Національна безпека

УДК 351:354

Чіпуріна Галина Михайлівна

Національна академія СБ України

Chipurina Halyna

National Academy of Security Service of Ukraine

Єрьоміна Людмила Валеріївна

Національна академія СБ України

Yeromina Liudmyla

National Academy of Security Service of Ukraine

СИСТЕМА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ: ТЕОРЕТИКО-ПРАВОВИЙ ВИМІР
STATE INFORMATION SECURITY SYSTEM: THEORETICAL AND LEGAL DIMENSION

Анотація. *Авторами статті здійснюється теоретико-правове дослідження системи забезпечення інформаційної безпеки держави та її складових. Проаналізовано наукові підходи до визначення системи забезпечення інформаційної безпеки та її складових. Серед складових системи забезпечення інформаційної безпеки виділено суб'єктів забезпечення, об'єктів, механізми та принципи забезпечення інформаційної безпеки. Визначено суб'єктів забезпечення інформаційної безпеки державного та недержавного рівнів.*

Ключові слова: *інформаційна безпека, система забезпечення інформаційної безпеки, загрози інформаційній безпеці держави, суб'єкти забезпечення інформаційної безпеки.*

Summary. *The authors of the article carry out a theoretical and legal study of the system of the information security of the state and its components. Scientific approaches to the definition of the information security system and its components are analyzed. Among the components of the system of information security, the subjects, the objects, the mechanisms and the principles of information security are highlighted. Subjects of ensuring information security at the state and non-state levels have been identified.*

Key words: *information security, information security system, threats to the information security of the state, subjects of information security.*

Постановка проблеми. Збройна агресія російської федерації проти України посилила загрози інформаційній безпеці нашої держави, що вимагає нових підходів до формування сучасної ефективної системи та механізмів забезпечення інформаційної безпеки, які б відповідали характеру і масштабу сучасних викликів. Інформаційна безпека є динамічним та складним явищем, яке залежить від багатьох факторів, як зовнішніх, так і внутрішніх. Крім того інформаційна безпека є невід'ємною складовою національної безпеки, вона тісно пов'язана з усіма сферами національної безпеки, такими як воєнна, державна безпека, економічна, внутрішньо- та зовнішньополітична безпека, а це вимагає системного підходу до забезпечення інформаційної безпеки. Ефективна організація системи забезпечення інформаційно безпеки ґрунтується на всебічному вивченні закономірностей, принципів, механізмів функціонування її складових, що потребує поглибленого теоретико-правового підходу.

Аналіз останніх досліджень і публікацій. Питанням забезпечення інформаційної безпеки держави сьогодні присвячено низка досліджень вітчизняних та зарубіжних учених. Зокрема, у наукових працях різні аспекти інформаційної безпеки вивчали В. Горбулін, В. Гурковський, О. Дзьобань, О. Довгань, Г. Ємельянов, К. Захаренко, Р. Калюжний, Б.

Кормич, В. Ліпкан, А. Марущак, Ю. Максименко, Д. Манзі, М. Мельник, В. В. Пилипчук, Г. Почепцов, М. Присяжнюк, А. Прозоров, В. Рубан, Ф. Саурвейн, Ш. Спенсер-Сміт, К. Тенове, О. Тихомиров, Т. Ткачук, О.Юдін, М.-Дж. Шварц та інші науковці.

П.Д. Біленчук, Л.В. Борисова, І.М. Неклонський та ін. у монографічному дослідженні розкривають особливості інформації як об'єкта правового регулювання інформаційної безпеки та досліджують систему та органи захисту інформації в Україні. Водночас автори слушно вважають, що «інформаційна безпека включає в себе сукупність організаційних, соціально-економічних, правових заходів, спрямованих на забезпечення стабільності розвитку суспільства і держави та цивілізації» [1, с. 65].

