБУ, Мінінформполітики, стосується і простих українців, так як Інтернет буде моніторитися на дуже розмитих підставах, що залишають широкий простір для зловживань. Якщо я, наприклад, критикую Прем'єр-міністра, мені можуть приписати, що це суперечить національним інтересам. Але все-таки, я думаю, більшою мірою це стосуватиметься експертів і блогерів, тому що вже до зовсім рядового українця руки не дійдуть. Якщо щось не подобається, критика влади наприклад, то відповідно до цієї Доктрини можуть контролюватися всі. Я не виключаю, що можуть бути в Україні проросійські блогери, які отримують гроші в Москві і зазіхають на національну безпеку, але в 90 % випадків це буде саме дубинка, якою будуть бити по неугодним владі» [513]. Щоби Доктрина нормально запрацювала, вважає політолог, потрібно чіткіше прописати, якими принципами влада керується, визначаючи загрозу нацбезпеці. «У документі загальні фрази, і під них можна підвести багато всього. Якщо проаналізувати стрічку в Facebook, то 60 % критичних публікацій там про те, що у країні відбувається, тобто за кожну другу публікацію можна висувати претензії», – підсумував експерт.

Депутат Верховної Ради України Д. Тимчук також спростовує побоювання щодо обмеження свободи слова. «Це не так. Утисків свободи слова немає. Деякі структури і до цього мали повноваження моніторингу медіа-ринку. Питання в іншому: як держава потім реагує на порушення. У нас, на превеликий жаль, держава через нечітке законодавство чи небажання суддів доводити справи до кінця не працює надміру ефективно

в питанні захисту інформаційного суверенітету. Є матеріали в ЗМІ, які дестабілізують ситуацію в країні, але не отримують жодних покарань. Бо там іде так звана м'яка форма пропаганди», – підкреслив нардеп [509].

Аналогічною є позиція й Міністерства інформаційної політики, речники якого переконують, що позицій, які обмежують громадянські права, у документі, котрий розглядається, немає. «Я не бачу, яким саме чином моніторинг соціальних мереж і ЗМІ може "сприяти цензурі". Українське законодавство і так на сьогодні містить норми, які зобов'язують правоохоронні органи відповідно реагувати на заклики до повалення конституційного ладу або порушення територіальної цілісності. У тому числі якщо такі заклики були опубліковані в ЗМІ, тобто моніторинг, у якомусь хаотичному порядку, здійснювався і так. Я можу запевнити, що Доктрина жодним чином не буде і не може бути застосована для скорочення прав і свобод громадян, які надані Конституцією. Більше того, за своєю логікою Доктрина є стратегічним документом і не може містити, та й не містить норм прямої дії. Вона визначає політику держави. Щодо відповідальності за пости в соціальних мережах, то, якщо ви відкриєте реєстр судових рішень в Україні, ви побачите, що подібні вироки там вже є», – зазначає, зокрема, Д. Золотухін [514].

Загалом експерти сходяться на думці, що поява Доктрини інформаційної безпеки України і набуття нею чинності ще не означає негайних радикальних змін в інформаційному просторі України, тим паче, що перебіг інформаційних воєн, як і будь-яких інших, багато в чому залежить від фінансової складової. Якщо Українська держава, окрім затвердження Доктрини, забезпечить ще й фінансову її підтримку, – на інформаційних фронтах з'явиться шанс на перемогу. Поки ж очевидним позитивом є те, що в Україні почали ставитися до інформаційного протистояння як до джерела цілком реальних загроз. У цілому слід констатувати, що визначення основних принципів державної інформаційної політики, розподіл повноважень і відповідальності

державних органів у забезпеченні інформаційної безпеки значно посилюють позиції України в інформаційному протистоянні та створюють, у разі прийняття на виконання рамкових положень Доктрини інформаційної безпеки відповідного законодавства, належний базис для ефективного подолання інформаційних загроз у гібридній війні, розгорнутій проти України Росією, та взагалі – до зміцнення інформаційної безпеки нашої країни [509].

Відзначаючи істотні позитивні зрушення щодо формування та реалізації державної політики у сфері забезпечення інформаційної безпеки, звернімо увагу й на численні проблемні аспекти цього напряму.

Так, уже понад десять років у країні ламаються списи навколо питання щодо закону про Концепцію національної (державної) інформаційної політики. Востаннє відповідний законопроект було відкликано з Верховної Ради 5 липня 2011 року, не зважаючи на попереднє прийняття його за основу [515]. Значною мірою це можна пояснити двома чинниками: відсутністю політичної волі для ухвалення такого нормативно-правового акта та сумнівами, як з боку державних чиновників, так і громадськості, щодо його необхідності (не в останню чергу через раніше взяті на себе Україною міжнародні зобов’язання в інформаційній сфері) [516].

Звісно, свою роль відіграє й недосконалість відповідних законопроектів. Зокрема, законопроект «Про Концепцію державної інформаційної політики» 2010 року передбачав схвалення законом України названої Концепції, якою визначатимуться мета, принципи, пріоритетні завдання та основні напрями діяльності держави у розвитку інформаційної сфери, що включає систему виробництва, використання ресурсів і регулювання суспільних відносин, пов’язаних з одержанням, використанням, поширенням та зберігання інформації. Одначе в даному разі слід, на нашу думку, виходити з того, що повноваження Верховної Ради України визначаються виключно Конституцією України, на що

неодноразово вказував Конституційний суд України. Це випливає зі змісту ч. 2 ст. 85 Основного Закону, де до повноважень парламенту України віднесено “прийняття законів”, “визначення засад внутрішньої і зовнішньої політики”, “затвердження загальнодержавних програм економічного, науково-технічного, соціального, національно-культурного розвитку, охорони довкілля” та інші. Що ж стосується затвердження документів на кшталт концепцій, яким не притаманний нормативний характер, то Конституція не наділяє Верховну Раду такими повноваженнями, що ставить під сумнів легітимність схвалення Концепції державної інформаційної політики законом.

У свою чергу, законопроектом «Про основні засади державної інформаційної політики» (реєстр. № 7251) пропонувалося схвалити законом України ці Основні засади, де визначатимуться, зокрема, мета, принципи, пріоритетні завдання, основні напрями діяльності держави з розвитку інформаційної сфери тощо.

А тим часом, більшість положень Основних засад державної інформаційної політики, викладених у додатку проекту (далі – Засади), мали декларативний, абстрактний, описовий характер, визначали бажані цілі розвитку у сфері державної інформативної політики. А така невизначеність відкриває суб’єктам правозастосування можливість довільно тлумачити норми закону. Крім того, у Засадах доволі широко й невиправдано, на нашу думку, вживається низка іншомовних слів, приміром, «конвергенція (поєднання) засобів мовлення та зв’язку», «захист плюралізму засобів масової інформації», «консолідації дій органів державної влади та суспільства» тощо. Положення документа часто-густо не несуть змістовного і правового навантаження, не містять механізмів їх реалізації, що суперечить, зокрема, рішенням Конституційного суду України від 7 липня 1998 року у справі щодо порядку голосування та повторного розгляду законів Верховною Радою України, де термін «закон» тлумачиться як «юридично цілісний і структурно завершений нормативно-

правовий акт, який приймається Верховною Радою України відповідно до її конституційних повноважень» [517].

Мало того, запропоновані Засади не досягають заявленої мети належного законодавчого регулювання, позаяк не враховують вимог статей 1, 8, 19 Конституції України, відповідно до яких Україна є правовою державою, де органи державної влади зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України. Проігнорована також правова позиція Конституційного суду України, наведена в рішенні від 30 травня 2001 року № 7-рп/2001 (справа про відповідальність юридичних осіб), за якою неповнота правового регулювання суспільних відносин не відповідає конституційному визначенню України як правової держави [518].

Засади також хибували термінологічними розбіжностями із чинними законами України «Про вищу освіту», «Про телебачення і радіомовлення», «Про національну програму інформатизації», «Про телекомунікації», «Про дозвільну систему у сфері господарської діяльності», «Про захист прав споживачів» тощо. Тож текст Основних засад державної інформаційної політики потребував суцільного техніко-юридичного та редакційного доопрацювання, зокрема таких формулювань, як «деградація суспільства», «трансформація моделі взаємовідносин», «сегменти вітчизняного інформаційного ринку», «журнали загальнодержавної, зарубіжної, регіональної, місцевої сфери розповсюдження», «засоби масової інформації загальнодержавної, регіональної та місцевої сфери», «недооцінка значення інформаційно-комунікаційного аспекту», «конвергенція (поєднання) засобів мовлення та зв'язку», «мультимедійні технології», «програмно-апаратна платформа» тощо.

Повертаючись до Доктрини інформаційної безпеки України, яка, за задумом її авторів, є «основою для розроблення проектів концепцій, стратегій, цільових програм і планів дій», зазначимо, що, зрештою, її затвердження, було оцінене як не вельми ефективний шлях від постановки

завдань та формулювання мети до практичного результату. Адже що таке Доктрина, як не стратегічний, програмний і концептуальний документ?

Такий підхід наражається на заперечні аргументи в сенсі того, що закон є нормативно-правовим актом прямої дії та не потребує на своє розгортання прийняття інших документів аналогічного рівня. Значною мірою складність у прийнятті та практичній реалізації різноманітних концепцій, стратегій, доктрин і т.п. зумовлена відсутністю усталеної ієрархії керівних документів державної політики й нерозумінням їх відмінності між собою та від інших нормативно-правових актів. Плутанина щодо цієї проблеми призводить до певної нестабільності та розбалансованості державної політики, знижує ефективність державного управлінського впливу в цілому, зокрема і в інформаційній сфері [519].

У теперішній час у сфері державної політики в інформаційній галузі функціонують такі керівні документи:

- Доктрина інформаційної безпеки України;
- Концепція розвитку електронного урядування в Україні;
- Концепція розвитку телекомунікацій в Україні
- Концепція формування системи національних електронних інформаційних ресурсів;
- Концепція технічного захисту інформації в Україні;
- Концепція створення Національного громадського телебачення і радіомовлення;
- Основні засади державної комунікативної політики;
- Національна програма інформатизації;
- Державна цільова науково-технічна програма «Образний комп'ютер»;
- Програма «Українська книга»

Існує також низка програмних документів, період дії котрих уже вичерпався, але чинність яких не припинена:

- Концепція розвитку зв'язку в Україні до 2010 року;

- Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки;

- Державна програма впровадження цифрового телерадіомовлення (на 2009-2015 рр.);

- Державна цільова програма формування позитивного міжнародного іміджу України на період до 2011 року;

- Державна програма інформування громадськості з питань євроатлантичної інтеграції України на 2008–2011 роки;

- Державна цільова науково-технічна програма впровадження і застосування грід-технологій на 2009 – 2013 роки;

- Концепція «Державної цільової програми популяризації вітчизняної книговидавничої продукції на 2009-2012 рр.»;

- Програма розвитку та переоснащення передавального обладнання Концерну радіомовлення, радіозв'язку та телебачення на основі сучасних технічних засобів на період до 2012 року;

- Державна програма розвитку архівної справи на 2006-2010 роки;

- Державна програма розвитку діяльності Національної бібліотеки України імені В.І.Вернадського на 2005-2010 роки;

- Державна програма «Журналіст» на 2004-2010 роки.

Цей перелік не є вичерпним (у частині документів, термін дії яких сплив), але він може вважатися репрезентативним для аналізу процесу правового регулювання інформаційної сфери за видами керівних документів державної політики.

Аналіз наведеного вище переліку дає підстави для таких висновків:

- відсутність у національному правовому просторі Стратегії розвитку інформаційної сфери;

- Доктрина інформаційної безпеки, яка є декларативним документом охоплює лише окремі сфери інформаційної діяльності і немає системного характеру;

- концептуальні документи з гуманітарних питань (бібліотечна, архівна, книговидавничої справи, імідж держави та офіційні комунікації тощо), котрі також мають входити до кола державної інформаційної політики, – не ухвалено;

- державне регулювання інформаційної сфери має орієнтуватися на двгосторокову перспективу. Натомість у вітчизняних реаліх це максимум середньострокові орієнтири;

- загалом масив керівних документів державної політики не має загальної логіки формування. До ідентичних за видом документів застосовано відмінні підходи, відсутня взаємна підпорядкованість різних видів документів [519].

Слід також зазначити, що сучасна інформаційна інфраструктура в нашій країні наразі перебуває у стадії формування. Не до кінця розроблене нормативно-правове підґрунтя відносин у сфері масової інформації. Бракує конкретної державної політики у сфері формування національного інформаційного простору, розвитку системи масової інформації, організації міжнародного інформаційного обміну. На цьому тлі спостерігається й погіршення ситуації із забезпеченням безпеки відомостей, що становлять державну таємницю.

Органи державної влади й місцевого самоврядування змушені закуповувати імпортну техніку із залученням іноземних фірм через недостатню державну підтримку розвитку вітчизняної індустрії інформаційних технологій, що підвищує ймовірність несанкціонованого доступу до інформації. Особливо небезпечною в цьому контексті є закупівля програмного й апаратного забезпечення виробництва країни-агресора.

На жаль, при забезпеченні безпеки в інформаційно-психологічній сфері розглядається здебільшого технічна сторона, а психологічна – практично залишається поза увагою. Це призводить до посилення інформаційної агресії з боку РФ, яка з метою просування своїх інтересів

використовує соціально-політичну ситуацію в Україні, залучаючи до цього в тому числі й наших співвітчизників. Події останнього часу, свідчать про використання іноземними суб'єктами зарубіжних і вітчизняних ЗМІ, соціальних мереж для зміни стану інформаційного простору з метою впливу на хід подій, що завдає нашій країні відчутної політичної шкоди й економічних збитків.

Відкритість національного інформаційного простору породжує реальну загрозу шкідливого інформаційно-психологічного впливу на суспільну свідомість населення, що становить особливу соціальну небезпеку. Безконтрольність електронних мас-медіа та соціальних мереж, які використовуються як майданчик для вербування в екстремістські організації, злочинні угруповання, незаконні збройні формування тощо, негативно впливає на користувачів мережі Інтернет, якими переважно є молодь і освічені люди з активною життєвою позицією.

Слід також враховувати, що в українське суспільство сьогодні розколоте за ставленням до таких фундаментальних цінностей, як демократія, незалежність, приватна власність, ринок тощо. Є розбіжності щодо уявлень про форму державного устрою та правління, про кількість мов офіційного спілкування та навчання, напрямки децентралізації, функції та завдання місцевого самоврядування тощо. Існує ціла низка міжрегіональних, міжетнічних, міжконфесійних суперечностей, різні шкали цінностей і пріоритетів, а тому наразі важко говорити про єдність інформаційного простору та про спільні ціннісні орієнтації [520, с. 96], що також є джерелом різнопланових внутрішніх загроз.

Нині в Україні на законодавчому рівні відсутні достатні гарантії захисту населення від негативних інформаційно-психологічних впливів, результатом яких може стати руйнування єдиного інформаційного й духовного простору. У цьому зв'язку виникає необхідність формування державної системи забезпечення інформаційно-психологічної безпеки, яка має будуватися на основі щільної взаємодії всіх владних інститутів, а

також громадських організацій. У ході реалізації державної політики у безпековій сфері варто, на наш погляд, звернути увагу на такі аспекти: розробку й реалізацію комплексних заходів щодо запобігання, нейтралізації й випередження негативних інформаційно-психологічних впливів на суспільство й державу; підготовку суспільства до активної інформаційної протидії; входження національного інформаційного поля у світовий інформаційний простір; удосконалення системи масової інформації й комунікації; формування системи підготовки кадрів для інформаційно-психологічної протидії; духовну консолідацію суспільства й віднаходження всіма верствами населення нової соціальної ідентичності [521, с. 400; 522, с. 36; 523, с. 41]. При цьому держава у правовому полі має встановлювати баланс між правами і свободами у сфері інформації й інформаційної діяльності та припустимими обмеженнями в цій сфері в інтересах захисту прав і свобод інших суб'єктів, інформаційної та національної безпеки України [524, с. 62].

Як слушно зазначили експерти Національного інституту стратегічних досліджень, відмова від доктринальних документів у сфері інформаційної безпеки в 2014 році, брак цілісного бачення у цій галузі, зволікання із розробленням Стратегії розвитку інформаційного простору України, – усе це зумовлює ситуативність багатьох заходів, спрямованих на подолання існуючих проблем [525, с. 289-290].

За сучасних умов інформаційна безпека має визнаватися основою інформаційної складової усіх сфер забезпечення національної безпеки. До головних завдань системи забезпечення інформаційної безпеки належить: прогнозування ризиків реалізації державної внутрішньої та зовнішньої політики, міждержавних та державних програм і проектів; виявлення внутрішніх і зовнішніх потенційних і реальних загроз; розробка та впровадження адекватних заходів і засобів реагування на виклики, як історичного походження, так і сучасного цивілізаційного розвитку; нейтралізація або послаблення дії проявів гібридної війни та інших загроз

національній безпеці України. Системний і комплексний підхід до вирішення цих завдань має відповідним чином визначати спрямування державної політики у сфері забезпеченні інформаційної безпеки нашої країни [505, с. 7].

Державна інформаційна політика на сучасному етапі має передбачати й вирішувати завдання щодо гармонійного забезпечення інформаційної безпеки особи, суспільства й держави з одночасним виокремленням нагальних пріоритетів. До останніх слід віднести створення/відновлення основних позицій захисту системи національної безпеки в інформаційній сфері, формування ефективної системи інформаційної безпеки держави, виявлення потенційних інформаційних загроз, усунення наявних із визначенням ступеня можливих наслідків та рівня їх інтенсивності. Головним підґрунтям державної інформаційної політики вбачається: забезпечення права на достовірну, повну та своєчасну інформацію, свободи слова та інформаційної діяльності в національному інформаційному просторі, недопущення втручання у зміст та внутрішню організацію інформаційних процесів, крім випадків, передбачених законодавством; збереження та вдосконалення вітчизняного національного інформаційного продукту й технологій, національно-духовних і культурних цінностей; забезпечення інформаційної та національно-культурної ідентифікації України у світовому інформаційному просторі; гарантування державної підтримки та розвитку ресурсів науково-технічної продукції та інформаційних технологій [526, с. 30]. Відповідно, державна політика у сфері забезпечення інформаційної безпеки має спрямовуватися передовсім на реалізацію комплексу системних превентивних заходів із наданням гарантій захисту життєво важливих інтересів особи, суспільства, держави та спроможності нейтралізувати чи послабити дію внутрішніх і зовнішніх потенційних і реальних загроз національній безпеці України [527, с. 68].

Спираючись на такі міркування та з огляду на сучасний стан загроз

інформаційній безпеці, доцільно, на нашу думку, виділити такі пріоритетні напрями державної політики у сфері забезпечення інформаційної безпеки:

1. **Захист життєво важливих інтересів особи, суспільства й держави від внутрішніх і зовнішніх загроз**. Виходячи із сучасних загроз національній безпеці України, цей напрям має концентруватися передусім на протидії загрозам, пов'язаним із застосуванням інформаційних технологій у військово-політичних цілях, у тому числі для здійснення ворожих дій і актів агресії, спрямованих на підрив суверенітету, порушення територіальної цілісності нашої держави. Відтак, першочерговими вбачаються такі заходи:

1.1. удосконалення діючої системи забезпечення інформаційної безпеки Збройних сил України, військових формувань і органів, що включає в себе сили і засоби інформаційного протиборства;

1.2. розробка та впровадження дієвих механізмів прогнозування, виявлення та оцінки інформаційних загроз;

1.3. нейтралізація інформаційно-психологічного впливу, в тому числі спрямованого на підрив історичної спадщини, її спотворення чи викривлення фактів;

1.4. поширення національного інформаційного продукту на тимчасово окупованих територіях; розробка та впровадження щодо них цілісної державної інформаційної політики;

1.5. розвиток інформаційної культури молоді, а також культури особистої інформаційної безпеки, профілактика правопорушень в інформаційній сфері.

2. **Захист суверенітету, підтримання політичної та соціальної стабільності, територіальної цілісності України**. Невідкладними заходами цього напряму мають стати:

2.1. протидія використанню інформаційних технологій з метою пропаганди екстремістської ідеології, поширення ксенофобії, ідей національної ворожнечі, в тому числі й на міжнародному рівні;

2.2. забезпечення захисту державної таємниці, іншої інформації обмеженого доступу, насамперед комерційної таємниці підприємств військово-промислового комплексу та інших, які мають особливе значення для економіки держави;

2.3. нейтралізація інформаційного впливу, спрямованого на розмивання традиційних духовно-моральних цінностей українського народу;

2.4. підготовка спеціалістів з протидії інформаційним загрозам на рівні державних освітніх програм.

3. **Захист критичної інформаційної інфраструктури**. З-поміж основних заходів цього напряму:

3.1. підвищення захищеності критичної інформаційної інфраструктури та стійкості її функціонування;

3.2. розвиток механізмів виявлення та попередження інформаційних загроз і ліквідації наслідків їх прояву, викликаних інформаційно-технічним впливом на об'єкти критичної інформаційної інфраструктури;

3.3. підвищення безпеки функціонування об'єктів інформаційної інфраструктури;

3.4. розробка механізмів обміну інформацією з країнами НАТО та ЄС про передові практики у сфері забезпечення безпеки функціонування елементів критичної інформаційної інфраструктури.

4. **Забезпечення розвитку інформаційно-комунікаційних технологій**. Серед пріоритетів виокремимо такі заходи:

4.1. розробка й виробництво конкурентоспроможних засобів забезпечення інформаційної безпеки;

4.2. інноваційний розвиток галузі інформаційних технологій, що має відбитися на розташування України в рейтингу Індексу розвитку інформаційно-комунікаційних технологій;

4.3. підтримка інноваційного та прискореного розвитку системи забезпечення інформаційної безпеки, галузі інформаційних технологій;

4.4. проведення наукових досліджень і здійснення дослідно-конструкторських розробок з метою створення перспективних інформаційних технологій забезпечення інформаційної безпеки.

5. **Забезпечення участі України в міжнародній системі інформаційної безпеки**. Провідними заходами цього напряму мають стати:

5.1. участь у формуванні системи міжнародної інформаційної безпеки на двосторонньому, багатосторонньому, регіональному, субрегіональному та глобальному рівнях;

5.2. участь у розробці міжнародних документів системи інформаційної безпеки;

5.3. формування механізмів міжнародного співробітництва у сфері протидії загрозам використання інформаційних та комунікаційних технологій у терористичних цілях;

5.4. продовження та посилення співпраці з НАТО та ЄС у сфері запобігання загрозам в інформаційній сфері на державному та глобальному рівнях;

5.5. участь у підготовці та прийнятті державами – членами Організації Об'єднаних Націй міжнародних правових актів, що регламентують застосування принципів і норм міжнародного права у сфері інформаційної безпеки;

5.6. розвиток співпраці з державами – членами НАТО та ЄС у сфері протидії інформаційній злочинності; підвищення ефективності інформаційного обміну між правоохоронними органами держав під час розслідування злочинів в інформаційній сфері.

Висновки до розділу 5

Ефективне забезпечення національної безпеки України потребує розробки науково обґрунтованої державної політики та стратегії в інформаційній сфері, визначення системи національних цінностей, життєво важливих інтересів в інформаційній сфері особистості, суспільства та держави, виявлення та постійного моніторингу актуальних загроз інформаційній безпеці держави, пошуку ефективних заходів для забезпечення інформаційної безпеки, захисту від інформаційних загроз і реалізації права на отримання достовірної інформації. При цьому забезпечення інформаційної безпеки вбачається наразі визначальним напрямом державної політики, від якого залежатиме існування суверенної України, її національна безпека, соціально-економічний розвиток та відповідне місце у світовому співтоваристві.

Основними цілями державної політики України у сфері забезпечення інформаційної безпеки є забезпечення: захисту інформаційного суверенітету держави (особливо – національного інформаційного простору з інформаційним ресурсом і систем формування суспільної свідомості) в сучасних умовах глобалізації та інтернаціоналізації інформаційних процесів; рівня інформаційної достатності для прийняття рішень державними органами, підприємствами та громадянами; реалізації гарантованих Конституцією інформаційних прав і свобод громадян, суспільства й держави.

Відтак, головне завдання державної політики у сфері забезпечення інформаційної безпеки – управління реальними та потенційними загрозами з метою створення необхідних умов для задоволення інформаційних потреб людини та громадянина, а також реалізації національних інтересів.

З огляду на сучасні загрози інформаційній безпеці уявляється доцільним виділити такі пріоритетні напрями державної політики у сфері її забезпечення:

Захист життєво важливих інтересів особи, суспільства й держави від внутрішніх і зовнішніх загроз. Виходячи із сучасних загроз національній безпеці України, цей напрям має концентруватися передусім на протидії загрозам, пов'язаним із застосуванням інформаційних технологій у військово-політичних цілях, у тому числі для здійснення ворожих дій і актів агресії, спрямованих на підрив суверенітету, порушення територіальної цілісності нашої держави. Відтак, першочерговими вбачаються такі заходи:

удосконалення діючої системи забезпечення інформаційної безпеки Збройних сил України, військових формувань і органів, що включає в себе сили і засоби інформаційного протиборства;

розробка та впровадження дієвих механізмів прогнозування, виявлення та оцінки інформаційних загроз;

нейтралізація інформаційно-психологічного впливу, в тому числі спрямованого на підрив історичної спадщини, її спотворення чи викривлення фактів;

поширення національного інформаційного продукту на тимчасово окупованих територіях; розробка та впровадження щодо них цілісної державної інформаційної політики;

розвиток інформаційної культури молоді, а також культури особистої інформаційної безпеки, профілактика правопорушень в інформаційній сфері.

Захист суверенітету, підтримання політичної та соціальної стабільності, територіальної цілісності України. Невідкладними заходами цього напряму мають стати:

протидія використанню інформаційних технологій з метою пропаганди екстремістської ідеології, поширення ксенофобії, ідей національної ворожнечі, в тому числі й на міжнародному рівні;

забезпечення захисту державної таємниці, іншої інформації обмеженого доступу, насамперед комерційної таємниці підприємств

військово-промислового комплексу та інших, які мають особливе значення для економіки держави;

нейтралізація інформаційного впливу, спрямованого на розмивання традиційних духовно-моральних цінностей українського народу;

підготовка спеціалістів з протидії інформаційним загрозам на рівні державних освітніх програм.

