

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА МОН УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА МОН УКРАЇНИ

Кваліфікаційна наукова праця
на правах рукопису

СЕМЕНЕНКО ІРИНА ОЛЕКСАНДРІВНА

УДК 351/354.072:004

ДИСЕРТАЦІЯ

**МЕХАНІЗМИ РЕАЛІЗАЦІЇ МЕРЕЖЕВОГО УПРАВЛІННЯ
У ДІЯЛЬНОСТІ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ**

Спеціальність 281 «Публічне управління та адміністрування»

Подається на здобуття ступеня доктора філософії

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

_____ І.О. Семененко

Науковий керівник – Карпенко Олександр Валентинович,
доктор наук з державного управління, професор

Київ – 2023

АНОТАЦІЯ

Семененко І. О. Механізми реалізації мережевого управління у діяльності органів державної влади. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 281 «Публічне управління та адміністрування». – Київський національний економічний університет імені Вадима Гетьмана, Київ, 2023.

У дисертаційній роботі здійснено теоретичне обґрунтування механізмів реалізації мережевого управління у діяльності органів державної влади та наданні практичних рекомендацій щодо їх удосконалення шляхом застосування інформаційно-комунікативних технологій.

Уперше розроблено процесну модель механізмів реалізації мережевого управління у діяльності органів державної влади, яка складається з мети, принципів функціонування (співпраці та партнерства, спільного прийняття рішень, децентралізації та автономії, горизонтальних та вертикальних зв'язків), факторів (політичної волі, вироблення державної політики, ресурсів та фінансування, розвитку інституційної культури, наявності кваліфікованих кадрів, міжнародних та геополітичних чинників, технологічних можливостей, готовності до змін), суб'єктів та об'єктів впливу (передбачає взаємодію між ними) та тристороннього алгоритму заходів практичного впровадження (фасилітації – залучення учасників до процесу для розуміння цілей їхньої участі, планування способів досягнення цих цілей і спільної роботи; координації – організації та синхронізації процесу спільної роботи всіх учасників для досягнення загальної мети; адміністрування – забезпечення виконання завдань, контролю, просування та підтримки функціонування мереж).

Удосконалено періодизацію еволюційних типів розвитку організаційних мереж, вважаючи їх початком лінійні, затим функціональні та

лінійно-функціональні мережі, згодом – дивізіональні та матричні; шляхом доповнення цього переліку новою організаційною структурою управління – мережевою, з огляду на стрімкий суспільний розвиток в умовах глобалізації та зростання інформаційно-комунікативних та цифрових зв'язків між органами державної влади та стейкхолдерами (беніфіціарами).

Також удосконалено підходи щодо застосування імітаційного (динамічного) моделювання ситуацій в мережевому управлінні шляхом імплементації адаптивних систем опису факторів та передумов виникнення можливих подій із використанням вихідних даних, що відображають умови і фактори прояву інформаційної окупації та подальшим аналізом негативного впливу зовнішньої пропаганди для визначення можливих наслідків, прийняття відповідних рішень органами державної влади та розробки відповідних заходів контрпропаганди з метою формування суспільної думки.

Окрім того, удосконалено класифікацію методів поширення інформації в соціальних мережах відповідно до загальних характеристик (розміщення інформації у власному співтоваристві або тематичному обліковому записі; промо-конкурси; спам – масове поширення інформації; несанкціоноване поширення повідомлень по «стінах» великих груп; розміщення платної контекстної реклами) шляхом виокремлення нової складової – методу добровільного поширення власної особистої та конфіденційної інформації, що стає об'єктом розвідки на основі відкритих джерел (OSINT).

В роботі набув подальшого розвитку понятійно-категорійний апарат публічного управління та адміністрування шляхом введення у науковий обіг нових дефініцій: «механізми реалізації мережевого управління у діяльності органів державної влади – норми, правила, інструменти, методи, підходи та процедури, які використовуються для впровадження і функціонування мережевих структур у процесі управління та прийняття рішень з метою забезпечення співпраці й взаємодії між різними зацікавленими сторонами (органами державної влади, громадськими організаціями та приватним сектором)» та «управління мережею в державному секторі – процес впливу

суб'єктів на об'єкти управління в межах організаційної мережі за допомогою відповідних механізмів (нормативно-правового, кадрового, організаційного, фінансово-економічного, технологічного, інформаційно-комунікативного та ін.) з метою досягнення запланованих результатів».

