

Теорія та історія державного управління

УДК 351

Палій Світлана Анатоліївна

головний фахівець

відділення організації освітнього процесу заочної форми навчання

Міжрегіональна Академія управління персоналом

Палий Светлана Анатольевна

главный специалист

отделения организации образовательного процесса заочной формы обучения

Межрегиональная Академия управления персоналом

Paliy Svitlana

Chief Specialist

department of organization of the educational process of distance learning

Interregional Academy of Personnel Management

ORCID: 0000-0002-9265-6407

**ТЕОРЕТИЧНІ ЗАСАДИ ФУНКЦІОНУВАННЯ ДЕРЖАВНОЇ
ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ФУНКЦИОНИРОВАНИЯ
ГОСУДАРСТВЕННОЙ ПОЛИТИКИ В СФЕРЕ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
THEORETICAL FUNDAMENTALS OF FUNCTIONING OF STATE
POLICY IN THE FIELD OF INFORMATION SECURITY**

Анотація. Аналіз теоретичних основ розроблення та функціонування державної політики у сфері інформаційної безпеки дав змогу дійти висновку, що у вітчизняних наукових колах дослідженням даного питання та проблем вдосконалення механізмів забезпечення безпеки в інформаційному просторі займалися значна кількість науковців,

зокрема: С. Горова, Н. Грабар, М. Гуцалюк, А. Турчак, Я. Чмир та інші. Разом з тим, обгрунтовано, що у науці публічного управління, на сьогоднішній день, не існує уніфікованого визначення поняття «державна політика сфери забезпечення безпеки в інформаційному просторі», адже розкриття сутності даної категорії у сучасній науковій думці не досить детальне.

Обгрунтовано думку про те, що політику держави у сфері забезпечення безпеки інформаційного простору можна окреслити як специфічне комплексне явище у суспільстві, яке включає велику кількість складових різних напрямів (економічного, зовнішньополітичного, військового, технологічного та інших характерів). У даному концепті, діяльність органів публічної влади має бути направлена на створення сприятливих умов для реалізації заходів держави з метою забезпечення високого рівня безпеки в інформаційному середовищі країни.

Доведено думку про те, що державно-правовий механізм публічного адміністрування у сфері забезпечення безпеки інформаційного простору держави виступає як цілісна система органів публічної влади та спеціальних установ, які окреслюють нормативно-правове поле даного напрямку та здійснюють ефективне регулювання економічних, фінансово-господарських та суспільних відносин між суб'єктами у сфері забезпечення безпеки інформаційного простору та захисту інформаційних даних.

Відмічено, що організаційно-правовий механізм публічного адміністрування у сфері забезпечення безпеки інформаційного простору держави дає можливість для узгодження процесів розроблення нормативно-правової бази відповідно до сучасного прогресу та розвитку інформаційних технологій у світі, а, також, створення алгоритму дій органів публічної влади щодо реалізації ефективної державної політики у

сфері інформаційної безпеки держави, з урахуванням необхідних ресурсів та шляхом здійснення функції контролю за їх використанням.

Ключові слова: державна політика у сфері інформаційної безпеки, структура інформаційної сфери, гарантування конституційних прав, використання комп'ютерних мереж, засекречування інформації.

Аннотація. Анализ теоретических основ разработки и функционирования государственной политики в сфере информационной безопасности позволил сделать вывод, что в отечественных научных кругах исследованием данного вопроса и проблем совершенствования механизмов обеспечения безопасности в информационном пространстве занимались значительное количество ученых, в частности: С. Горовая, Н. Грабарь, М. Гуцалюк, А. Турчак, Я. Чмырь и другие. Вместе с тем, обоснованно, что в науке публичного управления, на сегодняшний день, не существует унифицированного определения понятия «государственная политика в сфере обеспечения безопасности в информационном пространстве», ведь раскрытие сущности данной категории в современной научной мысли есть недостаточно детальным.

Обосновано мнение о том, что политику государства в сфере обеспечения безопасности информационного пространства можно определить как специфическое комплексное явление в обществе, которое включает большое количество составляющих различных направлений (экономического, внешнеполитического, военного, технологического и других характеров). В данном концепте, деятельность органов публичной власти должна быть направлена на создание благоприятных условий для реализации мер государства с целью обеспечения высокого уровня безопасности в информационной среде страны.

Доказано мнение о том, что государственно-правовой механизм публичного администрирования в сфере обеспечения безопасности

информационного пространства государства выступает как целостная система органов публичной власти и специальных учреждений, который определяют нормативно-правовое поле данного направления и осуществляют эффективное регулирование экономических, финансово-хозяйственных и общественных отношений между субъектами в сфере обеспечения безопасности информационного пространства и защиты информационных данных.