В. Шемчук здійснив аналіз теоретичних основ і методології вивчення механізму забезпечення інформаційної безпеки, в ході якого визначив механізм забезпечення інформаційної безпеки як регламентовану законодавством діяльність уповноважених суб'єктів, спрямовану на охорону та захист інформаційної сфери особи, суспільства та держави від зовнішніх і внутрішніх загроз й удосконалення заходів інформаційної протидії та боротьби. Надана дефініція охоплює ключові елементи механізму забезпечення інформаційної безпеки: об'єкт, суб'єкт, загрози, напрями, заходи [2, с. 56].

Учений О. Тихомиров, досліджує систему забезпечення інформаційної безпеки держави, застосовуючи методологічний підхід. Забезпечення інформаційної безпеки держави розглядається ним як діяльність, одним з основних суб'єктів якої є держава. Водночас зміст державного забезпечення інформаційної безпеки О. Тихомиров розуміє як систему державних гарантій в інформаційній сфері, безпосередньо чи опосередковано визначених фундаментальними нормативно-правовими

актами, що регламентують інформаційну сферу суспільних відносин [3, с. 72]

Т. Ткачук обґрунтовує думку про те, що забезпечення інформаційної безпеки України є складним комплексним поняттям, яке охоплює низку процесів і явищ, пов'язаних із протидією загрозам безпеці національних інтересів в інформаційній сфері [4, с. 114].

Вітчизняний науковець Т. Перун акцентує на тому, що забезпечення інформаційної безпеки становить складний соціально-правовий механізм, яким слід вважати формування та проведення державної політики щодо створення та підтримки необхідного рівня захищеності об'єктів безпеки за допомогою здійснення нормативно-правових, організаційних, управлінських й інших заходів, а також заходів, адекватних загрозам життєво важливим інтересам особи, суспільства та держави в інформаційній сфері [5, с. 52].

Українська дослідниця А. Ю. Нашинець-Наумова у своїй роботі обґрунтовує співвідношення системи та механізму забезпечення інформаційної безпеки. На думку ученої, механізм забезпечення інформаційної безпеки є системою різних засобів (політичних, кадрових, оперативно-розшукових, інформаційних, правових), за допомогою яких забезпечують захист інформаційних інтересів держави, суспільства, особи від внутрішніх і зовнішніх загроз [6, С. 53].

Аналіз численних публікацій засвідчує про відсутність усталеного підходу серед авторів до визначення системи забезпечення інформаційної безпеки та її складових.

Метою статті є теоретико-правове дослідження системи забезпечення інформаційної безпеки держави та її складових.

Виклад основного матеріалу. Академічний тлумачний словник української мови серед кількох визначень терміну система дає наступні: «форма організації, будова чого-небудь (державних, політичних,

господарських одиниць, установ і т. ін.); сукупність яких-небудь елементів, одиниць, частин, об'єднуваних за спільною ознакою, призначенням; сукупність принципів, які є основою певного вчення; сукупність способів, методів, прийомів здійснення чого-небудь; будова, структура, що становить єдність закономірно розташованих та функціонуючих частин [7].

Оксфордський словник англійської мови дає визначення терміну «система» як «група або сукупність пов'язаних або об'єднаних між собою речей, що сприймаються або розглядаються як єдність або складне ціле (переклад авторів). Слово походить від давньогрецького терміну sustēma [8].

Т. Ткачук, відносить до системи забезпечення інформаційної безпеки держави суб'єктів, уповноважених на забезпечення інформаційної безпеки, серед яких ним виділено спеціально уповноважених суб'єктів, для яких забезпечення національної безпеки, зокрема й інформаційної як у цілому, так і в її окремих аспектах, є основним завданням, і суб'єкти, які беруть участь у її забезпеченні. При цьому ученим виділяються підсистема, яка ґрунтується за принципом функціональних завдань суб'єктів:

– підсистема інформаційної розвідки (основні суб'єкти – розвідувальні органи, Міністерство оборони України, Служба безпеки України, Міністерство закордонних справ України, тощо);

– підсистема інформаційного захисту, яка включає в себе підсистему захисту інформації та підсистему захисту від інформаційних впливів, зокрема 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 культури та інформаційної політики України, Національна поліція України, Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку, Національна рада України з

питань телебачення й радіомовлення, Державний комітет телебачення й радіомовлення України тощо);

– підсистема інформаційного впливу (основні суб'єкти – Міністерство оборони України, Служба безпеки України, розвідувальні органи України, Міністерство культури та інформаційної політики України тощо) [4].