Також набув подальшого розвитку метод виявлення інформаційно-психологічних операцій у мережевому управлінні завдяки визначенню маркерів, які характеризують їх ознаки шляхом використання: соціально-загострених тем; нестандартної поведінки цільової аудиторії; інтуїтивних аргументів; стереотипів, узагальнень та кліше; дезінформації; спеціальних мовних конструкцій та експресивної лексики для виклику зайвих емоцій; соціальної інженерії (боти, фейкові профілі, штучні рейтинги та опитування в соціальних мережах); спеціальних технічних засобів («озвучення» або «підсвічування» певних фрагментів відео або аудіо контенту).

Доведено, що застосування технологій мережевої організації у державному управлінні дозволяє публічним службовцям краще адаптуватися до економічних, політичних та соціокультурних змін. У глобальному контексті мережева організація діяльності може сприяти співпраці між різними країнами та міжнародними організаціями для вирішення глобальних проблем, таких як зміна клімату, боротьба з пандемією, міграція та інші. Обґрунтовано, що на сучасному етапі відбувається новий період суспільного розвитку в умовах глобалізації та стрімко формується нова організаційна структура управління – мережева, розвиток якої став можливим завдяки зростанню інформаційно-комунікативних та цифрових зв'язків між органами державної влади, приватними компаніями та громадянами.

Виокремлено етапи формування правових механізмів мережевого управління у діяльності органів державної влади, які врегульовують суспільні відносини в інформаційній сфері та цифровізації, вироблення державної політики щодо взаємодії органів державної влади та інститутів громадянського суспільства, формування національного сегменту інтернет мережі та застосування цифрових технологій, право на інформацію та

реалізацію участі громадськості в державних справах, інструменти оприлюднення та поширення інформації про діяльність органів державної влади, розвиток громадянського суспільства, а також встановлення обмежень в інформаційній сфері у зв'язку із введенням воєнного стану в Україні.

Узагальнено зарубіжний досвід використання органами державної влади ситуаційних центрів як інституцій мережевого управління, діяльність яких спрямована на забезпечення національних інтересів країни та/чи безпеки міжнародної діяльності шляхом оперативного реагування на кризові виклики, ефективного прийняття рішень в сфері управління динамічними ситуаціями на основі виявлення та всебічного аналізу інформації щодо їх змін, а також прогнозування їх подальшого розвитку. В результаті чого визначено основні засади діяльності ситуаційних центрів у міжнародних міжурядових організаціях та об'єднаннях. Показано, що ситуаційні центри є інструментом постійного моніторингу, аналізу та оцінки даних, моделювання ситуацій для прийняття управлінських рішень в кризових ситуаціях, а також осередком здійснення результативної координації зусиль органів державної влади щодо протидії внутрідержавним чи міждержавним військовим конфліктам, політичним кризам, кіберзагрозам, пандемічним ситуаціям у випадку поширення хвороб, стихійним лихам, техногенним катастрофам, терористичним злочинам, загрозам стратегічної інфраструктури (зокрема, енергетичної, сільськогосподарської та ін.).

Застосування розробленої процесної моделі механізмів реалізації мережевого управління у діяльності органів державної влади здатне призвести до підвищення ефективності роботи органів державної влади через покращення координації та співпраці між ними та стейкхолдерами (беніфіціарами), що спричинить досягнення необхідних результатів у відповідності до поставлених цілей та потреб громадян; стимулюватиме залучення зацікавлених сторін до процесів державного управління і прийняття рішень; забезпечить розуміння потреб і очікувань громадськості; дозволить органам державної влади ефективно адаптуватися до змін в

політичному, економічному та соціокультурному середовищі; сприятиме впровадженню інновацій та креативності в роботі державних службовців.

Визначено сутність економічного механізму реалізації мережевого управління у діяльності органів державної влади, як такого, що передбачає узгодження процесів визначення їх потреб, акумулювання та використання необхідних ресурсів, а також оцінювання результатів їх роботи, що втілюються у створених ними продуктах та суспільних ефектах, які вони спричиняють, відповідно до визначених цілей та принципів. Обґрунтовано складові елементи економічного механізму реалізації мережевого управління у діяльності органів державної влади, якими є забезпечувальна та функціональна підсистеми ситуаційних центрів. Запропоновано алгоритм формування моделі процесу ресурсування ситуаційних центрів, яка передбачає виявлення ресурсних потреб ситуаційного центру, аналіз доступних джерел їх забезпечення та побудову відповідної системи ресурсного забезпечення, структура якої дозволяла б забезпечити успішне виконання завдань ситуаційного центру у відповідності до цілей державної політики, що реалізується відповідними органами державної влади.