Захист критичної інформаційної інфраструктури. З-поміж основних заходів цього напряму:

підвищення захищеності критичної інформаційної інфраструктури та стійкості її функціонування;

розвиток механізмів виявлення та попередження інформаційних загроз і ліквідації наслідків їх прояву, викликаних інформаційно-технічним впливом на об'єкти критичної інформаційної інфраструктури;

підвищення безпеки функціонування об'єктів інформаційної інфраструктури;

розробка механізмів обміну інформацією з країнами НАТО та ЄС про передові практики у сфері забезпечення безпеки функціонування елементів критичної інформаційної інфраструктури.

Забезпечення розвитку інформаційно-комунікаційних технологій. Серед пріоритетів виокремимо такі заходи:

розробка й виробництво конкурентоспроможних засобів забезпечення інформаційної безпеки;

інноваційний розвиток галузі інформаційних технологій, що має відбитися на розташування України в рейтингу Індексу розвитку інформаційно-комунікаційних технологій;

підтримка інноваційного та прискореного розвитку системи забезпечення інформаційної безпеки, галузі інформаційних технологій;

проведення наукових досліджень і здійснення дослідно-конструкторських розробок з метою створення перспективних інформаційних технологій забезпечення інформаційної безпеки.

Забезпечення участі України в міжнародній системі інформаційної безпеки. Провідними заходами цього напряму мають стати:

участь у формуванні системи міжнародної інформаційної безпеки на двосторонньому, багатосторонньому, регіональному, субрегіональному та глобальному рівнях;

участь у розробці міжнародних документів системи інформаційної безпеки;

формування механізмів міжнародного співробітництва у сфері протидії загрозам використання інформаційних та комунікаційних технологій у терористичних цілях;

продовження та посилення співпраці з НАТО та ЄС у сфері запобігання загрозам в інформаційній сфері на державному та глобальному рівнях;

підготовка та прийняття спільно з іншими державами – членами Організації Об'єднаних Націй міжнародних правових актів у сфері інформаційної безпеки;

розвиток співпраці з державами – членами НАТО та ЄС у сфері протидії інформаційній злочинності; підвищення ефективності інформаційного обміну між правоохоронними органами держав під час розслідування злочинів в інформаційній сфері.

Державна політика у сфері забезпечення інформаційної безпеки повинна втілюватися в нормах законодавства та програмних документах стратегічного планування. Водночас, систематизація інформаційного законодавства потребує створення стрункої комплексної галузі інформаційного права, формування положень, котрі знайдуть своє вираження в конкретних дефініціях законів та підзаконних нормативно-правових актів.

Так, нинішній стан правового забезпечення інформаційної безпеки зумовлює потребу виокремлення законодавчих актів, положень, норм, які

регламентують різні аспекти цієї сфери, їхнього аналізу на предмет наявності системних вад та систематизації, консолідації на цій основі загальних правових норм у єдиний базовий закон, позбавлений існуючих у теперішній час суперечностей, колізій та прогалин. Таким базовим законом, на наше переконання, має стати Закон України «Про інформаційну безпеку України». Його теоретичне обґрунтування має спиратися на сформовану у структурі вітчизняної системи права самостійну підгалузь – правове забезпечення інформаційної безпеки, а також відповідну законодавчу підгалузь, положення якої нині містяться в багатьох законодавчих актах різних галузей. Структурно-змістова схема пропонованого закону може мати такий вигляд:

Розділ 1. Має розкривати найзагальніші питання. Це, зокрема: мета та сфера дії цього закону; основні поняття (терміни), що в ньому вживаються; принципи забезпечення інформаційної безпеки, його суб'єкти та об'єкти; перелік актів законодавства, котрі цю сферу регулюють; загальна структура законодавства про інформаційну безпеку.

Розділ 2. Загальні засади функціонування державної системи забезпечення інформаційної безпеки. Тут слід визначити пріоритетні завдання у цій сфері, головним із яких убачається створення й удосконалення відповідного законодавства. На його основі має бути сформована вказана система задля неухильного втілення уповноваженими державними органами законодавчих вимог у цій галузі. Функції координації вказаної діяльності доцільно покласти на Службу безпеки України.

***Розділ* 3**. Загальні питання забезпечення безпеки інформації з обмеженим доступом: підстави та принципи віднесення відомостей до категорії інформації з обмеженим доступом (таємна, конфіденційна), види інформації з обмеженим доступом (державна, комерційна, лікарська та ін. таємниця; для службового користування тощо); загальні засади захисту інформації з обмеженим доступом.

***Розділ* 4**. Загальні питання захисту відкритої (загальнодоступної) інформації від протиправних маніпуляцій з нею (викривлення, приховування, блокування тощо), зокрема: засади та вимоги до захисту інформації в загальнодоступних державних мережах; інформаційно-правові аспекти (на відміну від цивільно-правових) захисту об'єктів інтелектуальної власності (державна реєстрація, акредитація тощо) та ін.

***Розділ* 5.** Загальні засади захисту від недостовірної та шкідливої інформації, негативного інформаційно-психологічного впливу. Тут варто, на наш погляд, зазначити загрози суб'єктам інформаційних відносин, спричинені застосуванням спеціальних методів і засобів інформаційно-психологічного впливу, зокрема: маніпулювання особистісною та суспільною свідомістю, навіювання хибних думок і провокування хибних дій, завдання шкоди здоров'ю та життю людини тощо.

***Розділ* 6**. Загальні питання протидії інформаційному екстремізму. Необхідно визначити вичерпний перелік чітких критеріїв, за якими інформація визнається екстремістською (що загрожує конституційному ладу України), зокрема: умисел суб'єкта її розповсюдження, конкретні умови оприлюднення тощо.

***Розділ* 7**. Види відповідальності за правопорушення, пов'язані із сферою інформаційної безпеки. Слід передбачити випадки застосування кожного з видів відповідальності – дисциплінарної, цивільно-правової, адміністративної, кримінальної.

Зрештою, цей закон має, на нашу думку, закріпити найзагальніші положення, які поширюватимуться на решту нормативно-правових актів у цій галузі, а саме: принципи правового забезпечення, структуру відповідного законодавства, єдині параметри правового забезпечення інформаційної безпеки, загальну термінологію. Крім того, вказаний закон, синтезувавши норми підгалузі правового забезпечення інформаційної безпеки, може стати одним із базових при кодифікації вітчизняного інформаційного законодавства та створенні Інформаційного кодексу

України, а також основою для керівних документів державної політики в інформаційній сфері та процесу стратегічного планування забезпечення інформаційної безпеки України.

Основні результати даного розділу висвітлено у працях [528-533].

ВИСНОВКИ

У дисертації наведено нове вирішення актуальної наукової проблеми, що полягає у розробленні концептуальних та правових засад забезпечення інформаційної безпеки України, а також практичних рекомендацій щодо вдосконалення механізмів її забезпечення у контексті євроінтеграції. Отримані у процесі дослідження результати підтверджують покладену в його основу гіпотезу, дають підстави стверджувати про досягнення поставленої мети, реалізацію визначених завдань та зробити такі головні висновки:

1. Виявлено, що сучасні наукові підходи до концепції інформаційної безпеки ґрунтуються на значній філософській базі. Вона формувалася впродовж кількох історичних етапів: Стародавнього світу, епохи Відродження, XVII–XX ст., кінець XX — початок XXI ст. У цих дискурсах Церква намагалася втримувати монополію на істину. Водночас виникали різноманітні напрями духовного розвитку суспільства, поступово визнавалися окремі права та свободи людини. Вагомими на цьому евристичному шляху стали праці Н. Макіавеллі, Гроція Гуго де Гроота, Т. Гоббса, І. Канта та ін. Розвиток інформаційно-комунікаційних технологій наприкінці XX ст. призвів до виникнення нових форм та методів ведення «війни четвертого покоління».

2. Дослідження джерельної бази дало змогу визначити три концептуальні підходи до тлумачення інформаційної безпеки України:

1) статичний (безпека як стан захищеності інформаційного середовища/інформації, система гарантій тощо);

2) діяльнісний (безпека як процес її забезпечення, здатність держави ефективно захистити національні інтереси і цінності);

3) комплексний (безпека як стан і процес).

Найбільш прийнятним із них є комплексний. За такого підходу

інформаційну безпеку України вперше визначено як *1)* стан, за якого в умовах дії реальних та потенційних загроз забезпечується самозбереження, сталий і прогресивний розвиток інформаційної сфери, зокрема захищеність інформаційної інфраструктури, інформаційного простору, інформаційних ресурсів, інформаційних процесів та їхніх суб'єктів, а також досягнення відповідних національних цілей та реалізація національних інтересів в інформаційній сфері; *2)* забезпечення інформаційної безпеки України визначено як постійний процес діяльності компетентних органів, спрямований на запобігання, протидію загрозам інформаційній сфері, застосування активних заходів інформаційного впливу, а також сукупність умов такої діяльності, які реалізуються й здатні контролюватися тривалий час.

Доведено, що *основна мета забезпечення інформаційної безпеки України* – це створення безпечного інформаційного середовища, що означає і захист національних інтересів і цінностей (пасивна форма), і протидію, активні контрзаходи (активна форма).

3. Підтверджено, що *основними об'єктами правового забезпечення інформаційної безпеки України* є: *а)* особа (людина і громадянин) – її конституційні права і свободи, фізичне та психічне здоров'я, захищеність від негативного впливу інформаційних технологій та інформації; *б)* суспільство і держава – захищеність їхніх законних інтересів в інформаційній сфері; *в)* інформаційні ресурси та інформаційна інфраструктура – їхня цілісність, доступність та захищеність. Доведено, що об'єкти правового забезпечення інформаційної безпеки держави втілюються в національних інтересах, цінностях, цілях та надбаннях в інформаційній сфері.

4. Обґрунтовано, що реалізація *національних інтересів* в інформаційній сфері, визначених Доктриною інформаційної безпеки України, буде дієвою в разі законодавчого визначення національних цінностей і зумовлених ними національних інтересів.

До *національних цінностей в інформаційній сфері* віднесено: *а)* матеріальний добробут населення (у т. ч. на основі розвитку ІКТ); *б)* інформаційна захищеність людини, суспільства, держави; *в)* духовність, доступність віросповідання, попередження релігійного фанатизму та екстремізму; *г)* мова; *ґ)* культура інформаційних відносин; *д)* свобода інформації, захищеність інформаційних прав людини, доступ до інформації, нейтралізація негативних інформаційних впливів та ін.

До *національних цілей в інформаційній сфері* віднесено: *а)* покласти край спотворенням поглядів людей на навколишній світ і самих себе (духовна безпека); *б)* забезпечити впровадження інформаційних технологій у військову сферу та забезпечити їх захист (воєнна безпека); *в)* прискорити розробку та впровадження новітніх ІКТ у суспільно-економічну сферу (економічна безпека); *г)* досягти належного рівня культури інформаційних відносин (соціальна безпека); *ґ)* створити загальнодержавні інформаційні системи для постійного моніторингу стану навколишнього середовища (екологічна безпека); *д)* сприяти інтеграції національної інформаційної інфраструктури зі світовою інфраструктурою; *е)* посилити захист інформаційних прав людини; *є)* вжити термінових заходів для створення позитивного іміджу держави в умовах інформаційної глобалізації.

5. Виходячи із розробленої моделі взаємодії національних цінностей, інтересів цілей та надбань в інформаційній сфері, запропоновано основними критеріями оцінки негативного впливу на інформаційну безпеку держави вважати деструктивні трансформації національних цінностей в інформаційній сфері, які можливо встановлювати шляхом соціологічних опитувань та вивчення громадської думки. Такі критерії доцільно акумулювати в методологічній базі і на її підставі моніторити стан і динаміку вітчизняної інформаційної сфери, виявляти найбільш вразливі сфери.

6. Доведено, що в основу вдосконалення правового забезпечення інформаційної безпеки України доцільно покласти принципи:

а) формування та застосування норм міжнародного права як складової правової системи України;

б) забезпечення балансу інтересів людини, суспільства і держави;

в) узгодженості діяльності органів державної влади щодо вдосконалення правового забезпечення інформаційної безпеки України.

7. Обґрунтовано доцільність *правового забезпечення інформаційної безпеки України* досліджувати як цілісну систему правового регулювання суспільних відносин, що виникають у процесі протидії загрозам національній безпеці України в інформаційній сфері. Зазначений правовий феномен має власний предмет правового регулювання. Об'єктом відносин, які належать до такої діяльності, є інформація та відповідна інфраструктура.

Із згаданим предметом правового регулювання формується новий комплексний інформаційний феномен – інформаційне право, а в його межах і на основі чинного вітчизняного законодавства – модель формування структурного утворення з правового забезпечення інформаційної безпеки. Це зумовило теоретичне підтвердження існування в системі права галузі інформаційного права, а також правового забезпечення інформаційної безпеки як підгалузі інформаційного права.

8. Підтверджено, що *інформаційне право* є комплексною галуззю не тільки за предметною ознакою, а й методами правового регулювання (дозвіл, заборона, примус, покарання тощо). *Підгалузь правового забезпечення інформаційної безпеки* тісно взаємодіє з конституційним, адміністративним, цивільним, кримінальним правом, консолідуючи їхні норми, котрі стосуються сфери регульованих нею відносин, сполучає й застосовує притаманні їм методи, способи, засоби та прийоми правового регулювання.

9. Відмічено, що інформаційна сфера має два основні складники, які, своєю чергою, визначають основні елементи інформаційної безпеки України: *а)* технічний (штучно створене людиною середовище техніки і

технологій); *б)* психологічний (система цінностей, переконань, установок тощо, які в межах державної інформаційної політики спрямовано формуються на рівні індивіда та соціуму).

Відповідно *предмет правового забезпечення інформаційної безпеки України* є суспільні відносини, які охоплюють дві сфери: *а)* технічну (комп'ютерні системи, телекомунікаційні мережі); *б)* психологічну (суспільна думка, національні цінності, стереотипи, установки). Предметом дослідження обрано інформаційно-психологічний складник інформаційної безпеки України. Оскільки інформаційно-психологічний вплив може викликати значні дисфункції (соціальне напруження, розбалансованість важелів стримувань і противаг гілок влади та ін.), то основним об'єктом захисту є суспільна свідомість населення.

10. На основі аналізу чинного законодавства та практики європейських країн запропоновано відмовитися від законодавчого закріплення фіксованого переліку загроз інформаційній безпеці України, оскільки він не має і не може мати вичерпного характеру. Підкреслено, що найбільш небезпечні з-поміж загроз – транскордонні і такі, що мають політичне забарвлення.

Відповідно запропоновано забезпечувати одночасно, по-перше, безпеку інформації від знищення, перекручення, блокування, несанкціонованого витоку або порушення встановленого порядку її маршрутизації, по-друге, інформаційну безпеку громадянина та суспільства. Ця вимога продиктована значенням інформаційної картини світу, що формується на індивідуальному та соцієтальному рівнях. Поширеним інструментом загроз є розповсюдження т. зв. патогенних текстів, спрямованих на деконструкцію ідеологічної, ціннісної, морально-етичної та інших ментальних систем.

11. Доведено, що *механізми протидії інформаційним загрозам від зовнішніх джерел* повинні передбачати: *а)* мету забезпечення безпеки, що полягає у збереженні цілісності й захищеності інформаційної сфери у

процесі її функціонування; *б)* рівень безпеки, що виокремлює складники системи, які можуть стикатися з потенційними і реальними небезпеками; *в)* сфери безпеки, що визначають можливості функціонування й розвитку інформаційної сфери; *г)* параметри безпеки, що встановлюють припустимі межі відхилень у потенціалі системи інформаційної безпеки, кількості її елементів, їх якості, зв'язки; *ґ)* перелік загроз, наслідки їх реалізації та механізми запобігання.

12. *Методи протидії інформаційним загрозам від зовнішніх джерел* умовно поділено на дві групи: *1)* профілактичні (превентивні) – використовуються для недопущення розгортання відповідних загроз або для запобігання виникненню нових ризиків на початковому етапі розгортання таких загроз; *2)* оперативні – застосовуються безпосередньо у відповідь на агресивні кроки зовнішніх джерел інформаційних загроз та пов'язані з їх розгортанням та реалізацією.

13. Доведено необхідність удосконалення функціональних обов'язків суб'єктів забезпечення інформаційної безпеки України в частині здійснення координації та взаємодії.

Запропоновано для вироблення узгоджених рішень щодо напрямів і заходів реалізації державної політики інформаційної безпеки створити при Раді національної безпеки і оборони України міжвідомчу комісію (або координаційну раду) у складі представників профільного Комітету Верховної ради України, Кабінету Міністрів України, Міністерства інформаційної політики, Міністерства оборони, Служби безпеки України, Міністерства внутрішніх справ, Міністерства закордонних справ та інших державних органів, спеціально уповноважених на виконання завдань щодо забезпечення інформаційної безпеки. Крім того, у статті 10 Закону України «Про Службу безпеки України» йдеться, що у структурі Центрального управління Службу безпеки України діє підрозділ контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, котрий може виконувати координуючу функцію у сфері

забезпечення інформаційної безпеки держави. Реалізація цього положення потребуватиме внесення змін до Закону України «Про національну безпеку України», а також до Доктрини інформаційної безпеки України та Стратегії кібербезпеки України.

14. Удосконалено теоретичні підходи до змісту *об'єктів системи забезпечення інформаційної безпеки України,* якими є: людина і громадянин (життя, здоров'я, культура, традиції тощо); суспільство (розвиток демократії, збереження культури й духовно-історичної спадщини, збереження і розвиток інформаційних ресурсів, досягнення і зміцнення суспільної злагоди, політичної стабільності, віротерпимості тощо; держава (конституційний лад, суверенітет і територіальна цілісність України, політична, економічна та соціальна стабільність, законність і правопорядок, розвиток рівноправного взаємовигідного міжнародного співробітництва тощо).

Визначено, що безпосередніми об'єктами правового впливу у рамках системи забезпечення інформаційної безпеки України є національні інтереси, цілі, цінності та надбання в інформаційній сфері.

15. На основі вивченого досвіду правового забезпечення інформаційної безпеки в НАТО запропоновано запровадити в Україні заходи попередження та процедури її гарантування, а також дотримання умов, запропонованих у плані дій Україна – НАТО. Це передбачає: *а)* забезпечення реалізації гарантій доступу до інформації; *б)* імплементацію відповідного законодавства для усунення перешкод діяльності ЗМІ; *в)* поглиблення інформаційного виміру співробітництва Україна – НАТО, включно з парламентським співробітництвом; *г)* створення прозорої та гнучкої структури електронного урядування; *ґ)* забезпечення розвитку спроможностей військових частин і підрозділів інформаційних операцій; *д)* підвищення рівня обізнаності громадськості щодо діяльності НАТО; *е)* підвищення рівня забезпечення інформаційної безпеки, кібербезпеки тощо.

16. Підтверджено, що країни позаблокового статусу усвідомлюють безпосередню залежність свого добробуту від інформаційної сфери, тож питання забезпечення інформаційної безпеки закономірно посідає одне з чільних місць у безпекових стратегіях таких держав. При цьому політика забезпечення інформаційної безпеки позаблокових країн має проактивний характер і спирається на засади управління ризиками інформаційної безпеки, передусім кібербезпеки.

17. Досвід зміни парадигми забезпечення інформаційної безпеки України з реактивної на проактивну, в контексті євроінтеграційних спрямувань, визначено надзвичайно важливим, адже дає змогу правильно визначати стратегічні пріоритети, акумулювати зусилля щодо забезпечення інформаційної безпеки, а також сприятиме плідному співробітництву з усіма європейськими країнами у розбудові систем регіональної та міжнародної інформаційної безпеки.

Важливим цей досвід є також для подальшої розбудови теорії національної безпеки та наукових засад забезпечення інформаційної безпеки.

18. Підтверджено, що для України корисним є досвід країн Центральної Європи у забезпеченні інформаційної безпеки, зокрема Хорватії та Німеччини.

Актуальним є приєднання України до інших європейських країн у розбудові системи міжнародної інформаційної безпеки, щоб протидіяти кібертероризму та кіберзлочинності, орієнтуючись при цьому на стандарти ЄС та НАТО. Для України важливим є також досвід Польщі, країн Прибалтики, Угорщини, Румунії щодо приведення національного законодавства у відповідність до вимог міжнародних організацій, передусім, щодо забезпечення балансу між свободою та безпекою в інформаційній сфері на законодавчому рівні.

19. Запропоновано розвивати співробітництво України у розбудові систем регіональної та міжнародної інформаційної безпеки у рамках

проекту «Міжмор'я» з метою протидії загрозам стратегічній стабільності, зокрема, кібертероризму та кіберзлочинності, орієнтуючись при цьому на стандарти ЄС та НАТО.

20. З'ясовано, що на сучасному етапі інформаційно-комунікаційні технології на міжнародному рівні зазнають усе дужчого мілітарного впливу. У прогнозі – подальше вдосконалення методів ведення інформаційно-психологічної війни і розширення сфер застосування відповідних технологій, що на глобальному рівні може суттєво позначитися на стратегічному балансі сил, спричинити зміни в підходах до його оцінювання на основі співвідношення геополітичних, економічних і військових чинників. Складність ідентифікації джерела інциденту в інформаційному просторі й неузгодженість у поглядах на те, які заходи у відповідь є прийнятними, підвищують імовірність виникнення конфлікту і завдання шкоди тій чи тій сфері життєдіяльності держави (держав).

21. Для ефективного правового забезпечення інформаційної безпеки України запропоновано проаналізувати законодавчі акти, положення, норми, які регламентують різні аспекти забезпечення інформаційної безпеки, консолідувати загальні правові норми у ЗУ «Про інформаційну безпеку України». Підтверджена гіпотеза, що даний закон може стати одним із базових при кодифікації вітчизняного законодавства у сфері інформації та створенні Інформаційного кодексу України, а також стати основою для керівних документів державної політики в інформаційній сфері та процесу стратегічного планування забезпечення інформаційної безпеки України.

22. Доведено, що забезпечення інформаційної безпеки України є визначальним напрямом державної політики, від якого залежатиме існування держави, її національна безпека, соціально-економічний розвиток та відповідне місце у світовому співтоваристві.

Визначено *основні цілі державної політики України у сфері забезпечення інформаційної безпеки*: *а)* захист інформаційного

суверенітету держави в сучасних умовах глобалізації та інтернаціоналізації процесів в інформаційній сфері; *б)* забезпечення інформаційної достатності для прийняття рішень державними органами, підприємствами та громадянами; *в)* реалізація конституційних прав і свобод громадян, суспільства і держави на інформацію.

Обґрунтовано, *що основна мета державної політики у сфері забезпечення інформаційної безпеки України* – це управління реальними та потенційними загрозами з метою створення необхідних умов для задоволення інформаційних потреб людини та громадянина, а також реалізації національних інтересів.

З огляду на сучасний стан загроз інформаційній безпеці, удосконалено *пріоритетні напрями державної політики у сфері забезпечення інформаційної безпеки України*:

а) захист життєво важливих інтересів особистості, суспільства та держави від внутрішніх і зовнішніх загроз;

б) захист суверенітету, підтримка політичної та соціальної стабільності, територіальної цілісності України;

в) захист критичної інформаційної інфраструктури;

г) забезпечення розвитку інформаційно-комунікаційних технологій;

ґ) забезпечення участі України в міжнародній системі інформаційної безпеки.

23. Запропоновано такі перспективні напрямами подальших наукових пошуків:

- дослідження у сфері оцінювання загроз інформаційній безпеці України та методів управління ризиками в інформаційній сфері;
- визначення місця інформаційної безпеки України в системі чинників національної безпеки;
- дослідження основних завдань інформаційної безпеки України і напрямів її функціонування;
- розробки критеріїв оцінки негативного впливу на інформаційну

безпеку України;

- дослідження проблем розвитку інформаційного суспільства в Україні;

- теоретико-правове обґрунтування інформаційно-правової відповідальності;

- дослідження складових ІТ-права та його місця у національній і міжнародній системі права;

- обґрунтування правових основ функціонування штучного інтелекту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Псалтирь. Харьков : Фолио. 2013. 574 с.

2. Плутарх Сравнительные жизнеописания. Плутарх; пер. с древнегреч. В. Алексеева. Х.: Фолио. 2013. 348 с.

3. Сенека Л.А, Трагедии; пер. с лат. С. Ошерова, коммент. Е. Рабинович. М.: Искусство. 1991. 494 с.

4. Платон. Диалоги; вступ, ст., коммент. А.Ф. Лосева; пер. с древнегреч. М.С. Соловьева. М.: Зксмо, 2007. Кн. 1. 1231с

5. Сунь-цзы: Искусство войньї: Древнейший в мире трактат о войне; пер. с кит., коммент., примеч. Л. Джайлса ; 2-е изд. Ростов-на-Дону : Феникс. 2003. 283 с.

6. Николо Макиавелли. Государь. М. : Олма Медиа Групп, 2011. 512 с.

7. Гроций Г. О праве войны и мира. Три книги, в которьіх обьясняются государственное право и право народов, а также принципы публичного права; пер. с лат. А.Л. Саккетти. М.: Гос. изд-во юрид. лит-ры, 1957. 868 с.

8. Дзьобань О.П. Національна безпека України: концептуальні засади та світоглядний сенс : [монографія]. Харків : Майдан, 2007. 284 с.

9. Сен-Симон А. Избранньїе сочинения; пер. с франц. под ред. и с коммент. Л.С. Цетлина ; вступ, ст. В.П. Волгина. М.; Л.: АН СССР, 1948. – Т. 1. 468 с.

10. Оуен Р. Організаційна поведінка в освіті: Керівництво учбовими закладами та шкільна реформа; пер. з англ. О.В. Христенко. Х.: Каравела, 2003. 488 с.

11. Бергсон А. Творческая зволюция. Материя и память. Минск : Харвест, 1999. 1407 с.