Рада національної безпеки й оборони України є координаційниим органом з питань національної безпеки і оборони при Президентові України і відповідно в сфері інформаційної безпеки. РНБО здійснює оцінку потенційних і реальних загроз національним інтересам в інформаційній сфері, розробляє й доповідає Президентові України, вносить пропозиції щодо їх попередження й нейтралізації; розглядає на своїх засіданнях і приймає рішення з найбільш актуальних проблем забезпечення інформаційної безпеки; здійснює координацію діяльності органів виконавчої влади щодо забезпечення інформаційної безпеки. Центр протидії дезінформації та Національний координаційний центр кібербезпеки є робочими органами при Раді національної безпеки і оборони України, які забезпечують здійснення заходів щодо протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері, забезпечення інформаційної та кібербезпеки України

На нашу думку, становлення та розвиток інформаційного суспільства в Україні зумовлює необхідність віднесення до суб'єктів системи забезпечення інформаційної безпеки також інституції громадянського суспільства та громадян, тобто суб'єктів забезпечення інформаційної безпеки державного та недержавного рівнів.

З початком повномасштабного вторгнення громадські організації та активісти стали не лише надійним тилом для забезпечення військових і гуманітарних потреб, все більше з них долучилися до інформаційної

боротьби, зокрема протидії російській дезінформації, пропаганді, кіберспротиву, їх метою є спільний захист інформаційного простору України та підвищення рівня медіаграмотності громадян.

За даними досліджень, проведених Інститутом аналітики та адвокації [9], повномасштабна війна призвела до змін у роботі громадських організацій, вони більше співпрацюють, зокрема це простежується в зростанні спільних ініціатив для допомоги українському суспільству, і в боротьбі з агресором. Результати досліджень вказують, що основними способами, якими неурядові організації допомагають у відновленні, є: організація громадських заходів; збір та поширення інформації; проведення досліджень; навчання людей на тренінгах.

Варто зазначити, що питання державно-громадського та державно-приватного партнерства в інформаційному просторі є досить розвинутою в США, Великобританії, країнах ЄС.

Національним інститутом стратегічних досліджень проведено узагальнення та аналіз досвіду надзвичайно різнобічної діяльності громадських об'єднань щодо забезпечення інформаційної безпеки та, зокрема, протидії інформаційній агресії з боку РФ, дає підстави виділити такі її основні напрями.

1. Консультативна та науково-аналітична допомога органам державної влади відповідальним за провадження державної інформаційної політики

2. Контрпропагандистська та інформаційно-просвітня діяльність. Збір, аналіз та поширення даних про суб'єктів зовнішньої агресії (включаючи інформаційну) проти України:

3. Соціологічні та науково-аналітичні дослідження стану масової свідомості та інформаційного простору, наслідків впливу на них інформаційної агресії та напрацювання науково-методологічних рекомендацій щодо протидії їй.

4. Наукова-дослідницька та просвітницька робота зосереджена на критичному аналізі неспроможності ідеологічних та теоретико-методологічних засад російської інформаційної агресії: зокрема, проросійських фальсифікацій історії та концепції «русского мира».

5. Збір даних, документування, узагальнення, аналіз та оприлюднення інформації щодо системних порушень прав людини та воєнних злочинів рф [10].

Погоджуємося з Н. Сіпайло та Л. Сіпайло, які вважають, що функціонування системи забезпечення інформаційної безпеки держави за підтримки неурядових організацій може здійснюватися шляхом залучення неурядових організацій до налагодження дієвої інфраструктури інформаційного забезпечення національної безпеки держави; спрямування діяльності неурядових організації з метою координації діяльності державних органів щодо визначення, попередження та прогнозування явищ у сфері впливу на інформаційну безпеку; сприяння залученню неурядовими організаціями досвіду міжнародного співробітництва у сфері забезпечення інформаційної безпеки; залучення неурядових організацій до розроблення та обговорення пропозицій щодо зміни нормативно-правової бази у сфері забезпечення інформаційної безпеки держави [11].