Надано практичні рекомендації щодо застосування інформаційно-комунікативних технологій удосконалення мережевого управління у діяльності органів державної влади в умовах збройної агресії проти України, а саме:

- унормувати на законодавчому рівні механізми використання соціальних мереж органами державної влади як феномену інформаційного обміну, що дозволить аналізувати процес масової цифрової комунікації, здійснювати прогнозування громадської думки, виявляти приховані можливості маніпулювання й управління суспільною свідомістю, забезпечувати легітимність віртуальної комунікації для врахування висловлених пропозицій, зауважень, ініціатив тощо;

- імплементувати у державне управління адаптивні системи опису факторів та передумов виникнення можливих ситуацій за допомогою

імітаційного (динамічного) моделювання, завданням якого має бути визначення вихідних даних, що відображають умови і фактори виникнення інформаційної окупації задля розробки заходів щодо запобігання їх появі у майбутньому (застосування динамічного моделювання ситуацій із використанням вихідних даних та подальшим аналізом ситуацій щодо пропаганди є необхідним для визначення можливих наслідків прийнятих рішень щодо контрпропаганди та їх впливу на суспільну думку);

- застосувати організаційні механізми мережевого управління у якості інструментарію реалізації державної кіберполітики у сфері аналізу й оцінювання даних, а також наявних кіберзагроз для забезпечення взаємодії суб'єктів національної системи захисту критичної інфраструктури, професійного навчання та підвищення кваліфікації державних службовців;

- протидіяти інформаційно-психологічним операціям, які, застосовуючи переконання, маніпулювання емоціями, створення образу, ідентифікація причетності до певних спільнот, психологічний тиск, контроль за інформацією, спотворення соціальних норм, використовуються для впливу на державних службовців як суб'єктів мережевого управління шляхом своєчасного здійснення моніторингу, аналізу, оцінюванню та прогнозування факторів інформаційної загрози, а також застосуванню контрвпливу, спрямованого на поширення, упередження, знешкодження, або максимальне зниження наслідків таких операцій;

- запровадити аналітико-цифрові механізми адміністрування даними в мережевій структурі державного управління, у якості яких можуть виступати алгоритми та технології штучного інтелекту за рахунок розподіленого доступу й децентралізованого підходу до вирішення державно-управлінських завдань: аналіз даних та прогнозування, підтримка прийняття рішень, оптимізація адміністративних процесів, обробка запитів та звернень громадян, цифрова безпека, кіберзахист та боротьба з корупцією, моделювання та прогнозування ризиків, електронний документообіг та логістика даних тощо);

– стандартизувати технології застосування інтелектуальних агентів у державному секторі з метою вирішення проблеми непрозорості алгоритмів мережевого управління, що лежить у площині використання моделі інтерпретованого штучного інтелекту.

Практичне значення отриманих результатів дисертаційного дослідження полягає у виробленні пропозицій щодо вдосконалення механізмів реалізації мережевого управління у діяльності органів державної влади України.

Ключові слова: державне управління, мережеве управління, мережевий підхід, органи державної влади, ситуаційні центри, державно-приватне партнерство, цифровізація, цифрові трансформації, цифрова інфраструктура, соціальні мережі, штучний інтелект.

ABSTRACT

Semenenko I. O. Mechanisms for implementing network management in the activities of public authorities. – Qualification scientific work, manuscript.

Thesis for the Academic Degree of Doctor of Philosophy in specialty 281 “Public management and administration”. – Kyiv National Economic University named after Vadym Hetman, Kyiv, 2023.

In the dissertation, a theoretical justification of the mechanisms for implementing network management in the activities of public authorities and providing practical recommendations for their improvement through the use of information and communication technologies has been carried out.

For the first time, a process model of mechanisms for implementing network management in the activities of public authorities has been developed, which consists of the goal, principles of functioning (cooperation and partnership, joint decision-making, decentralization and autonomy, horizontal and vertical

links), factors (political will, development of state policy, resources and financing, development of institutional culture, availability of qualified personnel, international and geopolitical factors, technological capabilities, readiness for change), subjects and objects of influence (involves interaction between them) and a tripartite algorithm of practical implementation measures (facilitation - involving participants in the process to understand the goals of their participation, planning ways to achieve these goals and common work; coordination - organization and synchronization of the process of joint work of all participants to achieve a common goal; administration - ensuring the fulfilment of tasks, control, promotion and support of the networks functioning).