Отмечено, что организационно-правовой механизм публичного администрирования в сфере обеспечения безопасности информационного пространства государства дает возможность для согласования процессов разработки нормативно-правовой базы в соответствии с современным прогрессом и развитием информационных технологий в мире, а также, создания алгоритма действий органов публичной власти по реализации эффективной государственной политики в сфере информационной безопасности государства, с учетом необходимых ресурсов и путем осуществления функции контроля за их использованием.

Ключевые слова: *государственная политика в сфере информационной безопасности, структура информационной сферы, обеспечения конституционных прав, использование компьютерных сетей, засекречивание информации.*

Summary. *The analysis of theoretical bases of development and functioning of the state policy in the field of information security has allowed to come to a conclusion that in domestic scientific circles the research of the given question and problems of perfection of mechanisms of maintenance of safety in information space was engaged by a considerable quantity of scientists, in particular: S. Gorova, N. Grabar, M Gutsalyuk, A. Turchak, J. Chmyr and others. At the same time, it is substantiated that in the science of public administration, today, there is no unified definition of "state policy in the field of*

security in the information space", because the disclosure of this category in modern scientific thought is not detailed enough.

The opinion is substantiated that the state policy in the field of information space security can be defined as a specific complex phenomenon in society, which includes a large number of components of different directions (economic, foreign policy, military, technological and other). In this concept, the activities of public authorities should be aimed at creating favorable conditions for the implementation of state measures to ensure a high level of security in the information environment of the country.

The opinion is proved that the state-legal mechanism of public administration in the field of ensuring the security of the information space of the state acts as a holistic system of public authorities and special institutions that outline the legal field in this area and effectively regulate economic, financial, economic and social relations. between subjects in the field of information space security and information data protection.

It is noted that the organizational and legal mechanism of public administration in the field of information security of the state provides an opportunity to coordinate the development of regulatory framework in accordance with modern progress and development of information technology in the world, as well as creating an algorithm for public authorities to implement effective state policy in the field of information security of the state, taking into account the necessary resources and by exercising the function of control over their use.

Key words: *state policy in the field of information security, structure of the information sphere, guarantee of constitutional rights, use of computer networks, classification of information.*

Постановка проблеми. У процесі формування сучасного інформаційного суспільства в міжнародному просторі, інформація

виступає як вирішальний фактор розвитку цивілізації, який здійснює активний вплив на всі сфери людського життя та створює нове розуміння ролі інформаційних ресурсів в ньому. За умови глобалізаційних змін різноманітних інформаційних ресурсів, відбуваються важливі процеси у суспільному житті, такі як: інтеграція національних інформаційних систем у єдину міжнародну інформаційну систему, формування єдиного простору інформаційних ресурсів, виникнення міжнародних інформаційно-телекомунікаційних мереж, активізація введення інноваційних інформаційних технологій у різноманітні сфери людського життя.

Забезпечення безпеки в інформаційному просторі будь-якої сучасної держави розглядається як її пріоритетна мета та виступає ключовою передумовою її стабільного розвитку у різних напрямках. Маємо вказати на той факт, що недосконалості механізмів забезпечення безпеки в інформаційному просторі держави призводять до виникнення суттєвих системних збоїв у соціально-політичній, економічній, техногенній та інших сферах життєдіяльності суспільства. Така ситуація, у свою чергу, може призвести до зниження ефективності діяльності органів публічної влади будь-якої країни та виконання покладених на них функцій. У даному ракурсі, для України надзвичайно важливим залишається вирішення питань підвищення результативності діяльності органів публічної влади у галузі забезпечення безпеки в інформаційному просторі [1].

Аналіз останніх досліджень і публікацій. У вітчизняних наукових колах дослідженням питань визначення сутності поняття «інформаційна безпека» та проблем вдосконалення механізмів забезпечення безпеки в інформаційному просторі займається велика кількість науковців, зокрема, пропонуємо виділити науковий доробок таких авторів, як: С. Горова, Н. Грабар, М. Гуцалюк, А. Турчак, Я. Чмир та інші.

Разом з тим, на сьогодні, актуальним питанням залишається всебічне розкриття категоріально-понятійного апарату політики держави у сфері

забезпечення безпеки в інформаційному просторі. Це, у свою чергу, передбачає здійснення ґрунтовного аналізу низки наукових поглядів вітчизняних авторів галузі публічного адміністрування щодо визначення базових теоретичних засад, основних категорій і термінів політики держави у галузі інформаційної безпеки, а, також, найпоширеніших наукових підходів до їх класифікації.