Одним із напрямів російських неформаційних атак проти України є посилення суперечностей між владою та суспільством, намагання штучно викликати будь-які форми протестної активності, у всіх сферах суспільного життя. Проти нашої країни ворог використовує найновіші інформаційні технології впливу на людську свідомість, спрямовані на пропаганду агресивної війни, поширення фейків про діяльність ЗСУ та органів влади України, розпалювання національної та релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету та територіальної цілісності України, дискредитації нашої держави серед

міжнародної спільноти з метою послаблення політичної та військової підтримки зарубіжних партнерів.

На сучасному етапі, в умовах російської військової агресії, відмічається тенденція до збільшення спроб з боку структур країни-терориста та її союзників використати інформаційні можливості електронних ЗМІ, інформаційні платформи Інтернет-мережі, Телеграм-канали, соціальні мережі для формування суспільної свідомості, інспірування панічних настроїв, глорифікації військових формування рф, терористичних формувань т.зв. «Л/ДНР», окупації українських територій.

У зв'язку з цим досягнення високого рівня ефективності системи забезпечення інформаційної безпеки є неможливим без залучення до інформаційної боротьби не лише громадських структур, але й окремих громадян: лідерів громадської думки, відомих блогерів та медійників.

Погоджуємося із запропонованим К. Захарченко твердженням, що кращі безпекові стратегії та практики, які успішно захищають сучасний інформаційний простір, побудовані на трьох визначальних принципах: ієрархічності, державної координованості та взаємодії [12].

На нашу думку, найбільш слушною є модель системи забезпечення інформаційної безпеки, запропонована О. Довганем та Т. Ткачуком, у якій до об'єктів інформаційної безпеки вони відносять: конституційні права, свободи людини і громадянина, фізичне та психологічне здоров'я населення, захищеність людини від деструктивного та маніпулятивного інформаційних впливів; інформаційне забезпечення, гарантії інформаційних прав та права на розвиток населення всіх регіонів України; інформаційний суверенітет, безпеку національного сегмента глобального інформаційного простору, інформаційної інфраструктури, захищеність, цілісність, доступність та безпечність інформаційних ресурсів, продукції і послуг [13].

Дослідження системи забезпечення інформаційної безпеки вимагає визначення основних принципів її формування та функціонування, які повинні відповідати умовам сучасного інформаційного суспільства та основним викликам і загрозам сьогодення. Зазначені принципи є основними положеннями, які визначають напрями побудови і функціонування системи інформаційної безпеки, а також які повинні лягти основу діяльності всіх системи.

О. Олійник визначив принципи формування і забезпечення функціонування системи інформаційної безпеки як системоутворюючого фактору всіх складових національної безпеки, норм і правил поведінки громадян, державних і суспільних інститутів України у цій сфері [14]. Серед них:

- пріоритет прав, свобод і законних інтересів людини і громадянина;
- верховенство права, рівність усіх суб'єктів правовідносин перед законом;
- відповідальність держави перед людиною за свою діяльність;
- комплексний підхід до вирішення завдань забезпечення інформаційної безпеки;
- єдність і взаємозв'язок напрямів забезпечення інформаційної безпеки;
- розмежування сфер відповідальності й повноважень державних органів і органів місцевого самоврядування з питань забезпечення інформаційної безпеки;
- участь у міжнародних і регіональних системах інформаційної безпеки;
- оперативність, своєчасність, превентивність і адекватність заходів щодо попередження і захисту від зовнішніх інформаційних загроз та нейтралізації джерел внутрішніх інформаційних загроз.

Висновки. Дослідження наукових підходів щодо визначення сутності та основних елементів системи забезпечення інформаційної безпеки засвідчили відсутність єдиного підходу до розуміння зазначених категорій.