The periodization of evolutionary types of development of organizational networks has been improved, considering their starting point to be the linear type, then functional and linear-functional networks, subsequently - divisional and matrix ones; by supplementing this list with a new organizational management structure - a network, taking into account the rapid social development in the context of globalization and the growth of information, communication and digital connections between public authorities and stakeholders (beneficiaries).

Also the approaches to the use of simulation (dynamic) modelling of situations in network management has been improved by implementing of the adaptive systems for describing factors and prerequisites for the occurrence of possible events using the initial data, reflecting the conditions and factors of manifestation of informational occupation and further analysis of the negative impact of external propaganda in order to determine the possible consequences, making appropriate decisions by public authorities and developing appropriate counterpropaganda measures in order to form the public opinion.

In addition, the classification of methods for disseminating information in social networks has been improved in accordance with general characteristics (posting information in one's own community or thematic account; promotional contests; spamming, also known as the mass dissemination of information; unauthorized distribution of messages on the 'walls' of large groups; placement of

commercial contextual advertising) by identifying a new component - the method of voluntary dissemination of one's own personal and confidential information, which becomes the object of intelligence on the basis of open sources (OSINT), due to the fact, that users, in particular civil servants, independently freely compose their own personal 'dossiers' (autobiographical data, professional profile, personal preferences, location, lifestyle, presence in photos and videos, etc.) and in fact information about their close environment (list of contacts, official and family ties), which may pose a threat to national security in the context of armed aggression against Ukraine.

In the work, the conceptual and categorical apparatus of public management and administration was further developed by introducing new definitions into scientific circulation: 'mechanisms for implementing network management in the activities of public authorities - norms, rules, tools, methods, approaches and procedures used to implement and operate network structures in the process of management and decision-making in order to ensure cooperation and interaction between various stakeholders (public authorities, public organizations and the private sector)' and 'network management in the public sector - the process of influence of subjects on management objects within the organizational network through appropriate mechanisms (regulatory, personnel, organizational, financial, economic, technological, information and communication ones, etc.) in order to achieve the planned results'.

Also, the method of identifying information and psychological operations in network management has been further developed by identifying markers that characterize their features by using: socially aggravated topics; non-standard behaviour of the target audience; intuitive arguments; stereotypes, generalizations and clichés; misinformation; special language constructions and expressive vocabulary to evoke unnecessary emotions; social engineering (bots, fake profiles, artificial ratings and surveys in social networks); special technical means ('voicing' or 'highlighting' certain fragments of video or audio content).

It has been proved that the use of network organization technologies in public administration allows public servants to better adapt to economic, political and socio-cultural changes. In the global context, networking activities can facilitate cooperation between different countries and international organizations to address global issues such as climate change, pandemic control, migration and others. It has been substantiated that at the present stage there is a new period of social development in the conditions of globalization and a new organizational structure of management is rapidly being formed - a network, the development of which became possible due to the growth of information-communicative and digital connections between public authorities, private companies and citizens.

The stages of formation of legal mechanisms of network management in the activities of public authorities, regulating public relations in the information sphere and digitalization, development of state policy on the interaction of public authorities and civil society institutions, formation of the national segment of the Internet network and the use of digital technologies, the right to information and the realization of public participation in public affairs, tools for disclosure and dissemination of information on the activities of public authorities, development of civil society, as well as the establishment of restrictions in the information sphere in connection with the introduction of martial law in Ukraine.

It has been generalized the foreign experience of using situational centres by public authorities as institutions of network management, whose activities are aimed at ensuring the national interests of the country and/or the security of international activity through rapid response to crisis challenges, effective decision-making in the field of management of dynamic situations on the basis of identification and comprehensive analysis of information on their changes, as well as forecasting their further development. As a result, the basic principles for the situational centres' activities in the international intergovernmental organizations and associations have been determined. It has been shown that situational centres are tools for continuous monitoring, analysis and evaluation of data, as well as modelling of situations for making managerial decisions in the crisis situations, as

well as the foci of effective efforts coordination of state authorities to counter domestic or interstate military conflicts, political crises, cyber threats, pandemic situations in the occasion of the spread of diseases, natural disasters, man-made disasters, terrorist crimes, threats to strategic infrastructure (in particular, to power and agricultural ones).