Мета статті – дослідження науково-теоретичного обґрунтування засад функціонування державної політики у сфері інформаційної безпеки.

Виклад основного матеріалу. У контексті наукових поглядів М. Криштанович [2, с. 251], в області науки публічного адміністрування, політика держави у сфері забезпечення безпеки інформаційного простору визначається як діяльність держави з реалізації комплексу заходів з метою забезпечення захисту власного інформаційного середовища, входження країни у міжнародний інформаційний простір, визначення причин дискримінацій у інформаційній сфері даної країни та їх усунення, ліквідації, або мінімізації, недопущення порушення національного інформаційного середовища та здійснення інформаційної експансії з боку зарубіжних держав, розроблення та застосування спеціальних засобів та методів для підвищення ефективності діяльності держави щодо зберігання, використання та поширення інформаційних даних загальнонаціонального значення, а, також, з метою формування ефективної інформаційної інфраструктури та її стабільного розвитку.

Вважаю, доволі широким дане визначення автора та додамо, що політика держави у сфері забезпечення безпеки інформаційного простору окреслена як процес забезпечення інформаційного суверенітету держави та захисту інформаційного середовища від виникнення внутрішніх та зовнішніх загроз даного напрямку.

Зважаючи на твердження М. Гаврильціва [3, с. 201], зазначимо, що політика держави у сфері забезпечення безпеки інформаційного простору

виступає як реалізація державою послідовних заходів з метою вирішення важливих завдань економічного, військово-політичного, соціального та інших напрямів в інформаційній сфері.

На мій погляд, політику держави у сфері забезпечення безпеки інформаційного простору можна окреслити як специфічне комплексне явище у суспільстві, яке включає велику кількість складових різних напрямів (економічного, зовнішньополітичного, військового, технологічного та інших характерів). У даному концепті, діяльність органів публічної влади має бути направлена на створення сприятливих умов для реалізації заходів держави з метою забезпечення високого рівня безпеки в інформаційному середовищі країни.

З наукової точки зору Є. Архипова та А. Черниченко, політика держави у сфері забезпечення безпеки інформаційного простору виступає як важливий процес, який направлений на розвиток організаційно-технічних компонентів та нормативної бази даного напрямку. Тож, забезпечення безпеки в інформаційному середовищі будь-якої держави – вектор діяльності органів публічної влади на основі норм чинного законодавства та міжнародного права [4, с. 233].

На мою думку, такий напрям діяльності держави відіграє ключову роль у функціонуванні системи забезпечення безпеки як кожного громадянина та суспільства, так і у процесі забезпечення національної безпеки, в цілому.

У деяких публікаціях поняття «політика держави у сфері забезпечення безпеки інформаційного простору» визначається пріоритетністю інтересів держави загальнонаціонального значення, можливістю виникнення інформаційних загроз і небезпек та реалізується згідно з державними програмами, концепціями та стратегіями інформаційної сфери, враховуючи положення чинного законодавства. Представником такого підходу виступає Я. Малик [5, с. 14].

На мою думку, реалізація політики держави у сфері забезпечення безпеки інформаційного простору базується на процесах прийняття ефективних управлінських рішень представниками органів публічної влади та, відповідно, затвердженні нормативно-правових актів даного напрямку, які регулюють інформаційні відносини та формують конкретні механізми контролю за дотриманням таких норм.

У контексті наукових поглядів О. Кириченка в області державно-управлінської науки, для ефективного забезпечення безпеки в інформаційному просторі будь-якої держави необхідне створення та впровадження уніфікованої системи економічної безпеки загальнонаціонального значення, а, також, механізму її реалізації на основі принципів комплексності, системності, спрямованості, єдності, безперервності тощо. З урахуванням змін у внутрішньому та зовнішньому середовищі, виникненням нових загроз та викликів, вищезазначений механізм, також, має постійно змінюватись та адаптуватись до зовнішніх змін, перебувати під постійним контролем, з метою досягнення повної відповідності постійно зростаючим вимогам сучасного світу та процесам розвитку інформаційного суспільства [6, с. 22].

Маю зазначити, що у процесі визначення понятійно-категоріального апарату забезпечення інформаційної безпеки, необхідно, також, розглянути сутність різних механізмів публічного адміністрування у сфері інформаційної безпеки.