Нові виклики та загрози, спричинені агресією російської федерації проти України зумовлюють необхідність постійних динамічних змін та трансформацій системи забезпечення інформаційної безпеки та її елементів, до яких входять суб'єкти державного та недержавного рівнів, об'єкти забезпечення, механізми та заходи, запорукою ефективного функціонування зазначених елементів є дотримання відповідних принципів забезпечення інформаційної безпеки.

Література

1. Правові засади інформаційної безпеки України: монографія / П.Д. Біленчук, Л.В. Борисова, І.М. Неклонський., В.О. Собина; за ред. П.Д. Біленчука. Харків, 2018. 289 с. URL: http://repositsc.nuczu.edu.ua/handle/123456789/18077 (дата звернення: 03.12.2023).
2. Шемчук В.В. Механізм забезпечення інформаційної безпеки держави: теоретично-методологічні основи. *Філософські та методологічні проблеми права.* 2019. № 1. С. 51-59. URL: http://nbuv.gov.ua/UJRN/Fmpp_2019_1_8 (дата звернення: 05.12.2023).
3. 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.
4. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: дис. ... д-ра юрид. наук: 12.00.07. Ужгород, 2019. 487 с.
5. Перун Т.С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні: дис. … канд. юрид. наук: 12.00.07. Львів, 2019. 268 с.

6. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.
7. Академічний тлумачний словник української мови. URL: https://sum.in.ua/s/systema (дата звернення: 05.12.2023).
8. *Oxford English Dictionary: вебсайт.* URL: https://www.oed.com/search/dictionary/?scope=Entries&q=system (дата звернення: 05.12.2023).
9. Мигаль М. Розвиток громадянського суспільства в умовах війни: рекомендації для міжнародних партнерів. *Інститут аналітики та адвокації.* 2023. URL: https://iaa.org.ua/articles/civil-society-development-in-times-of-war-recommendations-for-international-partners/ (дата звернення: 08.12.2023).
10. Опалько Ю.В. Участь громадських об'єднань у протидії інформаційній агресії рф: аналітична записка НІІСД. *Національний інститут стратегічних досліджень: вебсайт.* 25 с. URL: https://niss.gov.ua/sites/default/files/2016-09/AZ-Protid-ya--nformagres---166e3.pdf (дата звернення: 08.12.2023).
11. Сіпайло Л.Г., Сіпайло Н.А. Діяльність неурядових організацій у системі забезпечення інформаційної безпеки країни. *Глобальні та національнальні проблеми економіки: електронне наукове фахове видання. Миколаївський національний університет імені В.О. Сухомлинського.* 2017. Вип. 18. С. 296-299. URL: http://socrates.vsau.org/repository/getfile.php/14423.pdf (дата звернення: 09.12.2023).
12. Захаренко К. Ефективність використання потенціалу недержавних суб'єктів інформаційної безпеки. *Нова парадигма.* 2015. Вип. 127. С. 40-53.

13. Довгань О.Д., Ткачук Т.Ю. Система інформаційної безпеки України: онтологічні виміри. *Інформація і право.* 2018. № 1(24). С. 89-103.
14. Олійник О. В. Принципи забезпечення інформаційної безпеки України. *Юридичний вісник. Повітряне і космічне право.* 2016. № 4. С. 72-78. URL: http://nbuv.gov.ua/UJRN/Npnau_2016_4_14 (дата звернення: 09.12.2023).