12. Рассел Б.А. Человеческое познание, его сфера и границы. пер. с англ. Н.В. Воробьева. К. : Ника-Центр; М. : Институт общегуманитарньїх исследований, 2001. 560 с.

13. Thomas P. Rona. Weapon Systems and Information War, the Official Home of the Department of Defense. URL: http://www.dod.gov/pubs/foi/reading_room/09-F-0070WeaponSystems_and_Information_War.pdf (дата звернення: 16.12.2017).

14. DoD Directive TS-3600.1, "Information Warfare", December 21, 1992. URL:http://www.dtic.mil/whs/directives/corres/pdf/300003p.pdf (дата звернення: 16.12.2017).

15. Martin C. Libicki. What is Information Warfare? United States Government Printing, Washington DC, 1995. URL: http://www.dodccrp.org/files/Libicki_What_Is.pdf (дата звернення: 16.12.2017).

16. Martin C. Libicki Crisis and Escalation in Cyberspace URL: https://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1215.pdf (дата звернення: 16.12.2017).

17. Command and Control Warfare, Joint Publication 3-13.1. Washington D.C.: Joint Chiefs of Staff, Feb. 1996

18. Joint Publication 3-13, “Information Operations”, 27 November 2012, Incorporating Change 1, 20 November 2014, URL: http://www.fas.org/irp/doddir/dod/jp3_13.pdf (дата звернення: 16.12.2017).

19. Dictionary of Military and Associated Terms//JP 1-02 DOD / Information operations. (JP 3-13). URL: http://ra.defense.gov/Portals/56/Documents/rtm/jp1_02.pdf (дата звернення: 16.12.2017).

20. Сопілко І.М. Становлення інформаційного суспільства та інформаційні загрози в мережі Інтернет. Юридичний вісник 3 (44) 2017. С. 61-64

21. Присяжнюк М.М. Інформаційна безпека України в сучасних умовах. Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки. 2013. Вип. 30. С. 42-46

22. Сытников А.А. Обеспечение и защита права на информацию. М.: Городец-издат, 2001. 344 с.

23. Конституція України: Основний Закон України від 28.06.1996 № 254к/96-ВР. URL: http://zakon3.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 16.02.2018).

24. Цимбалюк В. Окремі питання щодо визначення категорії «інформаційна безпека» у нормативно-правовому аспекті. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Науково-технічний збірник. К., 2004. С. 30-33

25. Рубан В.Я. Інформаційна безпека України: сутність та проблеми. Стратегічна панорама. 1998. № 3-4. С. 170-175

26. Марущак А.І. Дослідження проблем інформаційної безпеки у юридичній науці. Правова інформатика. 2010. No 3(27). С. 17-21

27. Красноступ М.Д. Інформаційна безпека України: сутність та проблеми. Інформаційні технології та захист інформації. 1999. №1. С. 108-110.

28. Управление и право в период информатизации: [монографія]. К.: Издательство “КВІЦ”, 2001. 308 с.

29. Баранов А.А. Концептуальные вопросы информационной безопасности Украины. Нормативно-правовая база защиты информации: Сб-к материалов. К., 1997. С. 53-58

30. Згуровський М.З. Проблеми інформаційної безпеки в Україні, шляхи їх вирішення. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Науково-технічний збірник. К., 2000. С. 10-14.

31. Вус М.А., Нестеров Ю.М. Информационное общество. Информационное право. Информационная безопасность. Актуальные проблемы безопасности информационного пространства. Материалы Всероссийской научно-практической конференции. СПб., 5-8 октября 1999 г. СПб., 1999. С. 19-20

32. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції: [навчальний посібник]. К.: КНТ, 2006. 280 с.

33. Данильян О.Г., Дзьобань О.П., Панов М.І. Національна безпека України: структура та напрямки реалізації: [навчальний посібник]. Х.: Фоліо, 2002. 285 с.

34. Гурковський В.І. Безпека як об'єкт правовідносин в умовах глобального інформаційного суспільства. Правова інформатика. 2010. No 2(26). С. 72-77

35. Баранов О.П. Передумови створення Державної спеціальної служби транспорту та її завдання в системі національної безпеки України. Вісник Національної академії державного управління при Президентові України. 2014. № 3. С. 60-65

36. Шатун В. Т. Інформаційна безпека – невід'ємна складова національної безпеки України. Наукові праці Чорноморського державного університету імені Петра Могили комплексу «Києво-Могилянська академія». 2016. Т. 267. Вип. 255. С. 174-180

37. Калюжний Р. Питання концепції реформування інформаційного законодавства України. Правове, нормативне та метрологічне забезпечення системи інформації в Україні: Тематичний збірник праць учасників Другої науково-технічної конференції. К., 2000. С.17-21

38. Нижник Н. Р., Ситник Г. П., Білоус В. Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): [навчальний посібник]. Ірпінь : Акад. ДПС України, 2000.304 с.

39. Ярочкин В.И., Шевцова Т.А. Словарь терминов и определений по безопасности и защите информации. М.: Ось-89. 1996. 48 с.

40. Ліпкан В. А., Харченко Л. С., Логінов О. В. Інформаційна безпека України: Глосарій. К.: Текст, 2004. 136 с.

41. Лукашов А.И. Информационная безопасность как объект уголовно-правовой охраны в законодательстве Республики Беларусь. Материалы научной конференции «Концептуальные проблемы информационной безопасности в союзе России и Беларуси». СПб., 2000 – 03.10.2016 URL: http://jurfak.spb.ru/ conference/2001.htm

42. Бєляков К.І. Деякі питання щодо формування реформи інформаційного законодавства України. Систематизація законодавства в Україні: проблеми теорії і практики. Матеріали міжнародної науково-практичної конференції. К.: Інститут законодавства Верховної Ради України, 1999. С. 253-255

43. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: [навчальний посібник]. Київ: Кондор, 2004. 382 с.

44. Фисун Ю. А. Вопросы информационной безопасности личности, общества и государства накануне 21 века. Международная конференция «Информатизация правоохранительных систем». - 7-8 июня 2000 г, Москва: Сборник трудов. С. 86-92

45. Панарин И. Технология информационной войны: [монографія]. М.: КСП+, 2003. 320 с.

46. Тер-Акопов А.А. Безопасность человека: [монографія]. М.: Изд-во МНЭПУ. 1998. 256 с.

47. Шульга В. І. Сучасні підходи до трактування поняття інформаційна безпека. Ефективна економіка, № 4, 2015. 13.06.2017 URL: http://www.economy.nayka.com.ua/ ?op=1&z=5514

48. Лопатин В.Н. Правовые проблемы защиты единого информационного пространства страны. Информация и государство. Вопросы защиты информации. 2001. № 2. С. 8-20

49. Почепцов Г.Г. Информационные войны. М.: «Рефл-бук», К.: «Ваклер», 2000. 567 с.

50. Расторгуев С.П. Принципы целостности и изменчивости в решении задачи обеспечения безопасности. Конфидент. 1998. № 3. С. 11-15

51. Хаба Р.С. Деструктивні інформаційні впливи в сучасних умовах. Інформаційна безпека людини, суспільства, держави. № 1(21) 2017. С. 216-224

52. Емельянов Г.В., Стрельцов А.А. Проблемы обеспечения безопасности информационного общества. Информационное общество. 1999. №2. С. 15-18

53. Потрубач Н.Н., Максутов Р.К. Информационная безопасность и устойчивое развитие общества. Информационные технологии в проектировании. 2000. № 3. С. 32-36

54. Корж І.Ф. Внутрішні фактори загроз і викликів інформаційній безпеці України. Запобігання новим викликам та загрозам інформаційній безпеці України: правові аспекти **:** матеріали наук.-практ. конф. 06 жовт. 2016 р. Упоряд. : В. М. Фурашев. Київ : НТУУ «КПІ імені Ігоря Сікорського», Вид-во «Політехніка», 2016. 204 с.

55. Петраков М.В. Об основных направлениях обеспечения информационной составляющей в системе национальной безопасности. Материалы научной конференции «Концептуальные проблемы информационной безопасности в союзе России и Беларуси». СПб., 2000. 16.07.2017 URL: http://jurfak.spb.ru/ conference/2001.htm (дата звернення: 16.02.2018).

56. Лопатин В.Н. Информационная безопасность России: автореф. дис…докт. юрид. наук : 12.00. СПб., 2000. 28 с.

57. Шерстюк В.П. Информационная безопасность в системе обеспечения национальной безопасности России, федеральный и

региональный аспекты обеспечения информационной безопасности. Информационное общество. 1999. № 5. С. 3-5.

58. Литвиненко О.В. Інформаційний простір як чинник забезпечення національних інтересів України. К., 1998. 50 с.

59. Бондар І.Р. Інформаційна безпека як основа національної безпеки. Mechanism of Economic Regulation. 2014. № 1. С. 68-75

60. Ліпкан В.А. Теоретико-методологічні засади управління у сфері національної безпеки України. К.: Видавництво Національної академії внутрішніх справ України, 2005. 350 с.

61. Сацута А.А. Национальная безопасность как социальное явление: современная парадигма. Вестник Военного университета. 2007, № 3 (11). С.36 – 43

62. Encyclopedia of United States National Security, 2 Vol., Sage Publications (2005), ISBN 0-7619-2927-4

63. Новицький Г.В. Теоретико-правові основи забезпечення національної безпеки України: [монографія]. К.: Інтертехнологія, 2008. 496 с.

64. Концепція (основи державної політики) національної безпеки України, схвалена Постановою Верховної Ради України від 16.01.1997 р. № 3/97-ВР – 02.08.2017 URL: www.rada.gov.ua

65. Закон України «Про основи національної безпеки України» від 19.06.2003 р. – 28.07.2017 [URL: www.rada.gov.ua (дата звернення: 16.02.2018).

66. Зеленков М.Ю. Правовые основы общей теории безопасности российского государства в XXI веке. 20.07.2017 URL: society.polbu.ru/zelenkov_security/ch05_all.html (дата звернення: 16.02.2018).

67. Качинський А.Б. Індикатори національної безпеки: визначення та застосування їх граничних значень. К.: НІСД, 2013. 104 с.

68. Ивашов Л.Г. Экспансия и безопасность. Профи. 1998. № 1/2. С. 19-23

69. Wolfers A. Discord and Collaboration. Essay of International Politics. Foreword by Reinhold Niebuhr; Baltimore: The Johns Hopkins Press, 1962. 312 p.

70. Могилевский В.Д. Системная безопасность: формализованный поход. Материалы конференции «Проблемы внутренней безопасности России в XXI веке». М.: ЭДАС-ПАК, 2001. С. 84-90

71. Горбулін В.П., Качинський А.П. Засади національної безпеки України: [підручник]. К.: Інтертехнологія, 2009. 272 с.

72. Буркин А.И., Возженников А.В., Синеок Н.В. Национальная безопасность России в контексте современных политических процессов: [монография]. М.: Изд-во РАГС, 2008. 480 с.

73. Бельков О.А. О языке теории и политики национальной безопасности России. Национальная безопасность: научное и государственное управленческое содержание: материалы Всеросс. науч. конф., 4 дек. 2009 г., Москва Центр пробл. анал. и гос.-упр. проект. М., 2010. С. 144-155.

74. Сулакшин С.С. Угрозы национальной безопасности и модернизация России. 10.01.2013 URL: http://rusrand.ru/docconf/ugrozy-natsionalnoj-bezopasnosti-i-modernizatsija-rossii (дата звернення: 16.02.2018).

75. Горбулін В.П., Качинський А.Б. Системно-концептуальні засади стратегії національної безпеки України: [монографія]. К., 2007. 592 с.

76. Левин А.А. Приоритетные направления деятельности государства по обеспечению информационной безопасности Российской Федерации (Политологический анализ): Дис. ... канд. полит. наук: 20.01.02. М., 2004. 150 с.

77. Фомин А.А. Юридическая безопасность субъектов российского права (вопросы теории и практики): Дисс. … докт.юрид.наук: 12.00.01. Пенза, 2007. 466 с.

78. Рижук О. Аналіз підходів щодо визначення поняття «інформаційна безпека» в умовах глобалізації. 02.08.2017 URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3007/2697 (дата звернення: 16.02.2018).

79. Золотар О.О. Інформаційна безпека людини:теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с

80. Шамрай В.О. Інформаційна безпека як складова національної безпеки України. 12.06.2016 URL: http:// www.crime-research.org/ articles.html (дата звернення: 16.02.2018).

81. Довгань О.Д. Правові засади формування і розвитку системи забезпечення інформаційної безпеки України. Інформаційна безпека людини, суспільства, держави. 2015, № 3 (19). С. 6-17

82. Стратегія національної безпеки України, затверджена Указом Президента України від 26 травня 2015 року № 287/2015 28.07.2017 URL: www.rada.gov.ua (дата звернення: 16.02.2018).

83. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.

84. Шеннон К. Работы по теории информации и кибернетике. М. : ИЛ, 1963. 830 с.

85. Норберт Винер. Кибернетика или управление и связь в животном и машине. М.: Советское радио, 1968. 325 с.

86. Yarger Richard H, George Barber The U.S. Army War College Mehtodology for Determining Interests and Levels of Intensity. Carlisle Barracs, U.S. Army War College, 1997 URL: http://www.au.af.mil/au/awc/awcgate/army-usawc/natinte.htm

http://www.au.af.mil/au/awc/awcgate/army-usawc/natinte.htm (дата звернення: 16.02.2018).

87. Lerche Ch. Politics Concepts of International in Global. USA, 1979. 263 с.

88. Гудби Дж., Бувальда П., Тренин Д. Стратегия стабильного мира. Навстречу Евроатлантическому сообществу безопасности. М.: Международные отношения, 2003. 208 с.

89. Андрущенко С.В. Україна в сучасному геополітичному середовищі : [монографія]. К. : Логос, 2005. 286 с.

90. Said A. Global Persptctive. USA, 1979. 113 с.

91. Парахонський Б.О. Національні інтереси України (духовно-інтелектуальний аспект): монографія. К.: НІСД, 1993. 43 с.

92. Мануйлов Є.М. Аксіологічний вимір інформаційної безпеки української держави. Вісник Національного університету «Юридична академія України імені Ярослава Мудрого» № 3 (34) 2017. С. 13-30

93. Гоґвуд Б. Аналіз політики для реального світу / Б. Гоґвуд, Л. Ґан ; пер. з англ. А. Олійник ; наук. ред. пер. В. Тертичка. – Київ : Вид-во Соломії Павличко «Основи», 2004. – 396 с.

94. Вебер М. Избранное. Образ общества : пер. с нем. М. : Юристъ, 1994. 704 с.

95. Ларін С.В. Сутність та зміст поняття “національні цінності” в контексті сучасних дослідницьких підходів. Вісник НАДУ при Президентові України № 2. 2016 С. 44-49

96. Горбулін В. На захист національних інтересів. Політика і час. 1995. № 2. С. 3–8

97. Ситник Г. П. Державне управління національної безпеки (теорія і практика). Київ : Вид-во НАДУ, 2004. 408 с.

98. Парахонський Б.О. Національні інтереси України (духовно-інтелектуальний аспект): монографія. К.: НІСД, 1993. 43 с.

99. Марущак А. Інформаційна безпека: правовий аналіз // Детектор медіа 20 травня 2008 URL: https://detector.media/infospace/article/38472/2008-05-20-informatsiina-bezpeka-pravovii-analiz/ (дата звернення: 16.02.2018).

100. Безпека України: якою її бачать американські політичні діячі // MIND UA. 12 ГРУДНЯ 2017. URL: https://mind.ua/publications/20179511-bezpeka-ukrayini-yakoyu-yiyi-bachat-amerikanski-politichni-diyachi (дата звернення: 16.02.2018).

101. Trusted Computer System Evaluation Criteria. US Department of Defense. CSC-STD-001-83, 1983

102. ITSEC. Information Technology Security Evaluation Criteria (ITSEC): Preliminary Harmonised Criteria. Commission of the European Communities, 1991. 1 червня. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-en_pdf.pdf?__blob=publicationFile&v=1 (дата звернення: 16.02.2018).

103. Нестеряк Ю.В. Міжнародні критерії інформаційної безпеки держави: теоретико-методологічний аналіз. Вісник НАДУ. № 3. 2013. С. 40-45

104. Common Criteria for Information Technology Security Evaluation URL: https://www.commoncriteriaportal.org/ (дата звернення: 27.02.2018).

105. Про інформаційну безпеку України : проект Закону України 5732 від 22.09.2004 URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?id=&pf3516=5732&skl=5 (дата звернення: 27.02.2018).

106. IT-індустрія опинилася на третьому місці в структурі експорту України https://news.finance.ua/ua/news/-/411572/it-industriya-opynylasya-na-tretomu-mistsi-v-strukturi-eksportu-ukrayiny-infografika (дата звернення: 27.04.2018).

107. Корж І.Ф. Об’єкт і предмет наукового дослідження в інформаційній сфері. “Інформація і право” № 3(22)/2017. С. 19-26

108. Баранов О.А. Базовий принцип інформаційного права – забезпечення інформаційної безпеки. Запобігання новим викликам та загрозам інформаційній безпеці України: правові аспекти**:** матеріали наук.-практ. конф. 06 жовт. 2016 р. Упоряд. : В. М. Фурашев. Київ : НТУУ «КПІ імені Ігоря Сікорського», Вид-во «Політехніка». 2016. 204 с. С. 29-35

109. Ткачук Т. Ю. Принципи забезпечення інформаційної безпеки держави: інформаційний аспект. Митна справа. 2012. № 1. Ч. 2. С. 399–405

110. Ткачук Т. Ю. Принципи та провідні завдання взаємодії органів державної влади та суб’єктів господарювання у сфері забезпечення національної інформаційної безпеки. Наше право. 2012. № 1. Ч. 1. С. 141–148

111. Ткачук Т. Ю., Журавель В.І. Ризик-діяльність у сфері захисту інформації з обмеженим доступом. Інформаційна безпека людини, суспільства, держави. 2014. № 2. С. 86–95.

112. Ткачук Т. Ю., Журавель В. І. Організаційне проектування у системі захисту конфіденційної інформації суб’єктів господарювання. Інформаційна безпека людини, суспільства, держави. 2014. № 1. С. 76–84

113. Ткачук Т. Ю. Інформаційна безпека держави в онтологічному вимірі. Порівняльно-аналітичне право. 2015. №4. С. 284–287

114. Ткачук Т. Ю. Інформаційна безпека: сучасні підходи до визначення категорії. Актуальні питання публічного та приватного права. 2017. № 2 (16). С. 45–54

115. Bertalanffy L. von. General System Theory – A Critical Review. General Systems. Vol. VII. 1962. P. 1–20

116. Малиновский А.А. Основные понятия и определения теории систем (в связи с приложением теории систем к биологии). Системные исследования. Ежегодник. Наука, М.: Наука, 1980. 384 с.

117. Мишенин А.И. Теории экономических информационных систем. М.: Финансы и статистика, 2002. 240 с.

118. Алексеев С.С. Общая теория права: в 2 т. Т. 1. М.: Юрид. лит., 1981. 361 с.

119. Алексеев С.С. Структура советского права. М.: «Юрид. лит.», 1975. 264 с.

120. Соснін О. Передумови формування в Україні інформаційного права. Право і суспільство. 2005. № 11. С. 99-103

121. Козер Л.А. Функции социального конфликта. Пер. с англ. О.А.Назаровой; Под общ. ред. Л.Г.Ионина. М.: Идея-Пресс, Дом интеллектуал. книги, 2000. 205 с.

122. Окинавская хартия глобального информационного общества (Окинава, 22 июля 2000 года) URL: http://zakon5.rada.gov.ua/laws/show/998_163 (дата звернення: 27.04.2018).

123. Бачило И.Л. Информация — объект права // НТИ. Сер.1, Организация и методика информ. работы. 1999. № 8. 24-29

124. Золотар О.О. Досвід правового забезпечення інформаційної безпеки в країнах східного партнерства ЄС (Молдова, Грузія). LEX PORTUS № 3 (5)’2017. С. 70-80

125. Пилипчук В.Г., Брижко В.М. Проблеми становлення і розвитку інформаційного законодавства в контексті євроінтеграції України. “Інформація і право”, № 1(1). 2011. С. 11-19 с.

126. Мирошниченко М.М. Правове забезпечення інформаційної безпеки держави : автореф. дис. ... канд. юрид. наук : 12.00.07. Київ, 2018. 19 с.

127. Захаренко К.В. Категорія інформаційної безпеки у вітчизняному філософсько-політологічному дискурсі. Гуманітарний вісник ЗДІА. 2018. Випуск 72. С. 44-52

128. Ярема О.Г. Предмет правового забезпечення інформаційної безпеки в інформаційному праві. Науковий вісникЛьвівського державного університету внутрішніх справ. Серія Право. №2. 2016. С. 244-252

129. Панова І. В. Тенденції розвитку системи інформаційного права України на сучасному етапі. Форум права. 2011. № 2. С. 694–699 URL: http://www.nbuv.gov.ua/e-journals/FP/2011-2/11pivnce.pdf (дата звернення: 27.04.2018).

130. Баранов О. Інститути інформаційного права / О. Баранов // "Правова інформатика", № 3 (11) / 2006. С. 39-45

131. Бачило И. Л., Лопатин В. Н., Федотов М. А. Информационное право / Под. ред. Б. Н. Топорнина. СПб: Юрид. центр Пресс, 2001. 789 с.

132. Закон України «Про основи національної безпеки України» від 19 червня 2003 року: URL: http://zakon5.rada.gov.ua/laws/show/964-15 (дата звернення: 27.04.2018).

133. Закон України «Про телекомунікації» від 18.11.2003 року: URL: zakon2.rada.gov.ua/laws/show/1280-15 (дата звернення: 27.04.2018).

134. Michael Nieles, Kelley Dempsey, Victoria Yan Pillitteri. An Introduction to Information Security: URL: https://doi.org/10.6028/NIST.SP.800-12r1 (дата звернення: 27.04.2018).

135. National Security Telecommunications and Information Systems Security. National Training Standard for Information Systems Security (Infosec): URL: www.cnss.gov/Assets/pdf/nstissi_4011.pdf (дата звернення: 27.04.2018).

136. Federal Financial Institutions Examination Council (FFIEC). Information Technology Examination Handbook (IT Handbook): Information Security (2016): URL: https://www/ffiec.gov/press/pdf/ffiec-it-handbook_information_security_booklet.pdf (дата звернення: 27.04.2018).

137. Баришполец В.А. Информационно-психологическая безопасность: основные положення. Информационные технологии. 2013. №2, том 5. С.62-104.

138. Уханова Н.С. Інформаційно-психологічна безпека особистості, суспільства та держави: URL: ippi.org.ua/ ukhanova-ns-informatsiino-psikhologichna-bezpekaosobistosti-suspilstva-ta-derzhavi (дата звернення: 27.04.2018).

139. Николаев А. Государственно-идеологическая компонента информационной безопасности: URL: https://cyberleninka.ru/acticle/v/gosudarstvenno-ideologicheskaya-komponenta-informatsionnoy-bezopasnosti (дата звернення: 27.04.2018).

140. Гулай В.В. Загрози інформаційно-психологічній безпеці особи в реаліях інформаційно-психологічної війни як складової «гібридної війни» Російської Федерації проти України: URL:www. asv.ua/content/nauka/editions/25/2016-25/233-244.pdf (дата звернення: 27.04.2018).

141. Жатканбаева А. Е. Функциональные компоненты информационной безопасности. Право и государство. 2013. № 4. С.74-77

142. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: [монографія]. Одеса: Юридична література, 2003. 472 с.

143. Тихомиров О. О. Забезпечення інформаційної безпеки як функція сучасної держави: [монографія]; заг. ред. Р. А. Калюжний. Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. 196 с.

144. Картка законопроекту «Про основні засади забезпечення кібербезпеки України»: URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?pf3516=2126%D0%B0&skl=9 (дата звернення: 27.04.2018).

145. Рада ухвалила закон про кібербезпеку: URL: https://www.epravda.com.ua/news/2017/10/5/629817/ (дата звернення: 27.04.2018).

146. Корнейко О. Застосування та визначення терміна «інформаційна безпека» в національному законодавстві. Правове,

нормативне та метрологічне забезпечення системи захисту інформації в Україні. Науково-технічний збірник, 2009. Вип. 2(19). С. 9-13

147. Drucker P.F. The Age of Discontinuity. Guidelines to Our Changing Society. London: New Brunswick (US), 1994. P. 370

148. Білак Ю.Ю. Інформаційна безпека як елемент підвищення Ефективності інноваційного розвитку України. Вісник КНУТД №4 (113), 2017. С. 44-50

149. Felix Stalder Information Ecology A position paper (version 1.0) McLuhan Program in Culture and Technology, FIS, UofT, 1997 URL: http://felix.openflows.com/html/infoeco.html (дата звернення: 27.04.2018).

150. Проданюк Р. І. Інформаційна безпека в соціологічному контексті: до постановки проблеми. Науково-теоретичний альманах «Грані». 2018. Т. 21. № 4. С. 84-90

151. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки. URL: http:// journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php (дата звернення: 27.04.2018).

152. Данильян О.Г., Дзьобань О.П., Панов М.І. Національна безпека України: структура та напрямки реалізації: [навчальний посібник]. Х.: Фоліо, 2002. 285 с.

153. Гурковський В.І. Безпека як об’єкт правовідносин в умовах глобального інформаційного суспільства. Правова інформатика. 2010. No 2(26). С. 72-77

154. Нижник Н. Р., Ситник Г. П., Білоус В. Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): [навчальний посібник]. Ірпінь : Акад. ДПС України, 2000. 304 с.

155. Ярочкин В.И., Шевцова Т.А. Словарь терминов и определений по безопасности и защите информации. М.: Ось-89. 1996. 48 с.