The use of the process model of mechanisms for implementing network management in the activities of public authorities can lead to the increase in the efficiency of the work of public authorities by improving coordination and cooperation between them and stakeholders (beneficiaries), which will entail the achievement of the necessary results in accordance with the goals and needs of citizens; stimulate the involvement of stakeholders in the processes of public administration and decision-making; provide an understanding of the needs and expectations of the public; will allow public authorities to adapt effectively to changes in the political, economic and socio-cultural environment; will promote innovation and creativity in the work of civil servants.

The essence of the economic mechanism for the implementation of network management in the activities of public authorities has been determined as the one, which involves the harmonization of processes for determining their needs, accumulating and using the necessary resources, as well as evaluating the results of their work, which are embodied in the products they create and the social effects that they cause, in accordance with certain goals and principles. The components of the economic mechanism for the implementation of network management in the activities of public authorities, which are the supporting and functional subsystems of situational centres, have been substantiated. An algorithm for forming a model of the process of resourcing situational centres has been proposed, which involves identifying the resource needs of the situational centre, analysing the available sources of their provision and building an appropriate system of resource provision, the structure of which would ensure the successful implementation of the tasks of the situational centre in accordance with the goals of state policy implemented by the relevant public authorities.

Practical recommendations have been elaborated in the sphere of the use of information and communication technologies to improve network management in the activities of public authorities in the context of armed aggression against Ukraine, namely:

- to regulate at the legislative level the mechanisms of using social networks by public authorities as a phenomenon of information exchange, which will allow analysing the process of mass digital communication, predicting public opinion, identifying hidden opportunities for manipulating and managing public consciousness, ensuring the legitimacy of virtual communication to take into account the proposals, comments, initiatives, etc.;

- to implement adaptive systems for describing factors and preconditions for the occurrence of possible situations in public administration using simulation (dynamic) modelling, the task of which should be to determine the initial data reflecting the conditions and factors of the emergence of information occupation in order to develop measures to prevent their occurrence in the future (the use of dynamic modelling of situations using initial data and subsequent analysis of propaganda situations is necessary to determine the possible consequences of decisions made on counter-propaganda and their impact on public opinion);

- to apply organizational mechanisms of network management as tools for implementing state cyber policy in the field of data analysis and evaluation of the existing cyber threats to ensure interaction between the subjects of the national system for protecting critical infrastructure, vocational training and advanced training of civil servants;

- to counteract the information and psychological operations which, using beliefs, manipulating emotions, image creation, identifying involvement in certain communities, psychological pressure, control over information, distortion of social norms, are used to influence civil servants as subjects of network management by timely monitoring, analysis, evaluation and prediction of information threat factors, as well as the use of counter-influence aimed at spreading, preventing, neutralizing, or maximally reducing the consequences of such operations;

- to introduce analytical and digital mechanisms for data administration in the network structure of public administration, which may include the artificial intelligence driven algorithms and technologies, distributed access and decentralized approach to solving public management tasks: data analysis and forecasting, decision support, optimization of administrative processes, processing of requests and appeals of citizens, digital security, cyber defence and the fight against corruption, risk modelling and forecasting, electronic document management and data logistics, etc.);

- to standardize technologies for the use of intelligent agents in the public sector in order to solve the problem of opacity of network control algorithms, which lies in the plane of using the model of interpreted artificial intelligence.

The practical significance of the obtained results of the dissertation research is to develop proposals for improving the mechanisms for implementing network management in the activities of public authorities of Ukraine.

Key words: public administration, network management, network approach, public authorities, situational centres, public-private partnership, digitalization, digital transformation, digital infrastructure, social networks, artificial intelligence.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Статті у наукових фахових виданнях України