References

1. Bilenchuk, P.D., Borysova, L.V., Neklonskyi, I.M., & Sobyna, V.O. (2018). Pravovi zasady informatsiinoi bezpeky Ukrainy: monohrafiia [Legal principles of information security of Ukraine: monograph]. Bilenchuk P.D. (Eds.). Kharkiv. Retrieved from http://repositsc.nuczu.edu.ua/handle/123456789/18077 [in Ukrainian].
2. Shemchuk, V.V. (2019). Mekhanizm zabezpechennia informatsiinoi bezpeky derzhavy: teoretychno-metodolohichni osnovy [The mechanism of ensuring the information security of the state: theoretical and methodological foundations]. *Filosofski ta metodolohichni problemy prava, 1,* 51-59. Retrieved from http://nbuv.gov.ua/UJRN/Fmpp_2019_1_8 [in Ukrainian].
3. Tykhomyrov, O.O. (2014). Zabezpechennia informatsiinoi bezpeky yak funktsiia suchasnoi derzhavy: monohrafiia [Ensuring information security as a function of the modern state: monograph]. R. A. Kaliuzhnyi (Eds.). Tsentr navch.-nauk. ta nauk.-prakt. vyd. NA SB Ukrainy [in Ukrainian].
4. Tkachuk, T.Yu. (2019). Zabezpechennia informatsiinoi bezpeky v umovakh yevrointehratsii Ukrainy [Ensuring information security in the conditions of European integration of Ukraine]. *Doctor's thesis*. Uzhhorod [in Ukrainian].
5. Perun, T.S. (2019). Administratyvno-pravovyi mekhanizm zabezpechennia informatsiinoi bezpeky v Ukraini [Administrative and legal mechanism for

ensuring information security in Ukraine]. *Candidate's thesis.* Lviv [in Ukrainian].

6. Nashynets-Naumova, A.Iu. (2017). Informatsiina bezpeka: pytannia pravovoho rehuliuvannia: monohrafiia [Information security: issues of legal regulation: monograph]. Kyiv: Vydavnychyi dim «Helvetyka» [in Ukrainian].
7. Akademichnyi tlumachnyi slovnyk ukrainskoi movy [Academic explanatory dictionary of the Ukrainian language]. Retrieved from https://sum.in.ua/s/systema [in Ukrainian].
8. *Oxford English Dictionary: vebsait.* Retrieved from https://www.oed.com/search/dictionary/?scope=Entries&q=system
9. Myhal, M. (2023). Rozvytok hromadianskoho suspilstva v umovakh viiny: rekomendatsii dlia mizhnarodnykh partneriv [Development of civil society in conditions of war: recommendations for international partners]. *Instytut analityky ta advokatsii.* Retrieved from https://iaa.org.ua/articles/civil-society-development-in-times-of-war-recommendations-for-international-partners/ [in Ukrainian].
10. Opalko, Yu.V. Uchast hromadskykh obiednan u protydii informatsiinii ahresii rf: analitychna zapyska NIISD [Participation of public associations in countering informational aggression of the Russian Federation: Analytical note of NIISD]. *Natsionalnyi instytut stratehichnykh doslidzhen: vebsait.* Retrieved from https://niss.gov.ua/sites/default/files/2016-09/AZ-Protid-ya--nformagres---166e3.pdf [in Ukrainian].
11. Sipailo, L.H., & Sipailo, N.A. (2017). Diialnist neuriadovykh orhanizatsii u systemi zabezpechennia informatsiinoi bezpeky krainy [Activities of non-governmental organizations in the country's information security system]. *Hlobalni ta natsionalnalni problemy ekonmiky: elektronne naukove fakhove vydannia. Mykolaivskyi natsionalnyi universytet imeni V.O.*

Sukhomlynskoho, 18, 296-299. Retrieved from http://socrates.vsau.org/repository/getfile.php/14423.pdf [in Ukrainian].

12. Zakharenko K. (2015). Efektyvnist vykorystannia potentsialu nederzhavnykh subiektiv informatsiinoi bezpeky [The effectiveness of using the potential of non-state subjects of information security]. *Nova paradyhma, 127*, 40-53 [in Ukrainian].
13. Dovhan, O.D., & Tkachuk, T.Iu. (2018). Systema informatsiinoi bezpeky Ukrainy: ontolohichni vymiry [Information security system of Ukraine: ontological dimensions]. *Informatsiia i parvo, 1*(24), 89-103 [in Ukrainian].
14. Oliinyk, O. V. (2016). Pryntsypy zabezpechennia informatsiinoi bezpeky Ukrainy [Principles of ensuring information security of Ukraine]. *Yurydychnyi visnyk. Povitriane i kosmichne parvo, 4,* 72-78. Retrieved from http://nbuv.gov.ua/UJRN/Npnau_2016_4_14 [in Ukrainian].