156. Калюжний Р. Питання концепції реформування інформаційного законодавства України. Правове, нормативне та

метрологічне забезпечення системи інформації в Україні: Тематичний збірник праць учасників Другої науково-технічної конференції. К., 2000. С.17-21

157. Бєляков К.І. Деякі питання щодо формування реформи інформаційного законодавства України. Систематизація законодавства в Україні: проблеми теорії і практики. Матеріали міжнародної науково-практичної конференції. К.: Інститут законодавства Верховної Ради України, 1999. С. 253-255

158. Шульга В. І. Сучасні підходи до трактування поняття інформаційна безпека. Ефективна економіка, № 4, 2015: URL: http:// http://www.economy.nayka.com.ua/?op=1&z=5514 (дата звернення: 27.04.2018).

159. Лукашов А.И. Информационная безопасность как объект уголовно-правовой охраны в законодательстве Республики Беларусь. Материалы научной конференции «Концептуальные проблемы информационной безопасности в союзе России и Беларуси». СПб., 2000: URL: http://jurfak.spb.ru/ conference/2001.htm (дата звернення: 27.04.2018).

160. Панарин И. Технология информационной войны: [монографія]. М.: КСП+, 2003. 320 с.

161. Громико І., Державна домінантність визначення інформаційної безпеки України в умовах протидії загрозам. Право України. 2008. № 8. С.130-134

162. Баранов А.А. Концептуальные вопросы информационной безопасности Украины. Нормативно-правовая база защиты информации: Сб-к материалов. К., 1997. С. 53-58

163. Остроухов В. До проблеми забезпечення інформаційної безпеки України. Політичний менеджмент. 2008. № 4. С. 135-141

164. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.2007 року: URL: zakon5.rada.gov.ua/laws/show/537-16 (дата звернення: 27.04.2018).

165. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» від 15 березня 2016 року № 96/2016: URL: www.president.gov.ua/documents/962016-19836 (дата звернення: 27.04.2018).

166. Michael Nieles, Kelley Dempsey, Victoria Yan Pillitteri. An Introduction to Information Security: URL: https://doi.org/10.6028/NIST.SP.800-12r1 (дата звернення: 27.04.2018).

167. National Security Telecommunications and Information Systems Security. National Training Standard for Information Systems Security (Infosec): URL: www.cnss.gov/Assets/pdf/nstissi_4011.pdf (дата звернення: 27.05.2018).

168. Federal Financial Institutions Examination Council (FFIEC). Information Technology Examination Handbook (IT Handbook): Information Security (2016): URL: https://www/ffiec.gov/press/ pdf/ffiec-it-handbook_information_security_booklet.pdf (дата звернення: 27.05.2018).

169. Мельник С.В. Понятійно-категоріальний аппарат у системі професійної підготовки майбутніх фахівців з кібербезпеки. Інформаційні технології і засоби навчання. 2016, Том 55, №5 С.187-197

170. Баришполец В.А. Информационно-психологическая безопасность: основные положення. РЭНСИТ: Информационные технологии. 2013. №2, том 5. С. 62-104

171. Николаев А. Государственно-идеологическая компонента информационной безопасности: URL: https://cyberleninka.ru/acticle/v/gosudarstvenno-ideologicheskaya-komponenta-informatsionnoy-bezopasnosti (дата звернення: 27.05.2018).

172. Гулай В.В. Загрози інформаційно-психологічній безпеці особи в реаліях інформаційно-психологічної війни як складової «гібридної війни» Російської Федерації проти України: URL: www.asv.ua/content/nauka/editions/25/2016-25/233-244.pdf (дата звернення: 27.05.2018).

173. Уханова Н.С. Інформаційно-психологічна безпека особистості, суспільства та держави: URL: ippi.org.ua/ukhanova-ns-informatsiino-psikhologichna-bezpekaosobistosti-suspilstva-ta-derzhavi (дата звернення: 27.05.2018).

174. Жатканбаева А. Е. Функциональные компоненты информационной безопасности. Право и государство. 2013. № 4 (61) С.73-77

175. Довгань О.Д. Сучасні інформаційні структури як компоненти інформаційної безпеки. Інформація і право. № 2(14)/2015. С.111-120.

176. Довгань О.Д. Національний інформаційний суверенітет – об'єкт інформаційної безпеки. Інформація і право. № 3(12)/2014. С.102-112.

177. Довгань О.Д. Нейтралізація міжнародних інформаційних загроз. Правова інформатика. № 2(42)/2014. С.80-89

178. Концептуальні засади розвитку системи забезпечення національної безпеки України: аналіт. доп. / О. О. Резнікова, В. Ю. Цюкало, В. О. Паливода, С. В. Дрьомов, С. В. Сьомін. К.: НІСД, 2015. 58 с.

179. Ярочкин В.И. Информационная безопасность: [Учебное пособие для студентов непрофильных вузов]. М.: Междунар. отношения, 2000. 400 с.

180. Довгань О.Д. Правові засади формування і розвитку системи забезпечення інформаційної безпеки України. Інформаційна безпека людини, суспільства, держави. 2015, № 3 (19). С.6-17

181. Пилипчук В.Г. Забезпечення інформаційної безпеки України: сучасні тенденції та проблеми. Запобігання новим викликам та загрозам інформаційній безпеці України: правові аспекти : матеріали наук.-практ. конф. /06 жовт. 2016 р./ Упоряд.: В. М. Фурашев. Київ : НТУУ «КПІ імені Ігоря Сікорського», Вид-во «Політехніка», 2016. С. 24-28

182. Золотар О.О. Загрози інформаційній безпеці людини. Правова інформатика. № 2(42)/2014. С.70-79

183. Т. Ткачук. Складники інформаційної безпеки: аналіз критеріїв.Visegrad journal on human rights. 2017 (4). С.153-158

184. Тихомиров О. Перспективи зміни розуміння інформаційної безпеки. Правова інформатика. № 4(28). 2010 С. 68-75

185. Пилипчук В., Дзьобань О. Глобальні виклики й загрози національній безпеці в інформаційній сфері. Вісник Національної академії правових наук України. № 3 (78) 2014. С.43-52

186. Дзьобань О.П., Соснін О.В. Інформаційна безпека: нові виміри загроз, пов'язаних з інформаційно-комунікаційною сферою. Гуманітарний вісник ЗДІА. 2015. № 60. С.25-34

187. Могилевский В.Д. Системная безопасность: формализованный поход. Материалы конференции «Проблемы внутренней безопасности России в XXI веке». М.: ЭДАС-ПАК, 2001. С. 86-89

188. Закон України «Про основні засади забезпечення кібербезпеки України» від 05 жовтня 2017 року: URL: http://zakon3.rada.gov.ua/laws/show/2163-19 (дата звернення: 27.05.2018).

189. Европейская Конвенция по киберпреступлениям. URL: http://inter.criminology.onua.edu.ua/?p=2263 (дата звернення: 27.05.2018).

190. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» від 25.02.2017 № 47/2017: URL: www.president.gov.ua/documents/472017-21374 (дата звернення: 27.05.2018).

191. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» від 01.05.2014 № 449/2014: URL: www.president.gov.ua/documents/4492014-17157 (дата звернення: 27.05.2018).

192. Доктрина інформаційної безпеки України – це лише декларація – експерти: URL: https://www.radiosvoboda.org/a/28336852.html (дата звернення: 27.05.2018).

193. Довгань О. Д. Інформаційна безпека: стан, проблеми, тенденції. Інформаційні ресурси, інтелектуальна власність, комунікації в освітньо-науковій та інноваційній сферах: філософсько-правові та прикладні аспекти: матеріали круглого столу, 12 травня 2017 р., м. Вінниця / упоряд.: О. Д. Довгань, М. В. Беланюк, С. А. Лапшин, О. Г. Радзієвська, О. І. Яременко; Вінницький державний педагогічний університет ім. М. Коцюбинського [та ін.]. Київ : Видавничий дім «АртЕк», 2017. С. 31-39

194. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 17 січня 2018 року «Про проект Закону України "Про національну безпеку України» від 5 лютого 2018 року № 21/2018: URL: http://zakon3.rada.gov.ua/laws/ show/21/2018/paran2#n2 (дата звернення: 27.05.2018).

195. Ткачук Т. Ю. Теоретичний дискурс пошуку основних складових системи інформаційної безпеки держави. Jurnalul juridic national: teorie şi practică. 2018. № 2. С. 45-47

196. Ткачук Т. Ю. Обґрунтування потреби наукової розробки теоретико-правових засад комплексного захисту інформації з обмеженим доступом. Актуальні проблеми управління інформаційною безпекою держави: НА СБУ (Київ, 19.03.15). С. 368–371

197. Ткачук Т. Ю. Витоки гібридної війни та сучасні її технології. Пріоритетні напрями наукових досліджень: Мат. II Міжнарод. наук.-практ. конф. (Київ, 15–16.08.17) : МЦНД, 2017. С. 79–81

198. Ткачук Т. Ю. Кібербезпека: підходи до визначення в окремих країнах. Актуальні проблеми управління інформ. безпекою держави : мат. наук.-практ. конф. (Київ, 24.05.17). 2017. С. 142–144

199. Ткачук Т. Ю. Інформаційна безпека держави як пріоритетна складова національної безпеки. Верховенство права та правова держава : мат. міжн. наук.-практ. конф. (Ужгород, 15–16.09.17). 2017. С. 142–145

200. Ткачук Т. Ю. Теоретико-правове осмислення інформаційної безпеки держави у контексті розвитку інформаційного суспільства. Теоретико-правові основи формування та розвитку інформаційного суспільства : мат. наук.-практ. конф. (Київ, 29.11.17). 2017. С. 111–114

201. Ткачук Т. Ю. Інформаційна безпека держави у контексті національної безпеки. Science, research, development state and law. #2 (London, 27.02.18). С. 39–43

202. Ткачук Т. Ю. Взаємозв'язок національних цінностей, інтересів та цілей у концепції правового забезпечення інформаційної безпеки держави. Права, свободи і безпека людини в інформаційній сфері : мат. наук.-практ. конф. (Київ, 10.05.18). 2018. С. 47–50

203. Закон України «Про національну безпеку України» від 21.06.2018 №2496: URL: http://zakon3.rada.gov.ua/laws/show/2469-19 (дата звернення: 27.05.2018).

204. Лесков М.А. Гомеостатические процессы и теория безопасности. Безопасность. Инф. сб. 1994. №4(20). С. 66-67

205. Горлач М.І., Кремень В.Г. Політологія: наука про політику. К.: Центр Учбової літератури, 2009. 840 с.

206. Антонов А.Б., Балашов В.Г. Основы обеспечения безопасности личнос¬ти, общества и государства [учебное пособие. М.: Институт защиты предпринимателя, 1996. С.36-55

207. Ожегов С.И. Словарь русского языка. М.: Рус.яз., 1988. 748 с.

208. Словник української мови: [в 11-ти т.]. АН УРСР, Ін-т мовознавства ім.О.О. Потебні; [редкол.: І.К. Білодід (голова) та ін.]. Т.3 [ред.: Г.М. Гнатюк, Т.К. Черторизька]. К.: Наукова думка, 1972. 744 с.

209. Гордиенко В.В. Безопасность России в условиях глобализации (криминологические и социально-правовые проблемы): дисс. … докт. юрид. наук: 12.00.08. М., 2005. 409 с.

210. Гацко М. О соотношении понятий «угроза» и «опасност. Обозреватель – Observer: URL: observer.materik.ru/observer/N07_97/7_06.htm (дата звернення: 27.04.2018)

211. Дзлиев М.И., Урсул А.Д. Основы обеспечения безопасности России: [учебное пособие]. М.: Рос. гос. торгово-экон. ун-т, НИИ проблем безопасности и устойчивого развития, 2003. 423 с.

212. Возженников А.В. Парадигма национальной безопасности реформирующейся России. 2-е изд. М.: ЭДАК ПАК, 2000. 358 с.

213. Кардашова И.Б. МВД России в системе обеспечения национальной безопасности Российской Федерации: [монография].. М.: ВНИИ МВД России, 2006. 208 с.

214. Жаглин А.В. Общественная безопасность как социальное явление и элемент системы национальной безопасности. Вестник ВИ МВД России. 2007. №1. С.31-34

215. Общая теория национальной безопасности: [учебник]. под общ. ред. А.А. Прохожева, изд. 2. М.: РАГС. 2005. 344 с.

216. Гацко М. Ф. О типологии угроз военной безопасности Российской Федерации и их правовой регламентации. Стратегоческая стабильность. 2006. № 1(34). С. 52-60

217. Методика реагування на виклики, небезпеки та загрози національній безпеці держави: [навчальний посібник]. К.: НАДУ, 2009. 40 с.

218. Прохожев А.А. Теоретико-методологические основы безопасности России. Безопасность России в XXI веке. М.: РИЦ ИСПИ РАН, 2006. С. 129-140

219. А. Брега. Риск в системе категорий, характеризующих антитезу национальной безопасности. URL: http://www.milpol.ru/data/2009/1-12/brega_risk_doklad_konf_nb.doc (дата звернення: 27.07.2018)

220. Хілько О.Л. Визначення загроз національній безпеці в українській теоретико-політичній думці. URL: sevntu.com.ua/jspui/bitstream/123456789/ 1835/politolog.52.2003.48-56.pdf

221. Сулакшин С.С. Угрозы национальной безопасности и модернизация России. URL: http://rusrand.ru/docconf/ugrozy-natsionalnoj-bezopasnosti-i-modernizatsija-rossii (дата звернення: 27.07.2018)

222. Литвин М.М., Кохан В.Г. Умови та фактори внутрішньої загрози національній безпеці України. URL: plesetsk-info.ru/uchebnoe-posobie/umovi-ta-faktori-vnutrshno-zagrozi-natconalni-bez (дата звернення: 27.07.2018)

223. Ліпкан В.А. Національна безпека України: [навчальний посібник]. Київ, КНТ, 2009. 576 с.

224. Хусаинов М.И. Современные подходы к классификации транснациональных угроз безопасности. Вестник Военного университета. 2010. № 1 (21). С. 65-70

225. Мешкова Т. А. Безопасность в условиях глобальной информатизации: новые вызовы и новые возможности: Автореф. дисс. ... канд. юрид. наук: 23.00.04. М., 2009. 26 с.

226. Актуальні виклики та загрози регіональній безпеці: висновки для України; за заг.ред. К.А. Кононенка: аналіт.доп. / Б.Парахонський, Г.Яворська. К.: НІСД, 2014. 48 с.

227. Шерстюк В.П. Информационная безопасность в системе обеспечения национальной безопасности России, федеральный и региональный аспекты обеспечения информационной безопасности. Информационное общество. 1999. № 5. С. 3-5

228. Прокоф'єва-Янчиленко Д.М. Кримінологічна безпека як інтегративна складова національної безпеки. Наукові праці Національного

університету «Одеська юридична академія». 2014. № 14: URL: naukovipraci.nuoua.od.ua/tom-xiv (дата звернення: 27.07.2018)

229. Цивілізаційний вибір України: парадигма осмислення і стратегія дії: [національна доповідь] / ред.кол.: С.Пирожков, О.Майборода, Ю.Шайгородський та ін.; Інститут політичних і етнонаціональних досліджень ім. І.Ф.Кураса НАН України. К.: НАН України, 2016. 284 с.

230. Інформаційна безпека (соціально-правові аспекти): [підручник]. В.Остроухов, В.Петрик, М.Присяжнюк та ін.; за ред. Є. Д. Скулиша. К. : КНТ, 2010. 776 с.

231. Дереко В.Н. Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки. Інформаційна безпека людини, суспільства, держави. 2015. № 2 (18). С.16-22

232. Хмелевський Р.М. Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності. Сучасний захист інформації. 2016. №4. С.65-70

233. Александрович П.И., Ковалев И.П. Психологические методы и средства обеспечения информационной безопасности личности/ П. Александрович, И.Ковалев. Материалы научной конференции «Концептуальные проблемы информационной безопасности в союзе России и Беларуси»: URL: http://jurfak.spb.ru/conference/2001.htm (дата звернення: 27.07.2018)

234. Горбенко І.Д., Долгов В.І., Гріненко Т.О. Інформаційна війна - сутність, методи та засоби ведення. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: Матеріали ювілейної науково-технічної конференції. К., 1998. С. 36-40

235. Красноступ М.Д. Інформаційна війна - міфи чи реальність? Інформаційні технології та захист інформації. 1999. №1. С.111-136

236. Кузнецов П.А. Информационная война и бізнес. Конфидент. 1996. № 4. С. 21-23

237. Прокоф’єва Д.М. Інформаційна війна та інформаційна злочинність. Вісник Запорізького юридичного інституту. 2000. №1. С.288-307

238. Ярмиш Н. Проблема інформаційної причинності у науці кримінального права. Право України. 2003. № 7. С. 28-30

239. Світлична В.Ю., Світлична Т.І. Інформаційна безпека: багатогранність сутності, види загроз та шляхи забезпечення. Науково-технічний збірник. Х.: ХНАМГ. 2013. №109. С.360-369.

240. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: [монография]. К.: Інтертехнологія, 2009. 164 с.

241. Хананашвили М.М. Информационные неврозы. М. Хананешвили. М.: Медицина, 1986. 310 с.

242. Сопілко І.М. Інформаційні загрози та безпека сучасного українського суспільства. Юридичний вісник. 2015. № 1 (34). С.75-80

243. Куцька О.М. Особливості інформаційно-психологічного впливу Російської Федерації напередодні та початковому етапі антитерористичної операції на сході України. Інформаційна безпека людини, суспільства, держави. 2017. № 1(21). С.180-190

244. Снитко О.С. Проекти тотального зомбування в інформаційному просторі України. Інформаційна безпека людини, суспільства, держави. 2017. № 1(21). С.207-215

245. Юрченко И.А. Понятие и виды информационных пре ступлений. Российское право в Интернете. 2003. № 1 URL: http://rli.consultant.ru/ magazine/2003/01 (дата звернення: 27.07.2018)

246. Крылов В.В. Расследование преступлений в сфере информации. М.: Издательство «Городец», 1998. 264 с.

247. Платоненко А. В. Сучасні загрози інформаційної безпеки для державних та приватних установ України. Сучасний захист інформації. 2015. №4. С.86-90

248. Thor Olavsrud. 4 information security threats that will dominate 2017. CIO (December 29, 2016): URL: https:cio.com/article/3153706/security/4-information-security-threats-that-will-dominate-2017.html (дата звернення: 27.07.2018).

249. Силаева В.Л. Интернет и подмена реальности/ В.Силаева // Общество электронных коммуникаций: новые возможности и актуальные проблемы: Материалы VI Энгельмейеровских чтений. Москва-Дубна, 22-23.03.2002. Дубна, 2003. С. 138-141

250. Банников К. Трансцедентное в культуре. URL: www.liber.rsuh.ru/Conf/Etnos/bannikov.htm (дата звернення: 27.07.2018).

251. Маркеева А.В. Интернет вещей (IOT): возможности и угрозы для современных организаций. URL: https://cyberleninka.ru/article/n/internet-veschey-iot-vozmozhnosti-i-ugrozy-dlya-sovremennyh-organizasiy (дата звернення: 27.07.2018).

252. Живко З.Б., Живко М.О. Інформаційні загрози: суть і проблеми. Тези доповідей ІІ міжнародної НПК «Безпека та захист інформації в інформаційних системах». С.116-118

253. Домбровська С. М. Механізми забезпечення інформаційної безпеки як складової державної безпеки України. Теорія та практика державного управління. 2015. Вип. 1 (48). С.2-4

254. Григор'єв В.І. Технології сучасної інформаційно-психологічної війни. Інформаційна безпека людини, суспільства, держави. 2015. № 3 (19). С.48-52

255. Благодарний А.М., Штельмах О.В. Організаційні аспекти протидії інформаційній агресії як складової гібридної війни. Інформаційна безпека людини, суспільства, держави. 2015. № 2 (18). С.6-15.

256. Пилипчук В.Г., Дзьобань О.П. Проблема агресії і насильства: світоглядно-інформаційний вимір. URL: social-science.com.ua/article/806

257. Radicalisation Awareness Network (RAN): URL: http://ec.europa.eu/dgs/hame-affairs/what-we-do/networks/radicalisation_ awareness_network/ index-en.html (дата звернення: 27.07.2018).

258. The Global Information Technology Report 2016 Innovating in the Digital Economy. Insight Report/ World Economic Forum-2016: URL: http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_ Report.pdf (дата звернення: 27.07.2018).

259. Пономаренко Л.В. Інноваційні підходи до попередження радикалізації настроїв і проявів екстремізму в контексті забезпечення сталого демократичного розвитку. Інформаційна безпека людини, суспільства, держави. 2017. № 1 (21). С.74-81

260. Штельмах О.В. Організаційні аспекти протидії інформаційній агресії як складової гібридної війни. Актуальні проблеми управління державною безпекою: зб. Матер.наук.-практ. Конф (Київ, 19 березня 2015). К. Центр навч., наук. Та період.видань НА СБ України, 2015. С.393-396

261. Прозоров А.Ю. Ціннісні основи інформаційної безпеки особи, суспільства та держави. Інформаційна безпека людини, суспільства, держави. 2016. № 1 (20). С.29-37.

262. Размєтаєва Ю.С. Приватність в інформаційному суспільстві: проблеми правового розуміння та регулювання. Науковий вісник Ужгородського національного університету: серія «Право». Випуск 37, том 1. 2016. С.43-46

263. Брега А. Риск в системе категорий, характеризующих антитезу национальной безопасности – 02.09.2014 URL: http://www.milpol.ru/data/2009/1-12/brega_risk_doklad_ konf_nb.doc (дата звернення: 10.08.2018).

264. Гриненко І.М., Ковальчук А.Ю., Прокоф'єва-Янчиленко Д.М., Сокрут Б.В. Управління ризиками організованої злочинності в Україні. К.: ВАІТЕ, 2013. 380 с.

265. Гриненко І.М., Прокоф'єва-Янчиленко Д.М., Сокрут Б.В.

Ризики та загрози організованої злочинності в Україні: стан та перспективи. Київ, ВАІЕУ, 2014. 194 с.

266. Recommendation of the Council on the Governance of Critical Risks. Paris, 6-7 May 2014: URL: http://www.oecd.org/mcm/C-MIN%282014%298-ENG.pdf (дата звернення: 10.08.2018).

267. Rasmussen M.V. The Risk Society at War: Terror, Technology and Strategy in the Twenty-First Century. Cambridge: Cambridge University Press, 2006. P. 34.

268. National Security Strategy of the United States, The White House, February. 2015: URL: https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf (дата звернення: 10.08.2018).

269. Andrews and Bonta (2006-2007). Risk-need-responsivity model for offender assessment and rehabilitation. Public Safety Canada, Ottowa, Ontario. URL: http://www.publicsafety.gc.ca/ res/cor/rep/risk_need_200706-eng.aspx (дата звернення: 10.08.2018).

270. Олійник О. В. Структура суб'єктів забезпечення інформаційної безпеки в Україні. Актуальні проблеми держави і права. URL: http://www.apdp.in.ua/v69/18.pdf (дата звернення: 10.08.2018).

271. Левицька М. Б. Теоретико-правові аспекти забезпечення національної безпеки органами внутрішніх справ України : дис. … канд. юрид. наук : 12.00.01. К., 2002. 206 с.

272. В.Гусаров. Матриця інформаційної безпеки. URL: http://mediarnbo.org/2014/11/25/matritsya-informatsiynoyi-bezpeki-ukrayi/

273. Закон України «Про Раду національної безпеки і оборони України» від 05 березня 1998 року. URL: http://zakon3.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80 (дата звернення: 10.08.2018).

274. Закон України «Про Кабінет Міністрів України» від 27 лютого 2014 року. URL: http://zakon3.rada. gov.ua/laws/show/794-18 (дата звернення: 10.08.2018).

275. Положення про Державну службу України з питань захисту персональних даних, затверджене Указом Президента України від 06 квітня 2011 року № 390/2011. URL: http://zakon2.rada.gov.ua/laws/show/390/2011 (дата звернення: 10.08.2018).

276. Положення про Про Національну комісію, що здійснює державне регулювання у сфері зв'язку та інформатизації, затверджене Указом Президента України від 23 литопада 2011 року № 1067/2011. URL: http://zakon2.rada.gov.ua/laws/ show/1067/2011 (дата звернення: 28.08.2018).

277. Зайцев М. Суб'єкти забезпечення інформаційної безпеки України. URL: http://nbuv. gov. ua/j-pdf/FP_index. htm_2013_3_40.pdf (дата звернення: 28.08.2018).

278. Попова Т. Безпека інформаційного простору України. Координувати чи ні? URL: http://www.radiosvoboda.org/a/28337376.html (дата звернення: 28.08.2018).

279. Положення про Міністерство інформаційної політики України, затверджене постановою Кабінету Міністрів України від 14 січня 2015 року № 2. URL: http://mip.gov.ua/cr/documents/ 7.html (дата звернення: 28.08.2018).

280. Положення про Міністерство оборони України, затверджене Указом Президента України від 06 квітня 2011 року № 406/2011. URL: http://zakon3.rada.gov.ua/laws/ show/406/2011 (дата звернення: 28.08.2018).

281. Положення про Генеральний штаб Збройних Сил України, затверджене Указом Президента України від 06 квітня 2011 року № 406/2011. URL: http://zakon3.rada.gov.ua/laws/ show/406/2011(дата звернення: 28.08.2018).

282. Закон України «Про Службу безпеки України» від 25 березня 1992 року. URL: http://zakon3.rada. gov.ua/laws/show/2229-12 (дата звернення: 28.08.2018).

283. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23 лютого 2006 року. URL:

http://zakon2.rada.gov.ua/laws/show/3475-15 (дата звернення: 28.08.2018).

284. Закон України «Про Службу зовнішньої розвідки України» від 01 грудня 2005 року. URL: http://zakon3.rada.gov.ua/laws/show/3160-15 (дата звернення: 30.08.2018).

285. Закон України «Про розвідувальні органи України» від 22 березня 2001 року. URL: http://zakon3.rada.gov.ua/laws/show/2331-14 (дата звернення: 30.08.2018).

286. Закон України «Про Національну поліцію» від 02 липня 2015 року. URL: http://zakon5.rada.gov.ua/ laws/show/580-19 (дата звернення: 30.08.2018).