1. **Семененко І.О.** Правові механізми використання соціальних мереж у публічному управлінні. *Державне управління: теорія та практика* – електронне наук. фах. видання. Національна академія державного управління при Президентові України. 2019. № 2. С. 44-50. URL: <https://scholar.archive.org/work/3xi6h4loxrf5nnq2bdb636oqii/access/wayback/http://patp.academy.gov.ua/article/download/190046/189881> (0,63 д.а.).
2. **Семененко І.О.** Світовий досвід функціонування мережі ситуаційних центрів органів державної влади. *Державне управління: удосконалення та розвиток*. 2022. № 9. DOI: <https://doi.org/10.32702/2307-2156.2022.9.15> (1,1 д.а.).
3. Федірко Н.В., **Семененко І.О.** Економічний механізм забезпечення ситуаційного мережевого управління в діяльності органів державної влади в Україні. *Бізнес-Інформ*. 2023. № 10. DOI: <https://doi.org/10.32983/2222-4459-2023-10-86-94> (0,96 д.а., особисто автору 0,65 д.а., обґрунтовано зміст та структуру економічного механізму забезпечення функціонування ситуаційних центрів органів державної влади).
4. Осьмак А., Карпенко Ю., **Семененко І.** Використання інструментів штучного інтелекту в мережевому управлінні: переваги, ризики та розвиток. *Аспекти публічного управління*. 2023. № 11 (3). С. 38-42. URL: <https://aspects.org.ua/index.php/journal/article/view/1012>. DOI: <https://doi.org/10.15421/152333> (0,6 д.а., особисто автору – 0,45 д.а., визначено основні переваги, перспектив розвитку та ризиків застосування інструментів штучного інтелекту, як механізмів мережевого управління, а також надання практичних рекомендацій щодо підходів до розробки алгоритмів застосованих моделей та їхнього законодавчого регулювання).

В інших виданнях

5. **Семененко І.О.** Соціальні мережі як інструмент впливу на масову свідомість в умовах розвитку цифрового суспільства. *Публічне врядування в Україні: стан, виклики та перспективи розвитку* : матеріали щоріч. Всеукр. наук.-практ. конф. за міжнар. участю, присвяч. 100-річчю держ. служби в Україні, (Київ, 25 травня 2018 р.): у 5 т. / за заг. ред. В.С. Куйбіди, М.М. Білинської, О.М. Петроє. Київ: НАДУ, 2018. Т. 3. С. 117 – 119 (0,2 д.а.).

6. **Семененко І.О.** Роль цифрових комунікацій в публічному управлінні. *Теорія та практика публічного управління та адміністрування у XXI сторіччі*: матеріали I Всеукр. наук.-практ. конф. за міжнар. участю здобувачів вищої освіти та молодих вчених, (Київ, 30 листопада 2018 р.): за заг. ред. В.С. Куйбіди, О.М. Петроє, І.О. Дегтярьової. Київ: НАДУ, 2018. С. 309 – 311 (0,2 д.а.).

7. **Семененко І.О.** Реалізація мережевих технологій в публічному управлінні. *Альманах науки*. Науковий журнал. 2019. № 9 (30). С. 14 – 17 (0,15 д.а.).

8. **Семененко І.О.** Використання соціальних мереж в публічному управлінні. *Теорія та практика публічного управління та адміністрування у XXI сторіччі*: матеріали II Всеукр. наук.-практ. конф. за міжнар. участю здобувачів вищої освіти та молодих вчених, (Київ, 22 листопада 2019 р.): за заг. ред. М.М. Білинської, О.М. Петроє, І.О. Дегтярьової. Київ: НАДУ, 2019. С. 249 – 250 (0,16 д.а.).

9. **Semenenko I.O.** Sieci społecznościowe jako narzędzie do wdrażania decyzji zarządczych. *Cyfrowe instrumenty zarządzania publicznego: Ukraina – Polska: zbiór tez Dialogi zarządzania cyfrowego*. (Kijów, 27 listopada 2019 r.): kol. red.: O. Karpenko, M. Tenenbaum-Kulig, K. Gumenna. – Kijów, Wrocław: Narodowa Academia Administracji Publicznej przy Prezydencie Ukrainy, Uniwersytet Wrocławski, 2019. S. 80 – 83 (0,1 д.а.).

10. **Семененко І.О.** Соціальні мережі як цифровий інструмент маніпулювання свідомістю. *Україна 2030: публічне управління для сталого розвитку*: матеріали щоріч. міжнар. наук.-практ. конф., (Київ, 2020 р.): у 3 т. / за заг. ред. А.П. Савкова, М.М. Білинської, О.М. Петрось. Київ: НАДУ, 2020. Т. 2. – С. 128 – 130 (0,1 д.а.).

11. **Семененко І.О.** Оцінювання кібербезпеки: національний та глобальний виміри. *Кібербезпека державних інституцій та подолання кризових станів*: Матеріали I Міжнародної науково-практичної конференції (м. Київ, м. Вроцлав, 26 травня 2022 року). К.: ІСЗІ КПІ ім. Ігоря Сікорського, С.313-315 (0,15 д.а.).