Визначаючи сутність державно-правового механізму публічного адміністрування у сфері забезпечення безпеки інформаційного простору держави, О. Федорук розкриває його як комплекс дій системи відповідальних органів публічної влади держави, який направлений на створення належних та сприятливих умов для реалізації результативної державної інформаційної політики [6, с. 24].

На мою думку, державно-правовий механізм публічного адміністрування у сфері забезпечення безпеки інформаційного простору держави виступає як цілісна система органів публічної влади та спеціальних установ, які окреслюють нормативно-правове поле даного напрямку та здійснюють ефективне регулювання економічних, фінансово-господарських та суспільних відносин між суб'єктами у сфері забезпечення безпеки інформаційного простору та захисту інформаційних даних.

Організаційно-правовий механізм публічного адміністрування у сфері забезпечення безпеки інформаційного простору держави, у трактуванні А. Сліпчука, представляє собою впорядковану систему органів публічної влади держави, які відповідають за реалізацію дієвої політики із забезпечення інформаційної безпеки, при цьому, зовнішні та внутрішні взаємозв'язки між суб'єктами таких відносин регулюються системою законодавчих норм. Складовою організаційно-правового механізму публічного адміністрування у сфері забезпечення безпеки інформаційного простору держави, у даному концепті, виступає сукупність органів публічної влади та інститутів громадянського суспільства, які відповідальні за реалізацію процесів формування та впровадження політики держави із забезпечення інформаційної безпеки.

Іншим важливим компонентом державної політики у даному напрямі є сукупність правових відносин між суб'єктами, які виникають у процесі реалізації національної політики держави із забезпечення інформаційної безпеки, а, також, комплекс методів та алгоритмів дій представників органів публічної влади держави, які використовують їх з метою підвищення ефективності реалізації державної політики даної сфери. Правове складова даного механізму включає в себе ієрархічну систему законодавчих принципів та норм, на основі яких здійснюється

регулювання діяльності державних та громадських інституцій з метою забезпечення безпеки в інформаційному просторі держави [7, с. 7].

На мою думку, організаційно-правовий механізм публічного адміністрування у сфері забезпечення безпеки інформаційного простору держави включає процеси створення системи організаційно-управлінських заходів з метою реалізації ключових положень стратегії національної безпеки держави та розроблення шляхів удосконалення законодавчої бази держави у сфері забезпечення інформаційної безпеки, затвердження оптимальної системи оцінювання рівня інформаційної безпеки держави, а, також, створення дієвих механізмів саморегуляції процесів забезпечення безпеки в інформаційному просторі.

У свою чергу, організаційно-правовий механізм публічного адміністрування у сфері забезпечення безпеки інформаційного простору держави, на думку В. Панченка, виступає як впорядкована система органів публічної влади, відповідальних за реалізацію процесів формування та провадження державної політики у сфері інформаційної безпеки [8, с. 105].

На мою думку, організаційно-правовий механізм публічного адміністрування у сфері забезпечення безпеки інформаційного простору держави дає можливість для узгодження процесів розроблення нормативно-правової бази відповідно до сучасного прогресу та розвитку інформаційних технологій у світі, а, також, створення алгоритму дій органів публічної влади щодо реалізації ефективної державної політики у сфері інформаційної безпеки держави, з урахуванням необхідних ресурсів та шляхом здійснення функції контролю за їх використанням.

Визначаючи зміст інституційного механізму публічного адміністрування у сфері забезпечення безпеки інформаційного простору держави, Н. Грабар розкриває його як особливий структурний компонент механізму держави, який забезпечує дотримання нормативних норм та загальних правил поведінки, за допомогою чого здійснюється регулювання

взаємовідносин різних економічних суб'єктів у інформаційному середовищі з метою попередження виникнення загроз інформаційній безпеці держави [9, с. 168; 10].

На мою думку, інституційний механізм публічного адміністрування у сфері забезпечення безпеки інформаційного простору держави передбачає формування системи відповідальних органів публічної влади, які забезпечують реалізацію заходів із інформаційної безпеки держави на основі законодавчо-встановлених норм, а, також, визначають напрями удосконалення даного механізму з урахуванням змін у зовнішньому середовищі та адаптаційних параметрів сучасного розвитку інформаційних технологій з метою підвищення рівня результативності заходів з протидії виникнення загрозам інформаційній безпеці держави.