287. Закон України «Про Національний банк України» від 20 травня 1999 року. URL: http://zakon2.rada. gov.ua/laws/show/679-14 (дата звернення: 30.08.2018).

288. Положення про Державну службу України з питань захисту персональних даних, затверджене Указом Президента України від 06 квітня 2011 року № 390/2011. URL: http://zakon2.rada.gov.ua/laws/show/390/2011 (дата звернення: 30.08.2018).

289. Положення про Про Національну комісію, що здійснює державне регулювання у сфері зв'язку та інформатизації, затверджене Указом Президента України від 23 липопада 2011 року № 1067/2011. URL: http://zakon2.rada.gov.ua/laws/ show/1067/2011 (дата звернення: 30.08.2018).

290. Положення про Міністерство культури України, затверджене Постановою Кабінет Міністрів України від 03 вересня 2014 року № 495. URL: http://zakon3.rada.gov.ua/ laws/show/495-2014-%D0%BF (дата звернення: 30.08.2018).

291. Положення про Державне агентство України з питань кіно, затверджене Постановою Кабінет Міністрів України від 17 липня 2014 року № 277. URL: http://zakon2.rada.gov. ua/laws/show/277-2014-%D0%BF

292. Закон України «Про Національну раду України з питань телебачення і радіомовлення» від 23 вересня 1997 року. URL:

http://zakon2.rada.gov.ua/laws/show/538/97-%D0%B2%D1%80 (дата звернення: 30.08.2018).

293. Положення про Державний комітет телебачення і радіомовлення України, затверджене Постановою Кабінету Міністрів України від 13 серпня 2014 року № 341. URL: http://zakon3. rada.gov.ua/laws/show/341-2014-%D0%BF (дата звернення: 10.09.2018).

294. Доктрина інформаційної безпеки України, затверджена Указом Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України. URL: http://www.president. gov.ua/documents/472017-21374 (дата звернення: 10.09.2018).

295. Зайцев М. М. Суб'єкти забезпечення інформаційної безпеки України. Форум права. 2013. № 3. С. 231-238

296. Ткачук Т.Ю. Інформаційна безпеки у системі національної безпеки держави. Освіта і наука у сфері національної безпеки: проблеми та пріоритети розвитку : збірник наукових праць за матеріалами Міжнародної науково-практичної конференції (8 червня 2018 р., м. Острог). Острог: Видавництво Національного університету «Острозька академія», 2018. С. 138-140

297. Ткачук Т. Ю. Аксіологічні константи інформаційної без пеки держави. Актуальні проблеми управління інформац. безпекою держави : мат. всеукр. наук.-практ. конф. (Київ, 30.03.18). НА СБУ, 2018. С. 167–169

298. Ткачук Т. Ю. Протидія кіберзагрозам у країнах позаблокового статусу. Освіта і наука у сфері нац. безпеки: проблеми та пріоритети розвитку : мат. міжнарод. наук.-практ. конф. (Острог, 01.12.17). С. 66–70

299. Ткачук Т. Ю. Інформаційний чинник у гібридній війні. Кібербезпека у системі нац. безпеки України: пріоритетні напрями розвитку : мат. наук. круглого столу (Маріуполь, 26.04.18). МДУ, 2018. С. 39–42

300. Ткачук Т. Ю. Аксіологічні складові об'єкта правового

забезпечення інформаційної безпеки України. Сучасна юриспруденція Європейського Союзу: взаємодія права, нормотворчості та практики : мат. міжнарод. наук.-практ. конф. (Люблін, 17.04.18). 2018. С. 83–86

301. Ткачук Т. Ю. Теоретико-правове осмислення інформаційної безпеки держави у контексті розвитку інформаційного суспільства. Теоретико-правові основи формування та розвитку інформаційного суспільства : мат. наук.-практ. конф. (Київ, 29.11.17). 2017. С. 111–114

302. Ткачук Т. Ю. Суб'єкти забезпечення інформаційної безпеки держави: функціональний аналіз. Jurnalul juridic national: teorie şi practică. 2017. № 6. С. 42–46

303. Ткачук Т. Ю. Механізми протидії інформаційним загрозам зовнішніх джерел. Вісник НТУ України «Київський політехнічний інститут». Політологія. Соціологія. Право. 2017. № 1–2. С. 242–246.

304. Ткачук Т. Ю., Довгань О.Д. Система інформаційної безпеки України: онтологічні виміри. Інформація і право. 2018. № 1 (24). С. 89–104.

305. Ткачук Т. Ю., Довгань О. Д. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс. Інформація і право. 2018. № 2 (25). С. 73–85

306. Ткачук Т. Ю., Журавель В. І. Соціальна складова менеджменту у системі захисту інформації з обмеженим доступом. Інформ. безпека людини, суспільства, держави. 2015. № 3 (19). С. 93–102

307. Ткачук Т. Ю. Напрями імплементації міжнародних стандартів захисту персональних даних у законодавство України. Митна справа. 2010. № 5. Ч. 2. С. 3–9

308. Закон України «Про внесення змін до деяких законів України щодо зовнішньополітичного курсу України» від 08.06.2017 року. URL: www.zakon.rada.gov.ua/laws/show/2091-19 (дата звернення: 10.09.2018).

309. Закон України «Про засади внутрішньої і зовнішньої політики» від 01.07.2010 року. URL: www.zakon.rada.gov.ua/ laws/show/ 2411-17 (дата

звернення: 10.09.2018).

310. Політанський В.С. Інформаційне суспільство в Україні: від зародження до сьогодення. Науковий вісник Ужгородського національного університету: серія «Право». Випуск 42. 2017. С.16-22.

311. Політанський В.С. Світові моделі та фундаментальні принципи інформаційного суспільства. Науковий вісник Ужгородського національного університету: серія «Право». Випуск 43, том 1. 2017. С.34-39

312. Костенко О.В. Європейські стандарти правового регулювання обігу інформації з обмеженим доступом у роботі органів прокуратури/ О. Костенко. Науковий вісник Ужгородського національного університету: серія «Право». Випуск 34, том 3. 2015. С.109-114

313. Малик Я. Забезпечення інформаційної безпеки України у контексті світового досвіду. Збірник наукових праць: «Ефективність державного управління». Випуск 32. 2012. С.20-27

314. Background information on the Alliance, its policies, activities and structures. URL: http://www.nato.int/cps/en/natohq/ topics.htm (дата звернення: 10.09.2018).

315. Феденько С. Взаємодія України з НАТО у сфері інформаційної безпеки. URL: http://nato.pu.if.ua/old/ jornal/2009/2009-35.pdf (дата звернення: 10.09.2018).

316. Document C-V(2002)49: Security within tne North Atlantic Treaty Organization (NATO). URL: www.statewatch.org/ news/2006/sep/nato-sec-classifications.pdf (дата звернення: 10.09.2018).

317. Kaija E. Schilde. Cosmic top secret Europe? The legacy of North Atlantic Treaty Organization and cold war US policy on European Union information policy. URL: http://dx.doi.org/10.1080/09662839. 2014.911175 (дата звернення: 10.09.2018).

318. William D. Gerhard, Henry W. Millington Attack on a Sigint Collector.URL: http://nsarchive.gwu.edu/NSAEBB/NSAEBB24 /nsa10.pdf

(дата звернення: 10.09.2018).

319. Al. S. Roberts. Entangling Alliances: Nato's security of information policy and the entrenchment of State Secrecy. URL: https://www.researchgate.net/profile/Alasdair_Roberts/publication/228222455_ (дата звернення: 10.09.2018).

320. Партнерство заради миру: Рамковий документ, підписаний Україною 8 лютого 1994 року (набув чинності для України 8 лютого 1994 року). Офіційний вісник України. 2006. № 48. Ст. 3232

321. Проблеми застосування в Україні норм інформаційної безпеки НАТО. URL: http://www.db.niss.gov.ua/docs/ polmil/1fgs93.htm (дата звернення: 10.09.2018).

322. План дій Україна-НАТО (за матеріалами Національного центру з питань Євроантлантичної інтеграції України. URL: http://www.nceai.gov.ua/plan.phtml (дата звернення: 10.09.2018).

323. Указ Президента України «Про затвердження Річної національної програми під егідою Комісії Україна – НАТО на 2017 рік» від 08.04.2017 № 103/2017. URL: http://www.president.gov.ua/documents/1032017-21670 (дата звернення: 10.09.2018).

324. John E Dunn. NATO clause V could deter cyber attack, says defence minister. URL: https://www.networkworld.com/ article/2194246 (дата звернення: 10.09.2018).

325. North Atlantic Treaty Organization. Active Engagement/ Modern Defence Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation. URL: http://www.nato.int/lisbon2010/strategic–concept–2010–eng.pdf (дата звернення: 10.09.2018).

326. Cornish, P. Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks. Brussels: European Parliament, 2014. 34 p.

327. NATO Bucharest Summit Declaration, 3 April 2008. URL: http://www.nato.int/docu/pr/2008/p08-049e.html (дата звернення: 10.09.2018).

328. North Atlantic Treaty Organization. Defending against cyber

attacks. URL: http://www.nato.int/cps/en/natolive/topics_49193.htm (дата звернення: 10.09.2018).

329. Пилипчук В.Г. Інформаційна сфера як складова гібридної війни. Актуальні проблеми управління інформаційною безпекою держави : зб. тез наук. доп. наук.-практ. конф. (Київ, 30 березня 2018 р.). Київ : Нац. акад. СБУ, 2018. 408 с.

330. NATO Lisbon Summit Declaration, 20 Nowember 2010. URL: http://www.nato.int/docu/pr/2010/p10-049e.html (дата звернення: 10.09.2018).

331. Geers, K. Strategic Cyber Security/ K. Geers. – NATO Cooperative Cyber Defence Centre of Excellence, 2011. 169 p.

332. Бєлоусова Н.Б., Афанасьєва П.А. Основні вимоги НАТО щодо забезпеченння безпеки інформаційного простору. Актуальні проблеми міжнародних відносин. Випуск 102, частина І. 2011 С. 196-202

333. NATO CCD CoE Mission and Vision. URL: http: //www.ccdcoe.org/11.html (дата звернення: 10.09.2018).

334. NATO Cyber defence. URL: http://www.nato.int/cps/en/natohq/topics_78170.htm (дата звернення: 15.10.2018).

335. Центр информационной безопасности НАТО выпустил книгу о кибервойне Украины с Россией. URL: http://www.dut.edu.ua/ru/news-1-574-2267 (дата звернення: 15.10.2018).

336. Hughes, R.B. NATO and Cyber Security: Mission accomplished? URL: http://www.carlisle.army.mil/DIME/documents/ NATO%20and%20Cyber%20Defence.pdf (дата звернення: 15.10.2018).

337. NATO CCD CoE General Trends: [Online tool]. – Available at URL: http: //www.ccdcoe.org/8.html (дата звернення: 15.10.2018).

338. NATO Warsaw Summit Communiqué, 9 July 2016 URL: http://www.nato.int/cps/en/natohq/official_texts_133169.htm (дата звернення: 15.10.2018).

339. The North Atlantic Treaty. Washington D.C. URL: www.nato.int/cps/ru/natohq/official_text_17120.htm (дата звернення:

15.10.2018).

340. Goldgeier, J. The Future of NATO / J. Goldgeier // NATO Science for Peace and Security Series, E: Human and Societal Dynamics. – Amsterdam : IOS Press, 2011. Vol. 76. P. 1–12.

341. Казаковцев А.В. НАТО и кибербезопасность / А.Казаковцев// Вестн. Волгогр. гос. ун-та. Сер. 4, Ист. 2012. № 2 (22) С.109-114

342. Kempf, A. Considerations for NATO Strategy on Collective Cyber Defense URL: http://csis.org/blog /considerations-nato-strategy-collective-cyberdefense (дата звернення: 26.10.2018).

343. Політанський В.С. Інформаційне суспільство в Україні: від зародження до сьогодення. Науковий вісник Ужгородського національного університету: серія «Право». Випуск 42. 2017. С.16-22

344. Політанський В.С. Світові моделі та фундаментальні принципи інформаційного суспільства. Науковий вісник Ужгородського національного університету: серія «Право». Випуск 43, том 1. 2017. С.34-39

345. Federal Act on Data Protection (FADP) of 19 June 1992 URL: https://www.admin.ch/opc/en/classified-compilation/19920153/ index.html (дата звернення: 26.10.2018).

346. Швейцария признала незаконным сбор IP-адресов в интересах правообладателей URL: http://www.itsec.ru/newstext.php?news_id=70187 (дата звернення: 26.10.2018).

347. National strategy for Switzerland's protection against cyber risks. URL:https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Switzerlands_Cyber_Security_strategy.pdf (дата звернення: 26.10.2018).

348. Федеральный совет Швейцарии прокомментировал закон об информационной безопасности. URL: http://goldblum.eu/ru/pravovye-novosti/federalnyy-sovet-shveycarii-prokomm/ (дата звернення: 26.10.2018).

349. Information Tecnhology Security Evaluation Criteria. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ Zertifizierung/ITS

icherheitskriterien/itsec-en_pdf.pdf (дата звернення: 26.10.2018).

350. Common Criteria for Information Technology Security Evaluation. URL:https://www.commoncriteriaportal.org/files/ccfiles/CCPART 2V3.1R4.pdf (дата звернення: 26.10.2018).

351. Communication from the European Commission: Network and Information Security: Proposal for a European Policy Approach. COM (2001). URL: http://ec.europa.eu/information_society/eeurope/2002/ news_library/ pdf_files/netsec_en.pdf (дата звернення: 26.10.2018).

352. Communication from the Commission: Towards a general policy on the fight against cyber crime. COM (2007). URL: http://eurlex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf. (дата звернення: 30.10.2018).

353. Communication from the Commission on Critical Information Infrastructure Protection: Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. COM (2009) URL: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ ciip/index_en.htm. (дата звернення: 30.10.2018).

354. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року. URL: http://zakon2.rada.gov.ua/laws/show/994_242. (дата звернення: 30.10.2018).

355. В Евросоюзе приняли новый закон о защите даннях. URL: https://threatpost.ru/v-evrosoyuze-prinyali-novyj-zakon-o-zashhite-dannyh/15749/ (дата звернення: 30.10.2018).

356. ENISA Country Reports. URL: http://www.epractice.eu/ files/media/media2624.pdf. (дата звернення: 30.10.2018).

357. CERT-Fi. URL: http://www.cert.fi/en/index.html. (дата звернення: 30.10.2018).

358. Communication from the Commission on Critical Information Infrastructure Protection: Protecting Europe from large scale cyber-attacks and

disruptions: enhancing preparedness, security and resilience (2009). URL: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm. (дата звернення: 30.10.2018).

359. В Финляндии открылся центр информационной безопасности. URL: http://www.goodnewsfinland.ru/cgi-otkryvaet-v-finlyandii-novyj-tsentr-informatsionnoj-bezopasnosti/. (дата звернення: 30.10.2018).

360. Finnish Security and Defence Policy (2012). URL: https://www.bbn.gov.pl/ftp/dok/07/FIN_Finnish_Security_Defence_Policy_2012_Government_Report.pdf (дата звернення: 30.10.2018).

361. Finland's Cyber Security Strategy (2013). URL: http://www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/40-finlandas-cyber-security-strategy (дата звернення: 02.11.2018).

362. Орпо: надо как можно скорее разрешить сетевую разведку. URL: http://yle.fi/novosti/novosti/article8459992.html (дата звернення: 02.11.2018).

363. Austrian Security Strategy (2013). URL: https://www.bka.gv.at/DocView.axd?CobId=52251 (дата звернення: 02.11.2018).

364. Austrian Cyber Security Strategy (2013). URL: https://www.bka.gv.at/DocView.axd?CobId=50999 (дата звернення: 02.11.2018).

365. Зозуля О. С. Зарубіжний досвід державного управління забезпеченням інформаційної безпеки в умовах інформаційно-психологічного протиборства. Науково-інформаційний вісник Академії національної безпеки. 2016. № 1-2. С. 28-38

366. Климчук О.О., Ткачук Н.А. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки. Інформаційна безпека людини, суспільства, держави. 2015. № 3 (19). С.75-83.

367. Microsoft вложит в дата-центр в Ирландии дополнительные 170

млн евро. URL: https://www.bka.gv.at/DocView.axd?CobId=52251 http://www.itsec.ru/newstext.php?news_id=97395 (дата звернення: 02.11.2018).

368. Как сегодня обезопасить кибербезопасность завтрашнего дня? URL: https://www.kaspersky.ru/blog/ dublin-forum-2016/13013/ (дата звернення 03.10.2018) (дата звернення: 02.11.2018).

369. National Cyber Security Strategy: Securing our Digital Future. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM: 2009 0149:FIN:EN:PDF (дата звернення: 02.11.2018).

370. The World Factbook: Central Intelligence Agency. URL: https://www.cia.gov/library/publications/the-world-factbook/fields/2144.html (дата звернення: 02.11.2018).

371. Республика Хорватия // Гуманитарные технологии: Аналитический портал**.** URL: http://gtmarket.ru/ countries/croatia/ croatia-info

372. NATO Bucharest Summit Declaration, 3 April 2008: [Online tool]. – Available at: http://www.nato.int/docu/pr/2008/p08-049e.html (дата звернення: 17.11.2018).

373. Common Criteria for Information Technology Security Evaluation. URL:https://www.commoncriteriaportal.org/files/ccfiles/CCPART 2V3.1R4.pdf (дата звернення: 17.11.2018).

374. Communication from the European Commission: Network and Information Security: Proposal for a European Policy Approach. COM (2001) 298. URL: http://ec.europa.eu/information_society/eeurope/2002/ news_library/ pdf_files/netsec_en.pdf (дата звернення: 17.11.2018).

375. Safer Internet Programme. URL: http://ec.europa.eu/ information_society/activities/sip/policy/programme/current_prog/index_en.htm (дата звернення: 17.11.2018).

376.

377. Communication from the Commission: Towards a general policy on the fight against cyber crime. COM (2007). URL:

http://eurlex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf (дата звернення: 17.11.2018).

378. Communication from the Commission on Critical Information Infrastructure Protection: Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. COM (2009)149. URL: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm (дата звернення: 17.11.2018).

379. Про доступ до інформації, яка знаходиться в розпорядженні державних органів: Рекомендації Ради Європи № R (81)19. URL: http://medialaw.org.ua/library/rekomendatsiya-r-81-19-pro-dostup-do-informatsiyi-shho-znahodytsya-u-rozporyadzhenni-derzhavnyh-organiv (дата звернення: 17.11.2018).

380. General Assembly Resolution «The right to privacy in the digital age», A/RES/68/167: URL: http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx (дата звернення: 17.11.2018).

381. Гнатюк С.Л. Особливості захисту персональних даних в сучасному кіберпросторі: правові та техніко-технологічні аспекти: Аналітична доповідь. К. : Нац. ін-т стратегічних досліджень, 2013. 51 с.

382. Размєтаєва Ю.С. Приватність в інформаційному суспільстві: проблеми правового розуміння та регулювання. Науковий вісник Ужгородського національного університету: серія «Право». Випуск 37, том 1. 2016. С.43-46.

383. Директива 95/46/ЄС Європейського Парламенту і Ради "Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних" від 24 жовтня 1995 року. URL: http://zakon2.rada.gov.ua/laws/show/994_242 (дата звернення: 17.11.2018).

384. Nigel Waters, Graham. Interpreting the Security Principle. URL: http://www.cyberlawcentre.org/ipp/wp/WP1%20Security.pdf (дата звернення: 17.11.2018).

385. Василенко Д.П., Маслак В.І. Законодавство провідних країн

світу в сфері захисту інформації. Вісник КДУ імені Михайла Остроградського. Випуск № 61, частина 1. Частина 1. С.128-132.

386. Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (Sicherheitsüberprüfungsgesetz – SÜG. URL: http://www. gesetze -im-internet.de/s_g/BJNR086700994.html (дата звернення: 17.11.2018).

387. Teleservices Data Protection Act. URL: http://ourworld.compuserve.com/homepages/ckuner/multimd (дата звернення: 25.11.2018).

388. Federal Act Governing Access to Information held by the Federal Government (Freedom of Information Act). URL: http://www.gesetze-im-internet.de/ifg/BJNR272200005.html (дата звернення: 25.11.2018).

389. Stasi Files Act (Stasi-Unterlagengesetz, StUG). URL: http://germanlawarchive.iuscomp.org/?p=714 (дата звернення: 25.11.2018).

390. Act on the Federal Office for Information Security (BSI Act - BSIG). URL: https://www.bsi.bund.de/DE/DasBSI/Gesetz/ gesetz.html (дата звернення: 25.11.2018).

391. Taking advantage of opportunities – avoiding risks. URL: https://www.bsi/bund.de//EN/Home/home_node.html$jsessionid= EA326461A185448F29C194C194C91BC85F23.2_cid286 (дата звернення: 25.11.2018).

392. Verfassungsschutz (Bfv).URL: http://www. verfassungsschutz.de(дата звернення: 25.11.2018).

393. Cyber-und Informationsraum: URL: http://cir. bundeswehr.de/portal/a/cir/start (дата звернення: 25.11.2018).

394. Politique de sécurité des systèmes d'information de l'état. Mode acces. URL: http://circulaire.legifrance.gouv.fr/pdf/2014/08/cir_38641.pdf (дата звернення: 25.11.2018).

395. Publication du décret n° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale. Mode

acces. URL: http://www.ssi.gouv.fr/actualite/publication-du-decret-n-2015-351-du-27-mars-2015-relatif-a-la-securite-des-systemes-dinformation-des-operateurs-dimportance-vitale (дата звернення: 30.11.2018).

396. Laura Chappell, Palgrave Macmillan. Germany, Poland and the Common Security and Defence Policy. Converging Security and Defence Perspectives in an Enlarged EU. 29 august 2012. 232 p.

397. Тихомирова Є.Б., Смик Р.П. Інформаційна політика Польщі. Матеріали V Всеукраїнської науково-практичної конференції «Сучасні проблеми гуманітаристики: світоглядні пошуки, комунікативні та педагогічні стратегії». Рівне, 2015. С.113-115

398. Across Europe? Nations Mold Cyber Defenses. URL: http:// archive.defensenews.com/article/20130709/DEFREG01/307090008/Across-Europr-Nations-Mold-Cyber-Defenses (дата звернення: 30.11.2018).

399. Countering cyberterrorism. URL: http://msz.gov.pl/ en/foreign_policy/security_policy/international_terrorism/countering_cyber_terrorism/&printMode=true (дата звернення: 30.11.2018).

400. Доктрина кибезбезопасности Польщи. URL: constitutions.ru/?p=11083 (дата звернення: 30.11.2018).

401. Польща створює Доктрину інформаційної безпеки. URL: http://www.eurointegration.com.ua/news/2015/07/26/7036321/ (дата звернення: 30.11.2018).

402. Biuro Bezpieczeństwa Narodowego. URL: en.bbn.gov.pl дата звернення: 30.11.2018).

403. У Польщі створили центр боротьби з російською пропагандою. URL:https://zaxid.net/u_polshhistvorili_tsentr_borotbi_z_rosiyskoyu_propagandoyu_n1424662 дата звернення: 30.11.2018).

404. Телеховський Ю.Г. Досвід трансформації спецслужб Угорщини: висновки для України. Стратегічні пріоритети. №3 (28). 2013 р. С.151-155.

405. Европарламент принял резолюцию с осуждением Венгрии.

URL: http://www.novayagazeta.ru/news/ 54209.html дата звернення: 30.11.2018).

406. Затинайко О., Павленко В., Бочарніков В., Свєшніков С. Політика безпеки і воєнно_політичні відносини Угорщини. Наука і оборона. № 1. 2014. С.9-18.

407. Баранов А.А., Брижко В.М., Базанов Ю.К. Права людини і захист персональних даних. URL: http:/library.khpg.org/files/docs/Kn_L_.pdf дата звернення: 30.11.2018).

408. Nemzeti Adatvédelmi és Információszabadság Hatóság (Hungarian National Authority for Data Protection and Freedom of Information): URL: http://www.naih.hu/uegyfelszolgalat,--kapcsolat.html (дата звернення: 30.11.2018).

409. Act on the Electronic Information Security of Central and Local Government Agencies): URL: http://njt.hu/cgi_bin/njt_doc.cgi?docid= 160206.240508 (дата звернення: 30.11.2018).

410. Hungary's National Security strategy (2012): URL: http://2010-2014.kormany.hu/download/4/32/b0000/National%20Security% 20Strategy.pdf

411. National Cyber Security Strategy of Hungary (2013): URL: http://www.nbf.hu/anyagok/Government%20Decision%20No% 201139_2013%20on%20the%20National%20Cyber%20Security%20Strategy% 20of%20Hungary.docx (дата звернення: 30.11.2018).

412. Information security act of the Republic of Croatia (2007): URL: http://www.uvns.hr/UserDocsImages/en/dokumenti/info-security/Information-Security-Act.pdf (дата звернення: 30.11.2018).

413. The national cyber security strategy of the republic. URL: http://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20 National%20Cyber%20Security%20Strategy%20(2015).pdf (дата звернення: 30.11.2018).

414. Хорватія повернула свої території за три дні, а інформаційна війна тривала ще 15 років. URL: http://milnavigator.com.ua

/%D1%85%D0%BE%D1%80%D0%B2%D0%B0%D1%82%D1%96%D1%8F-%D0%BF%D0%BE%D0%B2%D0%B5%D1%80%D0% (дата звернення: 30.11.2018).

415. Як бачать в ЄС війну на сході України // Український інститут досліджень екстремізму. URL: http://uire.org.ua/novyni/yak-bachat-v-yes-viynu-na-shodi-ukrayini/ (дата звернення: 30.11.2018).

416. Ukraine and Russia are both trapped by the war in Donbas. The Economist. URL: https://www.economist.com/europe/2017/05/25/ukraine-and-russia-are-both-trapped-by-the-war-in-donbas (дата звернення: 30.11.2018).

417. It's Counterintuitive, but Arming Ukraine Will Actually Save US Taxpayers Money MAY 25, 2017. The Atlantic Council. URL: http://www.atlanticcouncil.org/blogs/ukrainealert/it-s-counterintuitive-but-arming-ukraine-will-actually-save-us-taxpayers-money (дата звернення: 30.11.2018).