12. **Семененко І.О.** Ситуаційне управління у формуванні інформаційної безпеки: досвід ЄС для України. Політичні технології пропаганди та контрпропаганди у російсько-українській війні. Матеріали Круглого столу за міжнародною участю (м. Київ, КНЕУ, 21 лютого 2023 р.). К.: КНЕУ, 2023. С. 145-148 (0,18 д.а.).

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ	19
ВСТУП.....	20
РОЗДІЛ 1 ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ФОРМУВАННЯ	
МЕРЕЖЕВОГО ПІДХОДУ У ДІЯЛЬНОСТІ ОРГАНІВ ДЕРЖАВНОЇ	
ВЛАДИ.....	28
1.1 Науковий дискурс застосування технологій мережевої організації	
в державному управлінні.....	28
1.2 Генеза правового формування механізмів мережевого управління у	
діяльності органів державної влади	46
1.3 Соціально-комунікативні імперативи реалізації мережевого управління	
Висновки до розділу 1	87
РОЗДІЛ 2 УКРАЇНСЬКИЙ ТА ЗАРУБІЖНИЙ ДОСВІД	
ЗАСТОСУВАННЯ МЕРЕЖЕВОГО УПРАВЛІННЯ	
У ДІЯЛЬНОСТІ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ.....	91
2.1 Практика організації мережевих структур державного управління в	
Україні	91
2.2 Зарубіжний досвід функціонування мережі ситуаційних центрів	
органів влади (на прикладі країн ЄС та США)	102
2.3 Процесна модель механізмів реалізації мережевого управління у	
діяльності органів державної влади	123
Висновки до розділу 2	139
РОЗДІЛ 3 РОЗВИТОК МЕХАНІЗМІВ МЕРЕЖЕВОГО УПРАВЛІННЯ	
У ДІЯЛЬНОСТІ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ УКРАЇНИ	145
3.1 Забезпечення розвитку економічного механізму реалізації мережевого	
управління у діяльності органів державної влади в Україні	145
3.2 Удосконалення інформаційно-комунікативних механізмів реалізації	
мережевого управління.....	162
3.3 Перспективи використання технологій штучного інтелекту в	
мережевому управлінні	170
Висновки до розділу 3	178
ВИСНОВКИ	183
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	189
ДОДАТКИ.....	216

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ІКТ	–	інформаційно-комунікативні технології;
КЕП	–	кваліфікаційний електроний підпис;
NCSI	–	National Cyber Security Index (Національний індекс кібербезпеки);
NAC	–	North Atlantic Council (Північноатлантична рада);
МС	–	Military Committee (Військовий комітет);
SAIT	–	Situational Awareness Integration Team (Група інтеграції ситуаційного моніторингу);
AKM	–	Administrative Support and Knowledge Management (Офіс адміністративної підтримки та управління знаннями);
ISAC	–	Information Sharing and Analysis Centres (Центри обміну та аналізу інформації);
NCI	–	National Council of ISACs (Національну раду центрів обміну та аналізу інформації);
EE-ISAC	–	The European Energy Information Sharing and Analysis Centre (Європейський центр обміну та аналізу інформації в сфері енергетики);
ІПСО	–	інформаційно-психологічні операції;
AI (ШІ)	–	штучний інтелект;
EXAI	–	Explainable artificial intelligence (Інтерпретований штучний інтелект).

ВСТУП

Актуальність теми. Сучасний етап розвитку та захисту української держави від збройної агресії РФ характеризується повсюдним застосуванням інформаційно-комунікативних та цифрових технологій у сфері публічного управління та адміністрування, що передбачає трансформацію всіх галузей суспільної діяльності для захисту національних інтересів України.

Необхідність забезпечення оперативної координації, швидкого обміну даними та зручності взаємодії між різними державними інституціями спричинює пошук нових парадигм організації публічного управління. Так, мережеве управління здатне стати дієвим інструментом для сучасних органів державної влади.