Висновки. Отже, здійснивши ґрунтовний аналіз низки вітчизняних наукових досліджень проблематики публічного адміністрування у сфері забезпечення безпеки інформаційного простору держави, можна вказати на наявність широкого спектру підходів до розкриття категоріальної сітки державної політики у сфері забезпечення інформаційної безпеки. Такі відмінності у наукових думках різних авторів можна пояснити наявністю різних тлумачень щодо пріоритетного розвитку національної безпеки, в тому числі, інформаційної та кібер-безпеки.

Література

1. EISAS – European Information Sharing and Alerting System : Deployment Feasibility Study // European Union Agency for Network and Information Security, 2013. 26 p.
2. Криштанович М. Ф. Механізми державної політики України щодо забезпечення національної безпеки // Публічне управління та митне адміністрування. 2019. № 3 (22). С. 248-253.

3. "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" : Communication of the European Communities, Brussels, Belgium, 30.03.2009. EUR-Lex: веб-сайт. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52009DC0149> (дата звернення: 13.01.2019).
4. Архипова Є. О., Черниченко А. В. Забезпечення інформаційної безпеки в органах державної влади як нагальна потреба сьогодення // Держава та регіони. Серія: Державне управління. 2018. № 4(64). С. 231-234.
5. Малик Я. Й. Інформаційна безпека України: стан та перспективи розвитку // Ефективність державного управління. 2015. Вип. 44(1). С. 13-20. URL: http://nbuv.gov.ua/UJRN/efdu_2015_44%281%29__3 (дата звернення: 11.01.2019).
6. Кириченко О. С. Концептуальні засади формування системи забезпечення інформаційної безпеки держави // Вчені записки Університету «КРОК». 2018. № 49. С. 19-26.
7. Узбстер Ф. Теории информационного общества; перевод с английского М.В. Арапова, Н.В. Малыхиной. Москва: Аспект Пресс, 2004. 400 с.
8. Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision: Eurocommision, Brussels, Belguim, 30.09. 2010. EUR-Lex: веб-сайт. URL: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52010PC0517> (дата звернення: 22.02.2018).
9. Attacks against information systems: European Parliament legislative resolution, 4.07.2013. EUR-Lex: веб-сайт. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013R0540>

lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013AP0321 (дата звернення: 04.03.2018).

10. Romanenko E. Chaplai I. Public administration by the modern information technologies in Construction of Ukraine / I. Chaplay // Публічне урядування. 2017. №2 (7) травень 2017. С. 172-180.

References

1. EISAS – European Information Sharing and Alerting System : Deployment Feasibility Study // European Union Agency for Network and Information Security, 2013. 26 p.
2. Kryshchanovych M. F. Mekhanizmy derzhavnoji polityky Ukrainy shhodo zabezpechennja nacionaljnoji bezpeky // Publichne upravlinnja ta mytne administruvannja. 2019. # 3 (22). S. 248-253.
3. “Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience” : Communication of the European Communities, Brussels, Belgium, 30.03.2009. EUR-Lex: veb-sajt. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52009DC0149> (data zvernennja: 13.01.2019).
4. Arkhypova Je. O., Chernychenko A. V. Zabezpechennja informacijnoji bezpeky v orghanakh derzhavnoji vlady jak naghajna potreba sjoghodennja // Derzhava ta reghiony. Serija: Derzhavne upravlinnja. 2018. # 4(64). S. 231-234.
5. Malyk Ja. J. Informacijna bezpeka Ukrainy: stan ta perspektyvy rozvytku // Efektyvnistj derzhavnogho upravlinnja. 2015. Vyp. 44(1). S. 13-20. URL: http://nbuv.gov.ua/UJRN/efdu_2015_44%281%29__3 (data zvernennja: 11.01.2019).

6. Kyrychenko O. S. Konceptualjni zasady formuvannja systemy zabezpechennja informacijnoji bezpeky derzhavy // Vcheni zapysky Universytetu «KROK». 2018. # 49. S. 19-26.
7. Uebster F. Teorii informatsionnogo obshchestva; perevod s angliyskogo M.V. Arapova, N.V. Malykhinoy. Moskva: Aspekt Press, 2004. 400 s.
8. Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision: Eurocommision, Brussels, Belguim, 30.09. 2010. EUR-Lex: veb-sajt. URL: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52010PC0517> (data zvernennja: 22.02.2018).
9. Attacks against information systems: European Parliament legislative resolution, 4.07.2013. EUR-Lex: veb-sajt. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013AP0321> (data zvernennja: 04.03.2018).
10. Romanenko E. Chaplai I. Public administration by the modern information technologies in Construction of Ukraine / I. Chaplay // Publichne urjaduvannja. 2017. #2 (7) travenj 2017. S. 172-180.