418. Пилипчук В.Г. Реформування і розвиток Служби безпеки в контексті євроінтеграції України: Науково-методичний посібник. К. : Нац. акад. СБУ, 2017. 260 с.

419. В Евросоюзе приняли новый закон о защите даннях. URL: https://threatpost.ru/v-evrosoyuze-prinyali-novyj-zakon-o-zashhite-dannyh/15749/ (дата звернення: 30.11.2018).

420. Персональные данные: новые правила в Европейском Союзе. URL: https://habrahabr.ru/post/300348/ (дата звернення: 30.11.2018).

421. Cyberintelligence. URL: https://www.sri.ro/ cyberintelligence-en.html. (дата звернення: 30.11.2018).

422. The Senate passed the draft low regarding the cyber security of Romania. URL: http://actmedia.ua/daily/the-senate-passed-the -draft-law-regarding-the ceber-security-of-romania/55734 (дата звернення: 30.11.2018).

423. Romania's Cyber Security Strategy and the National Action Plan on Implementation of the National Cyber Security (2013): [Online tool]. – Available at. URL: https://www.cert.ro/vezi/document/strategia-de-securitate-

cibernetica (дата звернення: 30.11.2018).

424. National Cyber Security Strategy: Cyber Resilient Bulgaria 2020 (2016 URL: https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/Cybersecurity%20Forum%20Bulgaria/Bulgaria_sharkov_todorov.pdf. (дата звернення: 30.11.2018).

425. Руснак А.К. Молдова и информационная безопасность. SECURITATEA INFORMATIONALĂ 2011: Conferinţa Internaţională, ediţia a VIII-a, 4 mai 2011. С.62-63.

426. Конвенція про кіберзлочинність від 23 листопада 2001 року. URL: http://zakon5.rada.gov.ua/laws/ show/994_575 (дата звернення: 08.12.2018).

427. Другий додатковий Протокол до Європейської Конвенції про взаємну допомогу у кримінальних справах від 08 листопада 2001 року. URL: http://zakon.rada.gov.ua/laws/show/994_518 (дата звернення: 08.12.2018).

428. Lege Nr. 20 din 03.02.2009 Privind prevenirea şi combaterea criminalităţii informatice. URL: http://lex.justice.md/viewdoc.php?action=view&view=doc&id=333508&lang=1 (дата звернення: 08.12.2018).

429. Факультативний протокол до Конвенції ООН про права дитини, що стосується торгівлі дітьми, дитячої проституції й порнографії від 01 січня 2000 року. URL: http://zakon3.rada.gov.ua/laws/show/995_b09.

430. Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства від 25 жовтня 2007 року. URL: http://zakon3.rada.gov.ua/laws/show/994_927 (дата звернення: 08.12.2018).

431. Lege Nr. 91 din 29.05.2014 Privind semnătura electronică şi documentul electronic. URL: http://lex.justice.md/viewdoc.php?action=view&view= doc&id=353612&lang=1 (дата звернення: 08.12.2018).

432. Директива 2006/24/ЕС Європейського парламенту та Ради Європи від 15 березня 2006 р. «Про збереження даних, створених або оброблених при наданні загальнодоступних послуг електронних

повідомлень або громадських мереж зв'язку, та внесення поправок в Директиву 2002/58/ЕС». URL: https://ain.ua/2009/10/27//директива-ес-о-сохранении-данных-укр. (дата звернення: 08.12.2018).

433. Директива N 2008/114/ЕС Європейского парламента и Совета Європы от 08 грудня 2008 року «О европейских критических инфраструктурах и мерах по их защите». URL: http://docs.pravo.ru/document/view/32671965/. (дата звернення: 08.12.2018).

434. HOTĂRÎRE Nr. 811 din 29.10.2015 Cu privire la Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020. URL: http://lex.justice.md/viewdoc.php?action=view&view=doc&id=361818&lang=1. (дата звернення: 08.12.2018).

435. Молдова: Национальный ИКТ-профайл (Информационная безопасность и защита информации). URL: https://digital.report/moldova-informatsionnaya-bezopasnost/ (дата звернення: 08.12.2018).

436. Мнения экспертов Молдовы: Законопроекты в области информационной безопасности противоречат друг другу, то есть ведут к злоупотреблениям. URL: http://www.allmoldova.com/ru/project/mnenie/mnieniia-ekspiertov-moldovy-zakonoproiekty-v-oblasti-informatsionnoi-biezopasnosti-protivoriechat-drugh-drughu-to-iest-viedut-k-zloupotrieblieniiam (дата звернення 26.09.2018).

437. Беларусь: Национальный ИКТ-профайл (Информационная безопасность и защита информации). URL: https://digital.report/belarus-informatsionnaya-bezopasnost/ (дата звернення: 08.12.2018).

438. Постановление Оперативно-аналитического центра при Президенте Республики Беларусь и Министерства связи и информатизации Республики Беларусь от 19 февраля 2015 года № 7/7 «О признании утратившим силу постановления Оперативно-аналитического центра при Президенте Республики Беларусь и Министерства связи и информатизации Республики Беларусь от 29 июня 2010 года № 4/11». URL: http://www.pravo.by/upload/docs/op/T21503058_1424811600.pdf (дата

звернення: 08.12.2018).

439. Указ Президента Республики Беларусь от 01 февраля 2010 года № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет»: URL: http://pravo.by/ document/?guid=3871&p0=P31000060. (дата звернення: 08.12.2018).

440. Закон Республики Беларусь от 15 июля 2015 года № 307-З «Об оперативно-розыскной деятельности»: URL: http://kgb.by/ru/zakon289-3/ (дата звернення: 08.12.2018).

441. Закон Республики Беларусь от 10 июля 2012 года № 390-З «Об органах государственной безопасности Республики Беларусь»: URL: http://kgb.by/ru/zakon390-3/. (дата звернення: 08.12.2018).

442. Указ Президента Республики Беларусь от 03 марта 2010 года № 129 «Об утверждении Положения о порядке взаимодействия операторов электросвязи с органами, осуществляющими оперативно-розыскную деятельность»: URL: http://oac.gov.by/ files/files/pravo/ukazi/Ukaz_129.htm. (дата звернення: 08.12.2018).

443. Концепция сотрудничества государств-участников Содружества Независимых Государств в борьбе с преступлениями, совершаемыми с использованием информационных технологий (утверждена Решением Совета глав государств СНГ от 25 октября 2013 года): URL: http://www.e-cis.info/page.php?id=23808 (дата звернення: 08.12.2018).

444. Страны СНГ будут сотрудничать в борьбе с киберпреступностью: URL: https://www.ritmeurasia.org/news--2017-08-28--strany-sng-budut-sotrudnichat-v-borbe-s-kiberprestupnostu-32043 (дата звернення: 08.12.2018).

445. Ткачук Т. Ю. Концептуальні засади функціонування конкурентної розвідки. Проблеми правового забезпечення реалізації функцій державного управління і місцевого самоврядування. Серія «Право». Т. 3. Вип. 3. Донецьк : ДонДУУ, 2010. С. 154–164

446. Ткачук Т. Ю. Інформація з обмеженим доступом на підприємстві: проблеми безпеки та захисту.Право України. 2011. № 3. С. 243–252.

447. Ткачук Т. Ю. Правові засади доступу громадян до публічної інформації у контексті законодавчих змін. Інформаційна безпека людини, суспільства, держави. 2011. № 2. С. 62–69.

448. Ткачук Т. Ю. Місце і роль конкурентної розвідки в стратегічному плануванні інформаційної безпеки підприємства. Інформаційна безпека людини, суспільства, держави. 2013. № 2. С. 47–54

449. Ткачук Т. Ю. Правова охорона службової інформації як елемент системи забезпечення інформаційної безпеки держави: досвід зарубіжних країн. Юрид. наук. електр. журнал. 2015. № 6 URL:http://www.lsej.org.ua/index.php/arkhiv-nomeriv?id=44 (дата звернення: 08.12.2015).

450. Ткачук Т. Ю., Яцко М.Г. Суспільно-економічні передумови створення недержавної системи безпеки в Україні. Молодий вчений. 2017. № 1 (41), січень С. 157–159.

451. Ткачук Т. Ю., Яцко М.Г. Стан інформаційної безпеки України та основні завдання недержавних суб'єктів по її забезпеченню. Інтернаука. 2017. № 1(1). С. 41–43.

452. Ткачук Т. Ю., Кравченко О.О. Яким має бути Закон «Про комерційну таємницю»? Вісник АПСВТ. 2017. № 2. С. 10–19

453. Ткачук Т. Ю. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. Підприємництво, господарство і право. 2017. № 10. С. 182–186.

454. Ткачук Т. Ю. Забезпечення інформаційної безпеки у країнах центральної Європи. Юридичний науковий електронний журнал. 2017 № 5. URL: http://lsej.org.ua/5_2017/30.pdf (дата звернення: 08.12.2018).

455. Ткачук Т. Ю. Забезпечення інформаційної безпеки: досвід окремих країн східної Європи. Інформація і право. 2017. № 4. С. 62–73.

456. Ткачук Т. Ю. Забезпечення інформаційної безпеки у країнах позаблокового статусу. Прикарпатський юрид. вісник. 2017. № 4. С. 61–65.

457. Ткачук Т. Ю. Інформаційна безпека держави у національному законодавстві європейських країн. Visegrad Journal on Human Rights. 2018. № 1. С. 145–150

458. Ткачук Т. Ю. Политика информационной безопасности НАТО. Legea si Viata. 2018. № 5. С. 187–191

459. Ткачук Т. Ю. Законодавчі підходи до кібербезпеки в окремих країнах світу. Сучасні правові системи світу: тенденції та фактори розвитку : мат. міжнарод. наук.-практ. конф. (Запоріжжя, 25–26.08.17). С. 84–86

460. Ткачук Т. Ю. Кібербезпека: підходи до визначення в окремих країнах. Кібербезпека в Україні: правові та організаційні питання : мат. всеукр. наук.-практ. конф. (Одеса, 17.11.17). ОДУВС, 2017. С. 54–55

461. Конвенція Ради Європи "Про доступ до офіційних документів". URL: http://zakon3.rada.gov.ua/laws/show/994_a33 (дата звернення: 08.12.2018).

462. Програма «Шлях Європи до Інформаційного Суспільства. План Дій» (Europe’s Way to the Information Society. An Action Plan)" URL: http://i.lekciya.com.ua/doc/3177/index.html?page=17; Europe’s Way to the Information Society. An Action Plan: URL: https://publications.europa.eu/en/publication-detail/-/publication/deed9eb9-0b6e-11e4-a7d0-01aa75ed71a1/language-en (дата звернення: 08.12.2018).

463. eEurope - An information society for all. URL: https://ec.europa.eu/digital- single-market/en/news/eeurope-information-society-all (дата звернення: 08.12.2018).

464. Йерсилд против Дании: Постановление суда от 23 сентября 1994 г. URL: https://webcache.googleusercontent.com/search?q=cache:xo62wY4WawQJ:https://hudoc.echr.coe.int/app/conversion/pdf%3Flibrary%3DECHR%26id%3D001-

93929%26filename%3DCASE%2520OF%2520JERSILD%2520v.%2520DENMARK%2520-%2520%255BRussian%2520Translation%255D.pdf+&cd=1&hl=uk&ct=clnk&gl=ua (дата звернення: 08.12.2018).

465. Ярема О.Г. Предмет правового забезпечення інформаційної безпеки в інформаційному праві. Науковий вісникЛьвівського державного університету внутрішніх справ. Серія Право. №2. 2016. С. 244-252

466. Тополевський Р., Захаров Є. Коментарі до проекту Закону України «Про інформаційну безпеку України» (№5732 від 22 вересня 2004 р.). URL: http://khpg.org/index.php?id=1105737155 (дата звернення: 08.12.2018).

467. Закону України «Про Національну програму інформатизації» від 04 лютого 1998 року. URL: http://zakon0.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80 (дата звернення: 08.12.2018).

468. Проект Закону України «Про засади інформаційної безпеки України» (реєстр. № 4949 від 28 травня 2014 року). URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=51123 (дата звернення: 08.12.2018).

469. Конвенція про кіберзлочинність. URL: http://zakon0.rada.gov.ua /laws/show/994_575 (дата звернення: 08.12.2018).

470. Закон України "Про боротьбу з тероризмом" від 20 березня 2003 року. URL: http://zakon5.rada.gov.ua/laws/show/638-15 (дата звернення: 08.12.2018).

471. Закон України "Про центральні органи виконавчої влади" від 17 березня 2011 року. URL: http://zakon3.rada.gov.ua/laws/show/3166-17 (дата звернення: 08.12.2018).

472. Закон України "Про запобігання корупції" від 14 жовтня 2014 року. URL: http://zakon5.rada.gov.ua/laws/show/1700-18 (дата звернення: 08.12.2018).

473. Рішення РНБО України "Про заходи щодо вдосконалення

формування та реалізації державної політики у сфері інформаційної безпеки України" (введено в дію Указом Президента України № 449/2014 від 1 травня 2014 року). URL: http://zakon2.rada.gov.ua/laws/show/449/2014 (дата звернення: 08.12.2018).

474. Закон України "Про внесення змін до Кримінального та Кримінально-процесуального кодексів України" від 23 грудня 2004 року. URL: http://zakon0.rada.gov.ua /laws/ show/2289-iv (дата звернення: 08.12.2018).

475. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах" від 5 липня 1994 року. URL: http://zakon3.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 (дата звернення: 08.12.2018).

476. Закон України "Про інформацію" від 02 жовтня 1992 року (в редакції від 01 січня 2017 року). URL: http://zakon5.rada.gov.ua/laws/show/2657-1 (дата звернення: 08.12.2018).

477. Закон України "Про науково-технічну інформацію" від 25 червня 1993 року. URL: http://zakon5.rada.gov.ua/laws/show/3322-12 (дата звернення: 08.12.2018).

478. Закон України "Про телекомунікації" від 18 листопада 2003 року. URL: http://zakon2.rada.gov.ua/laws/show/1280-15 (дата звернення: 08.12.2018).

479. Закон України "Про доступ до публічної інформації" від 13 січня 2011 року. URL: http://zakon2.rada.gov.ua/laws/show/2939-17 (дата звернення: 08.12.2018).

480. Закон України "Про боротьбу з тероризмом" від 20 березня 2003 року. URL: http://zakon5.rada.gov.ua/laws/show/638-15 (дата звернення: 08.12.2018).

481. Закон України «Про Регламент Верховної Ради України» від 10 лютого 2010 року. URL: zakon.rada.gov.ua/go/1861-17 (дата звернення: 08.12.2018).

482. Рудольф фон Иеринг. Юридическая техника / Сост. А.В. Поляков. М.: Статут, 2008. 231 с.

483. Палата представників Конгресу США підтримала законопроект з $250 млн для оборони України. URL: https://www.pravda.com.ua/news/2018/05/25/7181305/ (дата звернення: 08.12.2018).

484. Рудь І. Закон про кібербезпеку: основні положення, оцінки експертів та розвиток вітчизняного інформаційного простору. Україна: події, факти, коментарі. 2017. № 19. С. 42–48. Режим доступу: http://nbuviap.gov.ua/images/ukraine/2017/ukr19.pdf (дата звернення: 08.12.2018).

485. Коментар до проекту Доктрини інформаційної безпеки України. URL: http://www.rainbow.gov.ua/news/942.html (дата звернення: 08.12.2018).

486. Ситник Г.П. Державне управління у сфері забезпечення національної безпеки України: теорія і практика : Автореф. дис... д-ра наук з держ. управління: 25.00.01. Нац. акад. держ. упр. при Президентові України. К., 2004. 36 с.

487. Кузьменко А. Проблеми відповідності стратегії та системи забезпечення безпеки України національним потребам. Юридичний Журнал. 2006 р. №10. URL: http://www.justinian.com.ua/article.php?id=2432

488. Про державне прогнозування та розроблення програм економічного і соціального розвитку України: Закон України № 1602-III від 23.03.2000 р. URL: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1602-14&new=1 (дата звернення: 08.12.2018).

489. Про схвалення Концепції вдосконалення системи прогнозних і програмних документів з питань соціально-економічного розвитку України: Розпорядження Кабінету міністрів України № 504-р від 4.10.2006 р. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=504-2006-%F0 (дата звернення: 08.12.2018).

490. Концепція Державної програми економічного і соціального розвитку України на 2012 рік : Розпорядження Кабінету міністрів України № 219-р від 21.03.2011 р. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=219-2011-%F0 (дата звернення: 08.12.2018).

491. Прогнозирование, стратегическое планирование и национальное программирование: Учабник / Б.Н.Кузык, В.И.Кушлин, Ю.В.Яковец. 4-е изд., перераб. и доп. Москва: Экономика, 2011. 604 с.

492. Проект Закону України «Про державне стратегічне планування» (реєстр. № проекту 9407 від 03 листопада 2011 року): URL: http://w1.c1.rada.gov.ua/pls/zweb2/ webproc4_2?%20pf3516=9407&skl=7 (дата звернення: 08.12.2018).

493. Проект Закону України «Про державне стратегічне планування». URL: me.gov.ua http://me.gov.ua/Documents/Detail?lang=uk-UA&isSpecial=True&id=e7b8af7a-7c03-4d5b-aaa5-e1c0d7e84388&title=ProektZakonuUkrainiproDerzhavneStrategichnePlanuvannia (дата звернення: 08.12.2018).

494. Проект Закону України «Про національну безпеку України» № 8068 від 28 лютого 2018 року: URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=63531 (дата звернення: 08.12.2018).

495. Структура керівних документів державної політики в інформаційній сфері: нагальні проблеми та шляхи впорядкування: URL: http://www.niss.gov.ua/articles/572/ (дата звернення: 08.12.2018).

496. Шерстюк В. П. МГУ: научные исследования в области информационной безопасности. Информационное общество. 2005. № 1. С. 48-53

497. Лісовська Ю.П. Державна політика забезпечення інформаційної безпеки України: адміністративно-правовий аспект. Молодий вчений. 2015, № 2 (17). С.177-179

498. Сайфутдинова Л.Х. Информационная политика государства в

сфере межєтнических отношений (на примере республики Татарстан). Власть. 2014. № 5. С.44-48.

499. Champagne P. 1993. La vision médiatique. La misère du monde. Paris: Le Seuil. P. 72-74

500. Попов В.Д. Информационная политика. М.: Изд-во РАГС, 2003. 463 с.

501. Нисневич Ю.А. О необходимости государственной информационной политики. Межотраслевая информационная служба. 1997. № 1-2. С. 7-10.

502. Манойло А.В. Государственная информационная политика в особых условиях. М: МИФИ, 2003. 388 с.

503. Інформаційна політика: [навчальний посібник] Г.Почепцов, С.Чукут. К.: Знання, 2008. 663 с.

504. Бондаренко С.В. Государственная информационная политика России и Украины в контексте национальной безопасности: основы и принципы формирования. Youth World Politic. 2013. №4. С.112-118.

505. Шаповал Р.В., Клочко В.О. Вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України. Наше право. 2014. № 6. С.5-9

506. Данільян О.Г. Національна безпека України: сутність, структура та напрями реалізації. Навчальний посібник. Х: Фоліо, 2002. 285 с.

507. Жарков Я.М. Інформаційна безпека особистості, суспільства, держави: [підручник]. Видавничо-поліграфічний цента «Київський університет», 2008. 256 с.

508. Олійник О.В. Інформаційна безпека України: доктрина адміністративно-правового регулювання: дис ... д-ра юрид. наук: 12.00.07. Київ, 2013. 203 с.

509. Тарасенко Н. Доктрина інформаційної безпеки України в оцінках експертів. URL:

http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2760:doktrina-informatsijnoji-bezpeki-yak-zasib-protidiji-informatsijnim-zagrozam-2&catid=63&Itemid=393 (дата звернення: 08.12.2018).

510. Всіх перевірять: Рада підтримала новий захист від РФ. URL: http://ua.korrespondent.net/ukraine/3820536-vsikh-pereviriat-vlada-prydumala-novyi-zakhyst-vid-rf (дата звернення: 08.12.2018).

511. Доктрина інформаційної безпеки. URL: http://hromadske.ua/posts/doktrina-informaciinoi-bezpeki

512. Доктрина информационной безопасности Украины: медиаэксперт указала на недостатки документа. URL: http://apostrophe.ua/ua/news/society/media/2017-02-28/doktrina-informacionnoj-bezopasnosti-ukrainy-mediaekspert-ukazala-na-nedostatki-dokumenta/88336 (дата звернення: 08.12.2018).

513. Доктрину информационной безопасности Украины назвали дубинкой, которой будут бить по несогласным. URL: http://apostrophe.ua/ua/news/society/2017-03-01/doktrinu-informatsionnoy-bezopasnosti-ukrainyi-nazvali-dubinkoy-kotoroy-budut-bit-po-neugodnyim/88394 (дата звернення: 08.12.2018).

514. Борьба с неугодными или с Россией: что стоит за доктриной информационной безопасности. URL: http://apostrophe.ua/ua/article/society/2017-02-28/borba-s-neugodnyimi-ili-s-rossiey-chto-stoit-za-doktrinoy-informatsionnoy-bezopasnosti/10590 (дата звернення: 08.12.2018).

515. Про відхилення проекту Закону України про Концепцію державної інформаційної політики : Постанова Верховної Ради України від 5.07.2011 р. № 3590-VI. URL: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi

516. Нестеренко О. Чи потрібний такий закон про Концепцію державної інформаційної політики? URL: http://www.khpg.org/index.php?id=1256021138 (дата звернення: 08.12.2018).

517. Рішення Конституційного Суду України у справі щодо порядку

голосування та повторного розгляду законів Верховною Радою України від 7 липня 1998 року. URL: https://www.google.com.ua/?gws_rd=ssl (дата звернення: 08.12.2018).

518. Рішення Конституційного суду рішенні від 30 травня 2001 року за № 7-рп/2001 року. URL: http://zakon3.rada.gov.ua/laws/show/v007p710-01 (дата звернення: 08.12.2018).

519. Структура керівних документів державної політики в інформаційній сфері: нагальні проблеми та шляхи впорядкування. URL: http://www.niss.gov.ua/articles/572/ (дата звернення: 08.12.2018).

520. Руденко Ю.Ю. Плюралізм в Україні як складова інформаційної політики у контексті забезпечення національної безпеки. Актуальні проблеми управління інформаційною безпекою держави: зб. матер. наук.-практ. конф. К. : Наук-вид. відділ НА СБ України, 2012. С.96-97

521. Касаткин В.П., Варфоломеев М.А. К вопросу о государственной политике в сфере обеспечения информационной безопасности. Вестник БУПК. 2006. № 4. С. 399-401.

522. Токсоналиева Р.М. Государственная политика Кыргызской республики в сфере информационно-психологической безопасности. Вестник КРСУ. 2015. Том 15. № 5. С.35-38.

523. Комиссаров С.С. Информационная политика государства: трансформация в условиях модернизации общества/ С.Комиссаров. Вестник МГУКИ. 2011. № 2 (40). С.40-42.

524. Мастяниця Й.У. Інформаційні ресурси України: проблеми державного управління: [монографія]. К.: НІСД. 2002. 141 с.

525. Донбас і Крим: ціна повернення : монографія / за заг. ред. В. П. Горбуліна, О. С. Власюка, Е. М. Лібанової, О. М. Ляшенко. К. : НІСД, 2015. 74 с.

526. Боднар І.Р. Державна політика та інформаційна безпека України: післякризові виклики. Актуальні проблеми післякризового відновлення економіки України: зб. матер. наук.-практ. конф. Львів. 2013.

С.29-32

527. Олійник О. В. Державна політика інформаційної безпеки України. Юридичний вісник. 2012. №4(25). С.65-69

528. Ткачук Т. Ю. Державна політика у сфері забезпечення інформаційної безпеки на сучасному етапі. Наук. вісник УжНУ. Серія «Право». 2017. № 46. Т. 2. С. 39–43

529. Ткачук Т. Ю. Пріоритетні напрями державної політики забезпечення інформаційної безпеки на сучасному етапі державотворення. Науковий вісник ХДУ. Серія «Юридичні науки» №4. С. 23-28

530. Ткачук Т. Ю. Захист національних інформаційних ресурсів як пріоритетна складова інформаційної політики держави в умовах глобалізації. Розвиток України в 21 ст.: економічні, соціальні, екологічні, гуманітарні та правові проблеми: мат. міжнарод. наук.-практ. конф. (Тернопіль, 30.03.12). С. 209–212

531. Ткачук Т. Ю. Україна як форпост європейської безпеки. Zbornik prispevkov z medzinarodnej vedeckej konferencie “Pravna veda a prax: vyzvy modfrnych europskych integracnych procesov”. (Bratislava, 27–28.11.15). С. 242–245

532. Ткачук Т. Ю. Теоретико-правове осмислення інформаційної безпеки держави у контексті розвитку інформаційного суспільства. Теоретико-правові основи формування та розвитку інформаційного суспільства : мат. наук.-практ. конф. (Київ, 29.11.17). 2017. С. 111–114

533. Ткачук Т. Ю. Інформаційний чинник у гібридній війні. Кібербезпека у системі нац. безпеки України: пріоритетні напрями розвитку : мат. наук. круглого столу (Маріуполь, 26.04.18). МДУ, 2018. С. 39–42

ДОДАТКИ

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

В яких опубліковані основні наукові результати дисертації:

Монографія:

1. Ткачук Т. Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір: *моногр*. К. : ВД «АртЕк», 2018. 422 с.

Глави і розділи у підручниках:

2. Менеджмент інформаційної безпеки: підруч. : у 2 ч. / А. К. Гринь, О. Д. Довгань, В. І. Журавель, С. О. Князєв, Є. Д. Скулиш, О. М. Солодка, Т. Ю. Ткачук; за заг. ред. Є. Д. Скулиша. К. : НА СБУ, 2013. Ч. 2. 604 с. с. 43-132; с. 181-272

Глави і розділи у посібниках:

3. Ткачук Т. Ю. Конкурентна розвідка : *навч. посіб*. К. : НА СБУ, 2010. 240 с.
4. Довгань О. Д., Журавель В. І., Ткачук Т. Ю. Організаційно-правові основи охорони комерційної таємниці: *навч. посібн*. К. : НА СБУ, 2012. с. 137-277
5. Довгань О. Д., Журавель В. І., Ткачук Т. Ю. Протидія промисловому шпигунству: навч. посібн. К. : НА СБУ, 2015. с. 83-101, с. 121-198.
6. Організаційно-правові заходи захисту службової інформації : навч. посібник / І. П. Касперський, С. О. Князєв, О. І. Матяш, Т. Ю. Ткачук К. : НА СБУ, 2017. с. 14-36.
7. Кадрова політика у сфері інформаційної безпеки : *навч. посіб*. / Гуз А.М., Мамченко С.М., Ткачук Т.Ю. та ін. / Київ : Нац. акад. СБУ, 2017. с. 86-207.
8. Організація захисту інформації з обмеженим доступом : *навч. посібн.* / А. М. Гуз, І. П. Касперський, Т. Ю. Ткачук. К. : НА СБУ, 2018. с.

33-58.

Статті в наукових фахових виданнях України з юридичних наук, у т. ч. тих, які зареєстровані у міжнародних наукометричних базах:

9. Ткачук Т. Ю. Напрями імплементації міжнародних стандартів захисту персональних даних у законодавство України. *Митна справа.* 2010. № 5. Ч. 2. С. 3–9.

10. Ткачук Т. Ю. Інформація з обмеженим доступом на підприємстві: проблеми безпеки та захисту. *Право України*. 2011. № 3. С. 243–252.

11. Ткачук Т. Ю. Правові засади доступу громадян до публічної інформації у контексті законодавчих змін. *Інформаційна безпека людини, суспільства, держави.* 2011. № 2. С. 62–69.

12. Ткачук Т. Ю. Принципи забезпечення інформаційної безпеки держави: інформаційний аспект. *Митна справа*. 2012. № 1. Ч. 2. С. 399–405.

13. Ткачук Т. Ю. Принципи та провідні завдання взаємодії органів державної влади та суб'єктів господарювання у сфері забезпечення національної інформаційної безпеки. *Наше право*. 2012. № 1. Ч. 1. С. 141–148.

14. Ткачук Т. Ю. Місце і роль конкурентної розвідки в стратегічному плануванні інформаційної безпеки підприємства. *Інформаційна безпека людини, суспільства, держави*. 2013. № 2. С. 47–54.

15. Ткачук Т. Ю., Журавель В.І. Ризик-діяльність у сфері захисту інформації з обмеженим доступом. *Інформаційна безпека людини, суспільства, держави.* 2014. № 2. С. 86–95.

16. Ткачук Т. Ю. Правова охорона службової інформації як елемент системи забезпечення інформаційної безпеки держави: досвід зарубіжних країн. *Юрид. наук. електр. журнал*. 2015. № 6 URL:http://www.lsej.org.ua/index.php/arkhiv-nomeriv?id=44

17. Ткачук Т. Ю., Журавель В. І. Соціальна складова менеджменту у системі захисту інформації з обмеженим доступом. *Інформ. безпека людини, суспільства, держави.* 2015. № 3 (19). С. 93–102.

18. Ткачук Т. Ю. Інформаційна безпека держави в онтологічному вимірі. *Порівняльно-аналітичне право.* 2015. №4. С. 284–287.

19. Ткачук Т. Ю., Яцко М.Г. Стан інформаційної безпеки України та основні завдання недержавних суб'єктів по її забезпеченню. *Інтернаука*. 2017. № 1(1). С. 41–43.

20. Ткачук Т. Ю. Інформаційна безпека: сучасні підходи до визначення категорії. *Актуальні питання публічного та приватного права*. 2017. № 2 (16). С. 45–54.

21. Ткачук Т. Ю. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. *Підприємництво, господарство і право.* 2017. № 10. С. 182–186.

22. Ткачук Т. Ю. Державна політика у сфері забезпечення інформаційної безпеки на сучасному етапі. *Наук. вісник УжНУ. Серія «Право».* 2017. № 46. Т. 2. С. 39–43.

23. Ткачук Т. Ю. Забезпечення інформаційної безпеки у країнах центральної Європи. *Юридичний науковий електронний журнал*. 2017 № 5. URL: http://lsej.org.ua/5_2017/30.pdf

24. Ткачук Т. Ю. Забезпечення інформаційної безпеки: досвід окремих країн східної Європи. *Інформація і право*. 2017. № 4. С. 62–73.

25. Ткачук Т. Ю. Забезпечення інформаційної безпеки у країнах позаблокового статусу. *Прикарпатський юрид. вісник*. 2017. № 4. С. 61–65.

26. Ткачук Т. Ю. Механізми протидії інформаційним загрозам зовнішніх джерел. *Вісник НТУ України «Київський політехнічний інститут». Політологія. Соціологія. Право.* 2017. № 1–2. С. 242–246.

27. Ткачук Т. Ю., Довгань О.Д. Система інформаційної безпеки України: онтологічні виміри. *Інформація і право.* 2018. № 1 (24). С. 89–104.

28. Ткачук Т. Ю., Довгань О.Д. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс. *Інформація і право.* 2018. № 2 (25). С. 73–85.

29. Ткачук Т. Ю. Пріоритетні напрями державної політики забезпечення інформаційної безпеки на сучасному етапі державотворення. *Науковий вісник ХДУ. Серія «Юридичні науки».* 2018. №4. С. 32-36

30. Ткачук Т. Ю., Довгань О.Д. Наукова рефлексія інформаційної безпеки України: від позитивізму до метафізики права. *Інформація і право*. 2018. № 4 (24). С. 79–89.

Статті в наукових періодичних виданнях із юридичних наук інших держав:

31. Ткачук Т. Ю. Складові інформаційної безпеки: аналіз критеріїв. *Visegrad Journal on Human Rights*. 2017. № 4. С. 153–158.

32. Ткачук Т. Ю. Суб'єкти забезпечення інформаційної безпеки держави: функціональний аналіз. *Jurnalul juridic national: teorie şi practică.* 2017. № 6. С. 42–46.

33. Ткачук Т. Ю. Інформаційна безпека держави у національному законодавстві європейських країн. *Visegrad Journal on Human Rights*. 2018. № 1. С. 145–150.

34. Ткачук Т. Ю. Теоретичний дискурс пошуку основних складових системи інформаційної безпеки держави. *Jurnalul juridic national: teorie şi practică.* 2018. № 2. С. 45–47.

35. Ткачук Т. Ю. Политика информационной безопасности НАТО. *Legea si Viata.* 2018. № 5. С. 187–191.

Які засвідчують апробацію матеріалів дисертації:

36. Ткачук Т. Ю. Інформаційна безпека суб'єктів господарювання як складова частина системи державного безпеко творення. *Актуальні проблеми забезпечення інформ. безпеки держави : мат. наук.-практ. конф.*

(Київ, 20.03.09). : НА СБУ. С. 166–168.

37. Ткачук Т. Ю. Проблемні аспекти правового регулювання захисту персональних даних у процесі контррозвідувальної та оперативно-розшукової діяльності. *Актуальні проблеми управління інформ. безпекою держави : мат. наук.-практ. конф. (Київ, 17.03.10): НА СБУ*, 2010. С. 103–106.

38. Ткачук Т. Ю. Правові та організаційні засади взаємодії правоохоронних органів та приватних структур у сфері забезпечення інформаційної безпеки держави: досвід окремих країн. *Актуальні питання взаємодії інститутів громадянського суспільства та органів публічного адміністрування у напрямку розвитку правової системи України : мат. міжнарод. наук.-практ. конф. (Київ, 11–12.09.15)* : Центр правових наукових досліджень, 2015. С. 83–87.

39. Ткачук Т. Ю. Обґрунтування потреби наукової розробки теоретико-правових засад комплексного захисту інформації з обмеженим доступом. *Актуальні проблеми управління інформаційною безпекою держави: НА СБУ (Київ, 19.03.15).* С. 368–371.

40. Ткачук Т. Ю. Дозвільні засоби забезпечення інформаційної безпеки держави. *Політико-правові реформи та становлення громадянського суспільства в Україні : мат. всеукр. наук.-практ. конф. (Херсон, 09–10.10.2015).* 2015. С. 129–132.

41. Ткачук Т. Ю. Захист національних інформаційних ресурсів як пріоритетна складова інформаційної політики держави в умовах глобалізації. *Розвиток України в 21 ст. : економічні, соціальні, екологічні, гуманітарні та правові проблеми : мат. міжнарод. наук.-практ. конф. (Тернопіль, 30.03.12).* С. 209–212.

42. Ткачук Т. Ю. Охорона службової інформації в контексті забезпечення інформаційної безпеки держави. *Актуальні проблеми управління інформ. безпекою держави: мат. (Київ, 20.03.14).* Ч.2. К. : НА СБУ, 2014. С. 69–74.

43. Ткачук Т. Ю. Україна як форпост європейської безпеки. *Zbornik prispevkov z medzinarodnej vedeckej konferencie "Pravna veda a prax: vyzvy modfrnych europskych integracnych procesov". (Bratislava, 27–28.11.15).* С. 242–245.

44. Ткачук Т. Ю. Витоки гібридної війни та сучасні її технології. Пріоритетні напрями наукових досліджень: *Мат. II Міжнарод. наук.-практ. конф. (Київ, 15–16.08.17):* МЦНД, 2017. С. 79–81.

45. Ткачук Т. Ю. Законодавчі підходи до кібербезпеки в окремих країнах світу. *Сучасні правові системи світу: тенденції та фактори розвитку : мат. міжнарод. наук.-практ. конф. (Запоріжжя, 25–26.08.17).* С. 84–86.

46. Ткачук Т. Ю. Кібербезпека: підходи до визначення в окремих країнах. *Актуальні проблеми управління інформ. безпекою держави : мат. наук.-практ. конф. (Київ, 24.05.17).* 2017. С. 142–144.

47. Ткачук Т. Ю. Інформаційна безпека держави як пріоритетна складова національної безпеки. *Верховенство права та правова держава : мат. міжн. наук.-практ. конф. (Ужгород, 15–16.09.17).* 2017. С. 142–145.

48. Ткачук Т. Ю. Тіньовий інтернет: співвідношення можливостей і загроз. *Інтернет речей: проблеми правового регулювання та впровадження : мат. першої наук.-практ. конф. (Київ, 24.10.17).* С. 100–103.

49. Ткачук Т. Ю. Кібербезпека: підходи до визначення в окремих країнах. *Кібербезпека в Україні: правові та організаційні питання : мат. всеукр. наук.-практ. конф. (Одеса, 17.11.17).* ОДУВС, 2017. С. 54–55.

50. Ткачук Т. Ю. Теоретико-правове осмислення інформаційної безпеки держави у контексті розвитку інформаційного суспільства. *Теоретико-правові основи формування та розвитку інформаційного суспільства : мат. наук.-практ. конф. (Київ, 29.11.17).* 2017. С. 111–114.

54. Ткачук Т. Ю. Протидія кіберзагрозам у країнах позаблокового статусу. Освіта і наука у сфері нац. безпеки: проблеми та пріоритети

розвитку : *мат. міжнарод. наук.-практ. конф. (Острог, 01.12.17).* С. 66–70.

51. Ткачук Т. Ю. Інформаційна безпека держави як пріоритетна складова національної безпеки. *Science, research, development state and law. #2 (London, 27.02.18).* С. 39–43.

52. Ткачук Т. Ю. Аксіологічні складові об'єкта правового забезпечення інформаційної безпеки України. *Сучасна юриспруденція Європейського Союзу: взаємодія права, нормотворчості та практики : мат. міжнарод. наук.-практ. конф. (Люблін, 17.04.18).* 2018. С. 83–86.

53. Ткачук Т. Ю. Інформаційний чинник у гібридній війні. Кібербезпека у системі нац. безпеки України: пріоритетні напрями розвитку : *мат. наук. круглого столу (Маріуполь, 26.04.18).* МДУ, 2018. С. 39–42.

55. Ткачук Т. Ю. Аксіологічні константи інформаційної без пеки держави. *Актуальні проблеми управління інформац. безпекою держави : мат. всеукр. наук.-практ. конф. (Київ, 30.03.18).* НА СБУ, 2018. С. 167–169.

56. Ткачук Т. Ю. Україна як форпост європейської безпеки: аналіз інформаційної сфери. Україна та нац. інтереси в глобаліз. світі: візія націоналістів : *мат. п'ятих Бандерівських читань (Київ, 09.02.18).* 2018. С. 394–404.

57. Ткачук Т. Ю. Взаємозв'язок національних цінностей, інтересів та цілей у концепції правового забезпечення інформаційної безпеки держави. *Права, свободи і безпека людини в інформаційній сфері : мат. наук.-практ. конф. (Київ, 10.05.18).* 2018. С. 47–50.

58. Ткачук Т.Ю. Інформаційна безпеки у системі національної безпеки держави. *Освіта і наука у сфері національної безпеки: проблеми та пріоритети розвитку : збірник наукових праць за матеріалами Міжнародної науково-практичної конференції (8 червня 2018 р., м. Острог).* Острог: Видавництво Національного університету «Острозька

академія», 2018. С. 138-140.

Публікації, які додатково відображують результати дисертаційного дослідження:

59. Ткачук Т. Ю. Концептуальні засади функціонування конкурентної розвідки. *Проблеми правового забезпечення реалізації функцій державного управління і місцевого самоврядування. Серія «Право». Т. 3. Вип. 3*. Донецьк : ДонДУУ, 2010. С. 154–164.

60. Ткачук Т. Ю. Інформаційна функція грошей. Розвиток гуманітарних наук. *Проблеми і перспективи : мат. міжнарод. наук.-практ. конф. (Катовіце, 28.09-30.09.12)*. С. 69–72.

61. Ткачук Т. Ю., Журавель В. І. Організаційне проектування у системі захисту конфіденційної інформації суб'єктів господарювання. *Інформаційна безпека людини, суспільства, держави.* 2014. № 1. С. 76–84.

62. Ткачук Т. Ю. Конкурентна розвідка: *моногр.* Коломия : ПАТ «Коломийська друкарня ім. Шухевича», 2015. 296 с.

63. Ткачук Т. Ю., Яцко М.Г. Суспільно-економічні передумови створення недержавної системи безпеки в Україні. *Молодий вчений.* 2017. № 1 (41), січень С. 157–159.

64. Ткачук Т. Ю., Кравченко О.О. Яким має бути Закон «Про комерційну таємницю»? *Вісник* АПСВТ. 2017. № 2. С. 10–19.

Додаток Б

Проект

З А К О Н У К Р А Ї Н И

Про інформаційну безпеку України

Цей Закон відповідно до статей 1, 3, 16, 17, 18 і 92 Конституції України визначає основи та принципи інформаційної безпеки, цілі та засади державної політики у сфері забезпечення інформаційної безпеки в умовах зовнішніх, внутрішніх та системних загроз, гарантування безпеки особи, суспільства та держави в інформаційному просторі України.

Розділ І

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

Наведені в цьому Законі терміни вживаються в такому значенні:

безпека інформації – стан захищеності інформації від несанкціонованого доступу до неї, від порушень функціонування програмно-технічних засобів пошуку, збирання, оброблення, накопичення, збереження й передання інформації, виведення цих засобів із ладу, який забезпечується сукупність заходів і засобів захисту інформації;

безпека від інформаційних впливів – безпека суб‘єктів інформаційних процесів та соціальних зв‘язків між ними від інформаційних впливів, що здатні викликати знищення або пошкодження, спотворення інформації, об’єктів інформаційної інфраструктури, інших об‘єктів, зокрема нематеріального характеру, а також інформаційно-психологічна безпека;

виклики інформаційній безпеці - фактори, що не становлять безпосередньої загрози об’єктам інформаційної безпеки, але за відсутності реагування здатні негативно впливати на рівень інформаційної безпеки;

життєво важливі інтереси людини, суспільства й держави в інформаційній сфері – сукупність потреб людини, суспільства й держави в інформаційній сфері, задоволення яких забезпечує їх надійне існування й можливості сталого інформаційного розвитку;

забезпечення інформаційної безпеки – постійний процес діяльності компетентних органів, направлений на попередження, протидію загрозам інформаційній сфері, а також застосування активних заходів інформаційного впливу та сукупність умов такої діяльності, які реалізуються й здатні контролюватися тривалий час;

загрози інформаційній безпеці – фактори, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити досягнення національних цілей, реалізацію національних інтересів та збереження національних цінностей України в інформаційній сфері;

інформаційна безпека - стан, за якого в умовах дії реальних та потенційних загроз забезпечується самозбереження, сталий і прогресивний розвиток інформаційної сфери, зокрема захищеність інформаційної інфраструктури, інформаційного простору, інформаційних ресурсів, інформаційних процесів та їх суб’єктів, а також досягнення відповідних національних цілей та реалізація національних інтересів в інформаційній сфері;

інформаційна інфраструктура - середовище, яке забезпечує можливість здійснення інформаційних процесів, утворюючись сукупністю: систем формування та забезпечення безпеки інформаційних ресурсів, інформаційно-телекомунікаційних систем, мереж зв‘язку, а також систем забезпечення доступу до них; індустрії засобів інформатизації, телекомунікації і зв‘язку; індустрії інформаційних послуг та інформаційного ринку; систем підготовки та перепідготовки кадрів, проведення наукових досліджень;

інформаційна сфера – сфера життєдіяльності суспільства, яка утворюється сукупністю: суб‘єктів інформаційних процесів; інформації,

призначеної для використання суб‘єктами інформаційної сфери; інформаційної інфраструктури; суспільних відносин, що складаються у зв‘язку з формуванням, зберіганням, передачею та розповсюдженням інформації;

інформаційний екстремізм – протиправна діяльність, спрямована на створення, передання чи розповсюдження інформації, яка безпосередньо пов’язана з пропагандою та/або закликом до здійснення екстремістської діяльності, або на підрив інформаційної безпеки людини, суспільства і держави;

інформаційний вплив – цілеспрямована передача інформації суб’єктам інформаційних процесів або інформаційним системам, що ними використовуються, з метою зміни їх свідомості, поведінки чи порядку функціонування;

інформаційно-психологічний вплив – дія, спрямована на людину чи групу людей, яка вчиняється з використанням спеціальних методів і засобів впливу на психіку;

інформаційно-психологічна безпека – стан захищеності життєво важливих інтересів людини, суспільства й держави від інформаційних (інформаційно-психологічних впливів), що призводять до шкідливих наслідків.

національні інтереси в інформаційній сфері – життєво важливі потреби Українського народу, суспільства і держави в інформаційній сфері, реалізація яких забезпечує їхнє самозбереження, сталий і прогресивний розвиток;

національні цінності України в інформаційній сфері - суверенітет національного інформаційного простору, розвиток інформаційно-комунікаційних технологій як основа матеріального добробуту населення, інформаційна захищеність людини, суспільства, держави, духовність, зокрема свобода совісті, мова, як основний ідентифікатор нації, як спосіб передачі інформації та знань, як пам'ять поколінь, культура інформаційних

відносин, свобода інформації та доступу до інформації, інтелектуальні та духовні надбання Українського народу, а також інші цінності інформаційної сфери, які забезпечують самозбереження, сталий і прогресивний розвиток Українського народу, суспільства і держави;

національні цілі України в інформаційній сфері - завдання, які Українська держава ставить перед собою заради забезпечення захищеності своїх національних цінностей та реалізації національних інтересів в інформаційній сфері;

ризики інформаційної безпеки України – вразливості інформаційної безпеки та системи її забезпечення, які сприяють реалізації загроз, а також ймовірність зазнати шкоди внаслідок їх реалізації;

спеціальні засоби впливу – технічні й програмні засоби, які застосовуються для інформаційного чи/та інформаційно-психологічного впливу;

спеціальні методи впливу – сукупність та алгоритм прийомів інформаційного (інформаційно-психологічного) впливу;

стандарти інформаційної безпеки – параметри допустимого інформаційного впливу, затверджені в установленому порядку;

суб’єкти інформаційних процесів – фізичні та юридичні особи, їх об’єднання, держава в особі своїх органів та посадових осіб, які для реалізації своїх потреб та виконання покладених на них функцій вступають у взаємини, що складаються в процесі збирання, обробки, зберігання, передачі та розповсюдження інформації, різноманітність яких відображає множину сфер життєдіяльності суспільства.

Інші терміни у цьому Законі вживаються у значенні, наведеному в інших законах України.

Розділ II

ОСНОВИ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Стаття 2. Правова основа державної політики у сфері інформаційної

безпеки України

1. Інформаційна безпека України забезпечується шляхом проведення виваженої державної політики відповідно до прийнятих в установленому порядку доктрин, концепцій, стратегій і програм у інформаційній сфері.

2. Правову основу державної політики у сфері інформаційної безпеки України становлять Конституція України, Закон України «Про національну безпеку України», цей та інші закони України, а також міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, а також видані на виконання Конституції та законів України інші нормативно-правові акти.

Стаття 3. Принципи державної політики у сфері інформаційної безпеки України

Основними принципами, що визначають порядок формування державної політики у сфері національної безпеки та забезпечення інформаційної безпеки, є:

- пріоритет прав і свобод людини і громадянина;
- законність та верховенство права;
- збалансованість інтересів особи, суспільства та держави;
- своєчасність і адекватність заходів забезпечення інформаційної безпеки актуальним викликам і загрозам;
- чітке розмежування повноважень та взаємодія складових сектору безпеки і оборони та інших державних органів у забезпеченні інформаційної безпеки;
- єдине управління в усіх сферах забезпечення інформаційної безпеки з метою забезпечення ефективності виконання завдань та використання ресурсів;
- монополія держави на розробку й виготовлення спеціальних засобів інформаційного (інформаційно-психологічного) впливу;
- дотримання норм міжнародного права та участь у міжнародних зусиллях з підтримання інформаційної безпеки;

- використання в інтересах України міждержавних систем та механізмів міжнародної колективної безпеки;

- розвиток сектору безпеки і оборони як основного інструменту реалізації державної політики у сфері інформаційної безпеки;

- застосування превентивних заходів щодо захисту національних цінностей, реалізації національних інтересів та досягнення національних цілей в інформаційній сфері;

- прозорість, гласність та дотримання засад демократичного цивільного контролю у сфері забезпечення інформаційної безпеки;

- обов'язковість залучення до діяльності із забезпечення інформаційної безпеки громадських організацій.

Стаття 4. Система забезпечення інформаційної безпеки України

1. Державна політика у сфері інформаційної безпеки України реалізується через систему забезпечення інформаційної безпеки України.

2. Система забезпечення інформаційної безпеки України є механізмом взаємодії її складових, заснованим на національних цінностях, інтересах та цілях українського суспільства, та спрямованим на забезпечення реалізації стратегічних завдань держави, визначених державною політикою у сфері інформаційної безпеки.

3. Систему забезпечення інформаційної безпеки України складають суб'єкти забезпечення інформаційної безпеки та сукупність нормативно-правових актів, що регламентують відносини у сфері захисту національних цінностей, реалізації національних інтересів та досягнення національних цілей в інформаційній сфері.

Стаття 5. Міжнародне співробітництво з питань інформаційної безпеки

1. Міжнародне співробітництво з питань інформаційної безпеки є однією з форм реалізації державної політики у сфері інформаційної безпеки і спрямовується на захист національних цінностей, реалізацію

національних інтересів та досягнення національних цілей в інформаційній сфері.

2. Міжнародне співробітництво з питань інформаційної безпеки здійснюється під загальним керівництвом Президента України.

Розділ ІІІ

СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Стаття 6. Інформаційна безпека як складова національної безпеки України

1. Інформаційна безпека є однією з основних складових національної безпеки України.

2. Основними складовими інформаційної безпеки України є безпека інформації, безпека від інформаційних впливів, в тому числі інформаційно-психологічна безпека, а також належний порядок реалізації прав та інтересів суб'єктів інформаційної сфери.

Стаття 7. Об'єкти інформаційної безпеки України

1. Об'єктами національної безпеки України є:

людина і громадянин - їхні життя і здоров'я, честь і гідність, недоторканність і безпека, інформаційні права і свободи;

суспільство - його духовні, морально-етичні, культурні, історичні, інтелектуальні цінності, інформаційне середовище та інформаційні ресурси, суспільно-політична стабільність, міжетнічна та міжконфесійна злагода;

держава - її інформаційний суверенітет, недоторканність, інформаційні ресурси та інформаційна інфраструктура.

Стаття 8. Національні цінності України в інформаційній сфері

1. Перелік національних цінностей України в інформаційній сфері є невичерпним.

2. Фундаментальними національними цінностями України в інформаційній сфері є:

- суверенітет національного інформаційного простору;

- розвиток інформаційно-комунікаційних технологій як основа матеріального добробуту населення;

- інформаційна захищеність людини, суспільства, держави;

- духовність, зокрема свобода совісті;

- мова, як основний ідентифікатор нації, як спосіб передачі інформації та знань, як пам'ять поколінь;

- культура інформаційних відносин;

- свобода інформації та доступу до інформації.

Стаття 9. Національні інтереси України в інформаційній сфері

1. Перелік національних інтересів України в інформаційній сфері є невичерпним.

2. Фундаментальними національними інтересами України в інформаційній сфері є:

1) життєво важливі інтереси особи:

- забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації;

- забезпечення конституційних прав людини на захист приватного життя;

- захищеність від руйнівних інформаційно-психологічних впливів;

2) життєво важливі інтереси суспільства і держави:

- захист українського суспільства від агресивного впливу деструктивної пропаганди, передусім з боку іноземних держав;

- захист українського суспільства від агресивного інформаційного впливу іноземних держав, спрямованого на пропаганду війни, розпалювання національної і релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України;

- всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності у доступі до достовірної та об'єктивної інформації;

- забезпечення вільного обігу інформації, крім випадків, передбачених законом;

- розвиток та захист національної інформаційної інфраструктури;

- збереження і примноження духовних, культурних і моральних цінностей Українського народу;

- забезпечення всебічного розвитку і функціонування української мови в усіх сферах суспільного життя на всій території України;

- вільний розвиток, використання і захист мов національних меншин та сприяння вивченню мов міжнародного спілкування;

- зміцнення інформаційних зв'язків з українською діаспорою, сприяння збереженню її етнокультурної ідентичності;

- розвиток медіа-культури суспільства та соціально відповідального медіа-середовища;

- формування ефективної правової системи захисту особи, суспільства та держави від деструктивних пропагандистських впливів;

- створення з урахуванням норм міжнародного права системи і механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів, передусім пропаганди;

- розвиток інформаційного суспільства, зокрема його технологічної інфраструктури;

- безпечне функціонування і розвиток національного інформаційного простору та його інтеграція у європейський і світовий інформаційний простір;

- розвиток системи стратегічних комунікацій України;

- ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації державної політики в інформаційній сфері;

- забезпечення розвитку інформаційно-комунікаційних технологій та інформаційних ресурсів України;

- захищеність державної таємниці та іншої інформації, вимоги щодо захисту якої встановлені законом;

- формування позитивного іміджу України у світі, донесення оперативної, достовірної і об'єктивної інформації про події в Україні до міжнародної спільноти;

- розбудова системи іномовлення України та забезпечення наявності іншомовного українського каналу в кабельних мережах та у супутниковому мовленні за межами України.

Стаття 10. Національні цілі України в інформаційній сфері

1. Перелік національних цілей України в інформаційній сфері визначається необхідністю забезпечення захищеності національних цінностей та реалізації національних інтересів в інформаційній сфері.

2. Пріоритетними національними цілями України в інформаційній сфері є:

- побудова та розвиток інформаційного суспільства;
- інтеграція України у світовий інформаційний простір;
- сприяння інтеграції національної інформаційної інфраструктури до світової інформаційної інфраструктури;
- недопущення інформаційної залежності, інформаційної блокади України, інформаційної експансії з боку інших держав та міжнародних структур;
- забезпечення ефективної взаємодії органів державної влади та інститутів громадянського суспільства при формуванні, реалізації та коригуванні державної політики в інформаційній сфері;
- забезпечення економічного та науково-технологічного розвитку України;
- формування позитивного іміджу України в умовах інформаційної глобалізації;
- зміцнення захисту інформаційних прав людини;

- унеможливлення спотворення поглядів людей на навколишній світ і самих себе, що здійснюється шляхом культивування уявних цінностей, насадження деструктивних пріоритетів, завдань і цілей перед суспільством і окремою особистістю;

- забезпечення впровадження інформаційних технологій у військову сферу та забезпечення їх захисту;

- прискорення розробку та впровадження новітніх конкурентоспроможних ІКТ до суспільно-економічної сфери;

- досягнення належного рівня культури інформаційних відносин;

- створення загальнодержавних інформаційних систем для постійного екологічного моніторингу стану навколишнього середовища.

Стаття 11. Виклики та загрози інформаційній безпеці України

1. Перелік викликів та загроз інформаційній безпеці України, а також їх джерел є невичерпним і з урахуванням особливостей безпекового середовища визначається у документах довгострокового, середньострокового та короткострокового планування відповідно до Закону України «Про національну безпеку України» та цього Закону.

2. Факторами безпекового середовища, що сприяють реалізації викликів та загроз інформаційній безпеці України є, зокрема, наступні:

- несформованість на належному рівні суверенного інформаційного простору;

- намагання маніпулювати суспільною свідомістю, в тому числі шляхом поширення шкідливої, недостовірної, неповної або упередженої інформації у глобальних інформаційних мережах;

- зростання залежності людини від соціальних мереж;

- вплив на інформаційну інфраструктуру України, інформаційні ресурси, на суспільство, свідомість та підсвідомість особистості, з метою нав’язати власну систему цінностей, поглядів, інтересів і рішень у життєво

важливих сферах суспільної й державної діяльності, керувати їхньою поведінкою і розвитком у бажаному для іншої сторони;

- незаконне обмеження прав і свобод громадян, законних інтересів організацій в інформаційній сфері, свободи засобів масової інформації;

- незаконне розкриття інформації з обмеженим доступом, порушення інших передбачених законом обмежень на розповсюдження інформації;

- протиправні дії щодо відкритої інформації;

- порушення встановленого порядку захисту інформації;

- недобросовісна конкуренція на ринку інформаційних послуг, його монополізація;

- протиправне застосування спеціальних засобів інформаційного (інформаційно-психологічного) впливу на індивідуальну, групову та суспільну свідомість;

- розповсюдження інформації, що пропагує культ насильства й жорстокості, порнографічної продукції;

- інформаційний екстремізм.

3. Загрози інформаційній безпеці України за своїм спрямуванням мають внутрішній, зовнішній або системний характер і зумовлюють ризики у інформаційній сфері, а також у сфері державного управління, зовнішньополітичній, воєнній, правоохоронній, економічній, фінансовій, соціальній, науково-технологічній, гуманітарній, екологічній сферах тощо.

4. Вибір конкретних засобів і шляхів забезпечення інформаційної безпеки обумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру і масштабам викликів та загроз інформаційній безпеці України.

Розділ IV

СУБ’ЄКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Стаття 12. Суб’єкти забезпечення інформаційної безпеки України

1. Суб’єктами забезпечення інформаційної безпеки України є сектор безпеки і оборони, а також державні органи, органи місцевого самоврядування, підприємства, установи та організації, об’єднання громадян та окремі громадяни, які беруть участь у забезпеченні інформаційної безпеки.

2. Завдання, функції та повноваження складових сектору безпеки і оборони визначаються цим Законом та іншими законами України.

Інші суб’єкти забезпечення інформаційної безпеки виконують завдання та здійснюють функції у сфері забезпечення інформаційної безпеки в межах своїх повноважень та у взаємодії з органами, які входять до складу сектору безпеки і оборони.

Стаття 13. Основні функції суб’єктів забезпечення інформаційної безпеки України

1. Основними функціями суб’єктів забезпечення інформаційної безпеки є:

- вироблення і періодичне уточнення Стратегії національної безпеки України і Стратегії воєнної безпеки України в частині, що стосується забезпечення інформаційної безпеки, а також доктрин, концепцій, стратегій і програм у сфері інформаційної безпеки, планування і здійснення конкретних заходів щодо протидії і нейтралізації загроз інформаційної безпеці України;
- створення нормативно-правової бази, необхідної для ефективного функціонування системи забезпечення інформаційної безпеки;
- удосконалення організаційної структури системи забезпечення інформаційної безпеки;
- комплексне кадрове, фінансове, матеріальне, технічне, інформаційне та інше забезпечення життєдіяльності складових (структурних елементів) системи забезпечення інформаційної безпеки;

- підготовка сил та засобів суб'єктів системи забезпечення інформаційної безпеки до їх застосування за призначенням;

- постійний моніторинг безпекового середовища з метою відстеження впливу на інформаційну безпеку процесів, що відбуваються в політичній, соціальній, економічній, екологічній, науково-технологічній, інформаційній, воєнній та інших сферах, релігійному середовищі, міжетнічних стосунках;

- систематичне спостереження за станом і проявами міжнародного та інших видів інформаційного тероризму та екстремізму, транснаціональної організованої злочинності в інформаційній сфері;

- прогнозування змін безпекового середовища, визначення та оцінювання актуальних викликів та загроз інформаційної безпеці;

- прогнозування, визначення та оцінювання ризиків, зумовлених загрозами інформаційної безпеці України;

- розроблення науково обґрунтованих пропозицій і рекомендацій щодо прийняття рішень з метою управління ризиками інформаційної безпеки України;

- оцінка результативності дій щодо забезпечення інформаційної безпеки та визначення витрат на ці цілі;

- участь у двосторонньому і багатосторонньому співробітництві у сфері інформаційної безпеки, якщо це відповідає національним інтересам України;

- спільне проведення заходів у рамках міжнародних організацій та договорів у сфері інформаційної безпеки.

Стаття 14. Основні завдання сектору безпеки і оборони у сфері забезпечення інформаційної безпеки України

Основними завданнями сектору безпеки і оборони у сфері забезпечення інформаційної безпеки України є:

- *Захист життєво важливих інтересів особистості, суспільства та держави від внутрішніх і зовнішніх загроз:*

a. вдосконалення діючої системи забезпечення інформаційної безпеки Збройних Сил України, військових формувань і органів, що включає в себе сили і засоби інформаційного протиборства;

b. розробка та впровадження дієвих механізмів прогнозування, виявлення та оцінки інформаційних загроз;

c. нейтралізація інформаційно-психологічного впливу, в тому числі спрямованого на підрив історичної спадщини, її спотворення чи викривлення фактів;

d. поширення національного інформаційного продукту на тимчасово окупованих територіях. Розробка та впровадження цілісної державної інформаційної політики щодо окупованих територій;

e. розвиток інформаційної культури серед молоді, а також культури особистої інформаційної безпеки, профілактика правопорушень в інформаційній сфері;

- *Захист суверенітету, підтримку політичної та соціальної стабільності, територіальної цілісності України:*

f. протидія використанню інформаційних технологій для пропаганди екстремістської ідеології, поширення ксенофобії, ідей національної ворожнечі, в тому числі й на міжнародному рівні;

g. забезпечення захисту державної таємниці, іншої інформації обмеженого доступу, особливо комерційної таємниці підприємств військово-промислового комплексу та інших, які мають особливе значення для економіки держави;

h. нейтралізація інформаційного впливу, спрямованого на розмивання традиційних духовно-моральних цінностей українського нарду;

i. підготовка спеціалістів з протидії інформаційним загрозам на рівні державних освітніх програм;

- *Захист критичної інформаційної інфраструктури:*

j. підвищення захищеності критичної інформаційної інфраструктури та стійкості її функціонування;

k. розвиток механізмів виявлення та попередження інформаційних загроз і ліквідації наслідків їх прояву, викликаних інформаційно-технічним впливом на об'єкти критичної інформаційної інфраструктури;

l. підвищення безпеки функціонування об'єктів інформаційної інфраструктури;

m. розробка механізмів обміну інформацією з країнами НАТО та ЄС про передові практики в сфері забезпечення безпеки функціонування елементів критичної інформаційної інфраструктури;

- *Забезпечення розвитку інформаційно-комунікаційних технологій:*

n. розробка і виробництво конкурентоспроможних засобів забезпечення інформаційної безпеки;

o. інноваційний розвиток галузі інформаційних технологій підтвердженням чого має стати підняття у рейтингу Індексу розвитку інформаційно-комунікаційних технологій;

p. підтримка інноваційного та прискореного розвитку системи забезпечення інформаційної безпеки, галузі інформаційних технологій;

q. проведення наукових досліджень і здійснення дослідно-конструкторських розробок з метою створення перспективних інформаційних технологій забезпечення інформаційної безпеки;

- *Забезпечення участі України в міжнародній системі інформаційної безпеки:*

r. участь у формуванні системи міжнародної інформаційної безпеки на двосторонньому, багатосторонньому, регіональному, субрегіональному та глобальному рівнях;

s. участь у розробці міжнародних документів системи інформаційної безпеки;

t. формування механізмів міжнародного співробітництва в сфері протидії загрозам використання інформаційних та комунікаційних технологій у терористичних цілях;

u. продовження та посилення співпраці з НАТО, ЄС у сфері попередження загроз в інформаційній сфері на державному та глобальному рівнях;

v. сприяння підготовці та прийняттю державами - членами Організації Об'єднаних Націй міжнародних правових актів, що регламентують застосування принципів і норм міжнародного права в сфері інформаційної безпеки;

w.розвиток співпраці в сфері протидії інформаційній злочинності з державами – членами НАТО та ЄС та підвищення ефективності інформаційного обміну між правоохоронними органами держав в ході розслідування злочинів в інформаційній сфері;

- *Сприяння вдосконаленню науково-практичних засад забезпечення інформаційної безпеки;*

- *Розробка і прийняття стандартів у сфері інформаційної безпеки;*

- *Організація системи ліцензування, сертифікації, експертизи та контролю у сфері інформаційної безпеки;*

- *Створення загальнодержавної системи підготовки кадрів у сфері інформаційної безпеки;*

- *Координація діяльності органів державної влади, місцевого самоврядування, організацій усіх форм власності у сфері забезпечення інформаційної безпеки.*

Стаття 15. Завдання державних органів, які не входять до складу сектору безпеки і оборони, а також органів місцевого самоврядування у сфері забезпечення інформаційної безпеки України

1. Міністерства, інші центральні органи виконавчої влади в межах своїх повноважень забезпечують виконання передбачених Конституцією і законами України, актами Президента України, Кабінету

Міністрів України завдань, здійснюють реалізацію концепцій, програм у сфері інформаційної безпеки, підтримують у стані готовності до застосування сили та засоби забезпечення національної безпеки.

2. Правоохоронні органи ведуть боротьбу із злочинністю у інформаційній сфері відповідно до своєї компетенції, визначеної законами України.

3. Суди загальної юрисдикції здійснюють судочинство у справах про злочини, що становлять загрозу інформаційній безпеці України, а також інформаційним правам і свободам людини та громадянина.

4. Прокуратура України здійснює повноваження у сфері інформаційної безпеки України відповідно до Конституції України та Закону України «Про прокуратуру України».

5. Місцеві державні адміністрації та органи місцевого самоврядування забезпечують вирішення питань у сфері інформаційної безпеки, віднесених законодавством до їхньої компетенції.

Стаття 16. Завдання громадян України та їх об’єднань у сфері забезпечення інформаційної безпеки України

1. Громадяни України, впроваджуючи культуру інформаційних відносин, реалізують виконання визначеного Конституцією України завдання щодо забезпечення інформаційної безпеки.

2. Громадяни України через участь у виборах, референдумах та через інші форми безпосередньої демократії, а також через органи державної влади та органи місцевого самоврядування, які вони обирають, реалізують національні інтереси, добровільно і в порядку виконання конституційних обов'язків здійснюють заходи, визначені законодавством щодо забезпечення інформаційної безпеки України.

3. Громадяни України як безпосередньо, так і через об'єднання громадян привертають увагу суспільних і державних інститутів до небезпечних явищ і процесів у різних сферах життєдіяльності країни; у законний спосіб і законними засобами захищають власні інформаційні

права та інтереси, а також власну інформаційну, зокрема інформаційно-психологічну безпеку.

Стаття 17. Координація діяльності у сфері забезпечення інформаційної безпеки

1. Органами, які в межах своїх повноважень координують діяльність у сфері забезпечення інформаційної безпеки є Рада національної безпеки і оборони України та Служба безпеки України.

2. Координація діяльності органів державної системи забезпечення інформаційної безпеки полягає в: організації ліцензування фізичних і юридичних осіб, які беруть участь у забезпеченні інформаційної безпеки, та контролі за їхньою діяльністю; організації сертифікації методів і засобів інформаційного впливу, контролі за цією діяльністю; організації проведення експертиз у сфері забезпечення інформаційної безпеки, контролі за діяльністю експертів (експертних організацій чи підрозділів); розміщенні державного замовлення на проведення досліджень у сфері інформаційної безпеки; загальному контролі за забезпеченням інформаційної безпеки.

3. Рада національної безпеки і оборони України з урахуванням змін у безпековому середовищі визначає концептуальні підходи, напрями, заходи із забезпечення інформаційної безпеки, схвалює проекти стратегій, концепцій, державних програм та інших стратегічних документів, якими визначаються основні напрями і завдання державної політики у сфері інформаційної безпеки, здійснює координацію і контроль за їх виконанням.

4. Для організації і здійснення заходів з питань інформаційної безпеки та координації суб’єктів забезпечення інформаційної безпеки України при Службі безпеки України створюється та функціонує Центр інформаційної безпеки. Положення про Центр інформаційної безпеки при Службі безпеки України затверджується Президентом України за поданням Кабінету Міністрів України.

Розділ V

ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНОФРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Стаття 18. Мета, принципи і види планування у сфері забезпечення інформаційної безпеки України

1. Метою планування у сфері забезпечення інформаційної безпеки України є забезпечення реалізації державної політики у цих сферах шляхом розроблення стратегій, концепцій, програм, планів розвитку органів сектору безпеки і оборони, управління ресурсами та ефективного їх розподілу.

2. Планування у сфері забезпечення інформаційної безпеки України здійснюється відповідно до таких принципів:

- дотримання національного законодавства і міжнародних зобов'язань України;

- демократичний цивільний контроль за сектором безпеки і оборони, відкритість інформації про державну політику, стратегічні документи, цілі, пріоритети і завдання планування, прозорість та підзвітність використання ресурсів;

- цілісність, узгодженість, системність планування у сфері забезпечення інформаційної безпеки України, врахування пріоритетів і обмежень, встановлених державними програмами, планами та прогнозними документами;

- своєчасність та відповідність прийнятим рішенням щодо забезпечення інформаційної безпеки України.

3. Планування у сфері забезпечення інформаційної безпеки України поділяється на довгострокове (понад п’ять років), середньострокове (до п'яти років) та короткострокове (до трьох років).

Порядок планування у сфері забезпечення інформаційної безпеки України визначається Законом України «Про національну безпеку України» та цим Законом

Стаття 19. Вимоги до заходів забезпечення інформаційної безпеки

1. Заходи, здійснювані сектором безпеки і оборони та іншими державними суб’єктами забезпечення інформаційної безпеки, повинні забезпечити прийнятний рівень інформаційної безпеки, достатній для уникнення шкідливих інформаційних впливів або мінімізації їх наслідків.

2. Ліцензування діяльності із захисту інформації допускається виключно в разі сертифікації методів і засобів, що в ній використовуються.

3. Діяльність з виявлення шкідливих інформаційних впливів здійснюється з обов’язковим проведенням експертиз відповідно до державних стандартів. Порядок проведення експертиз встановлюється цим законом та нормативно-правовими актами Кабінету міністрів України.

4. Контроль за дотриманням законності у діяльності із забезпечення інформаційної безпеки та її достатнім державним забезпеченням здійснюється органами, які в координують діяльність у сфері забезпечення інформаційної безпеки.

Стаття 20. Основні принципи обмеження доступу до інформації

1. Обмеження доступу до інформації ґрунтується на таких принципах:

- законність;
- відповідність встановлюваного режиму доступу та заходів захисту інформації її значущістю;
- недопустимість встановлення режиму обмеження доступу до відкритої інформації, обмеження доступу до якої забороняється законом.

Стаття 21. Заходи забезпечення безпеки відкритої інформації

1. Заходи забезпечення безпеки відкритої інформації вживаються з метою:

- реалізації права на доступ до інформації;
- запобігання протиправному доступу, наданню, копіюванню, розповсюдженню, трансформації, блокуванню, знищенню та іншим незаконним діям щодо такої інформації.

2. Заходи забезпечення безпеки відкритої інформації здійснюються із застосуванням виключно ліцензійних програмних засобів, сертифікованих спеціалізованого програмно-технічного обладнання та засобів зв’язку.

Стаття 22. Заходи забезпечення безпеки інформації в загальнодоступних державних інформаційних мережах

1. Основними принципами забезпечення безпеки інформації в державних інформаційних мережах загального користування є:

- дотримання конституційних прав людини і громадянина;

- забезпечення достовірності інформації, що міститься в загальнодоступних державних інформаційних мережах;

- неприпустимість втручання в роботу загальнодоступних державних інформаційних мереж;

- підтримання оптимального співвідношення між доступністю інформації, що міститься в загальнодоступних державних інформаційних мережах, із забезпеченням її безпеки.

2. Заходи забезпечення безпеки інформації, що міститься в загальнодоступних державних інформаційних мережах, здійснюються виключно державними органами й установами.

3. Заходи забезпечення безпеки інформації, що міститься в загальнодоступних державних інформаційних мережах, проводяться із застосуванням виключно ліцензійних програмних засобів, сертифікованих спеціалізованого програмно-технічного обладнання та засобів зв’язку.

4. Контроль за діяльністю із забезпечення безпеки інформації, що міститься в загальнодоступних державних інформаційних мережах, здійснюється органами, які в координують діяльність у сфері забезпечення інформаційної безпеки.

Стаття 23. Обмеження у здійсненні інформаційного впливу

1. Забороняється здійснення інформаційного, зокрема інформаційно-психологічного впливу з метою заподіяння шкоди життю і здоров’ю людини, знищення, пошкодження, порушення нормального

порядку функціонування об’єктів інформаційної інфраструктури, порушення інформаційних процесів, а також прав та свобод людини і громадянина.

2. Застосування представниками уповноважених державних органів спеціальних методів і засобів інформаційно-психологічного впливу допускається виключно у таких випадках:

1) без відома об’єктів інформаційно-психологічного впливу:

- у надзвичайних ситуаціях (стихійні лиха, катастрофи техногенного чи іншого характеру тощо) – для рятування людей, ліквідації наслідків тощо;

- під час воєнних дій, проведення антитерористичних та миротворчих операцій, боротьби з організованою злочинністю - проти зовнішнього агресора, учасників незаконних збройних формувань, терористичних або організованих злочинних угруповань, інших осіб, що вчиняють тяжкі або особливо тяжкі злочини;

2) за згодою об’єктів інформаційно-психологічного впливу:

- з науковою метою (психічні, психологічні дослідження тощо);

- під час підготовки фахівців: із застосування методів і засоби психологічного впливу; з управління екстремальними та надзвичайними ситуаціями; з протидії тероризму; з питань забезпечення інформаційної безпеки.

Розділ VI. ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО ІНФОРМАЦІЙНУ БЕЗПЕКУ

Стаття 24. Порушення законодавства про інформаційну безпеку та відповідальність за їх вчинення

1. Відповідальність за порушення законодавства про інформаційну безпеку несуть суб’єкти забезпечення інформаційної безпеки, суб’єкти інформаційних процесів, а також інші особи, якщо порушення законодавства відбулися внаслідок їх протиправного втручання.

2. Особи, винні у:

- несанкціонованому знищенні чи модифікації інформації або її матеріальних носіїв;
- порушенні встановленого режиму доступу до інформації;
- порушенні порядку встановлення режиму доступу до інформації;
- необґрунтованому віднесенні інформації до категорії таємної;
- невиконанні вимоги закону про віднесення інформації до категорії таємної державними органами, які здійснюють формування переліків відомостей, що становлять певний вид таємної інформації;
- ненаданні грифу обмеження доступу матеріальним носіям таємної інформації, його безпідставному скасуванні, а також у наданні грифуа обмеження доступу матеріальним носіям таємної інформації з порушенням правил, що встановлені цим Законом;
- невжитті суб‘єктом, відповідальним за інформацію з обмеженим доступом, заходів, а також невиконання норм і вимог щодо забезпечення безпеки інформації з обмеженим доступом, яка перебуває в їхньому віданні;
- розповсюдження недостовірної інформації, яка шкодить законним інтересам людини, суспільства, держави;
- розповсюдженні інформації, яка шкодить розвитку та моральному здоров’ю дітей та молоді;
- порушенні недоторканості приватного життя та конфіденційності персональних даних;
- здійсненні незаконного інформаційного та інформаційно-психологічного впливу;
- інформаційному екстремізмі;
- пропаганді культу насильства, жорстокості, порнографії, протиправних, антисуспільних та аморальних дій;
- інших протиправних діях, визначених законами України,

несуть відповідальність згідно з чинним законодавством.

Стаття 25. Відшкодування шкоди

1. Відшкодування матеріальної та моральної шкоди, завданої порушенням законодавства про інформаційну безпеку, здійснюється у повному обсязі відповідно до вимог цивільного законодавства України та цього Закону.

2. Відшкодуванню підлягає шкода, що завдана цілісності та достовірності інформації, конфіденційності (таємності) інформації з обмеженим доступом, шкода, завдана порушенням встановленого режиму доступу до інформації або необґрунтованим встановленням режиму обмеженого доступу до неї, шкода, пов‘язана з вибуттям інформації із виключного законного володіння, шкода, завдана внаслідок інформаційних впливів інформації, інформаційній інфраструктурі та суб’єктам інформаційних процесів, зокрема фізична та моральна шкода, завдана здоров’ю людини інформаційно-психологічним впливом, а також шкода, зокрема моральна, завдана внаслідок несанкціонованого поширення інформації.

3. Шкода, пов‘язана з вибуттям інформації з обмеженим доступом із виключного законного володіння, відшкодовується незалежно від того, чи є таке вибуття фактичним внаслідок викрадення матеріальних носіїв інформації, або таким, що зумовлене несанкціонованим ознайомленням з інформацією чи (та) її копіюванням.

4. Моральна шкода, завдана порушенням законодавства про інформаційну безпеку, підлягає відшкодуванню незалежно від того, чи доведе особа, діями якої завдано моральної шкоди, що інформація, яка була поширена нею в порушення встановленого режиму доступу до неї, відповідає дійсності.

5. Суб‘єкт, відповідальний за інформацію з обмеженим доступом зобов‘язаний відшкодувати шкоду, завдану порушенням встановленого

режиму доступу до такої інформації, якщо не доведе, що шкода виникла внаслідок непереборної сили або протиправних дій інших осіб.

Стаття 26. Оскарження та судовий захист

Учасники суспільних відносин, що виникають в інформаційній сфері, зокрема з приводу забезпечення інформаційної безпеки, які вважають, що їхні законні права та інтереси порушено, мають право на оскарження в порядку підлеглості рішень уповноважених державних органів, а також на звернення до суду за захистом своїх прав безпосередньо або після розгляду скарги в порядку підлеглості.

Якщо законодавством України передбачене досудове врегулювання спірних питань, звернення до суду є можливим після здійснення такого врегулювання.

Розділ VII

ПРИКІНЦЕВІ ТА ПЕРЕХІДНІ ПОЛОЖЕННЯ

1. Цей Закон набирає чинності з дня, наступного за днем його опублікування.

2. До приведення інших законодавчих актів у відповідність з нормами цього Закону вони діють у частині, що не суперечить цьому Закону.

Додаток В

Пам’ятка для посадових осіб органів державної влади та місцевого самоврядування як не стати жертвою шпигунських посягань