Проблематика мережевого управління стала об'єктом досліджень багатьох зарубіжних та українських вчених. Так К. Джонс, В. Хестерлі, С. Боргаті [165], Р. Абрамс [133], Є. Соренсен, Я. Торфінг [204] розглядали мережеву організацію як неформальну соціальну систему невеликих та гнучких самокерованих команд, що об'єднують обмежений, стійкий і структурований набір автономних установ, які займаються створенням продуктів або послуг, натомість Е. Клайн та Дж. Коппеня [168] уособлюють вирішення проблем державної політики через мережі та безпосередньо в них. Дослідженню принципів, технологій та секторальних особливостей розвитку мереж ситуаційних центрів присвячено праці таких науковців як М. Амановіч [136], А. Астіакопулос, А. Блум, В. Драгос, Р. Лежчина, В. Овенс, Н. Павлов, Т. Уолліс [208], Ф. Феррейра та ін. Питання мережевих технологій та комунікацій у державному управлінні досліджували такі науковці як В. Брижко, Т. Галіч [129], Н. Гудима, Г. Красноступ, Г. Почепцов [58], О. Якимчук [129] та ін. Значний внесок у дослідження концепцій мереж у різних сферах публічного управління внесли Н. Васюк [5], Л. Гаєвська [10] Т. Запорожець, О. Карпенко [27; 167; 124; 31; 30; 29], Я. Цимбаленко [120] та ін. Незважаючи на зростання ролі міжорганізаційних мереж як організаційної

форми публічного управління, сучасні вчені лише нещодавно почали досліджувати, яким чином та з якою ефективністю комунікативні підрозділи органів державної влади забезпечують координацію різних суб'єктів інституціональної мережі публічного управління з різними цілями, обов'язками та можливостями.

Аналіз стану розробленості цієї проблематики свідчить про значущість мережевого підходу для розвитку галузі публічного управління та адміністрування, що спонукає до формування нових, вдосконалення та розвитку існуючих механізмів реалізації мережевого управління у діяльності органів державної влади України. Потреба у вирішенні зазначених проблемних питань на науковому та практичному рівнях і зумовили вибір теми дослідження.

Зважаючи на швидкі зміни у сфері інформаційно-комунікативних технологій і їхній вплив на суспільство та державне управління, досліджувана тема є актуальною, привертає увагу науковців та практиків у галузі державного управління та потребує подальших наукових пошуків.

Актуальність теми дослідження зумовлена недостатністю теоретичного обґрунтування механізмів реалізації мережевого управління у діяльності органів державної влади та відсутністю практичних рекомендацій щодо їх удосконалення шляхом застосування інформаційно-комунікативних технологій, що не було предметом окремої дисертаційної роботи у галузі науки державного управління.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконана відповідно за комплексним науковим проєктом «Державне управління та місцеве самоврядування» (№ ДР 0199U002827) науково-дослідної роботи Національної академії державного управління при Президентові України «Сервісна діяльність органів публічної влади в умовах розвитку цифрового суспільства» (№ ДР 0119U101449), де автором узагальнено зарубіжний досвід цифрових трансформацій мережі ситуаційний центрів органів державної влади.

Мета і завдання дослідження. *Метою* дисертаційної роботи є теоретичне обґрунтування механізмів реалізації мережевого управління у діяльності органів державної влади та надання практичних рекомендацій щодо їх удосконалення шляхом застосування інформаційно-комунікативних технологій.

Досягнення визначеної мети зумовило вирішення таких *завдань*:

- розкрити сутність існуючих наукових розробок щодо застосування технологій мережевої організації у державному управлінні;
- визначити генезу правового формування механізмів реалізації мережевого управління у діяльності органів державної влади на основі аналізу законів та підзаконних актів України;
- узагальнити зарубіжний досвід використання органами державної влади ситуаційних центрів як інституцій мережевого управління;
- розробити процесну модель механізмів реалізації мережевого управління у діяльності органів державної влади та спрогнозувати наслідки її практичного впровадження;
- сформулювати сутність економічного механізму реалізації мережевого управління у діяльності органів державної влади та визначити складові його розвитку в контексті функціонування ситуативних центрів;
- надати практичні рекомендації щодо застосування інформаційно-комунікативних технологій удосконалення мережевого управління у діяльності органів державної влади в умовах збройної агресії проти України.

Об’єкт дослідження – мережеве управління у діяльності органів державної влади.

Предмет дослідження – механізми реалізації мережевого управління у діяльності органів державної влади.

Методи дослідження. У процесі досягнення мети та вирішення завдань дисертаційної роботи застосовувалися наступні наукові методи: аналізу, синтезу, індукції та дедукції – для розкриття сутності існуючих наукових розробок українських та зарубіжних вчених щодо застосування технологій

мережевої організації у державному управлінні; історико-правовий – при дослідженні генези правового формування механізмів мережевого управління в діяльності органів державної влади; теоретичного узагальнення – для узагальнення зарубіжного досвіду використання органами державної влади ситуаційних центрів як інституцій мережевого управління; систематизації, узагальнення та аналогії – для етапізації розвитку основних періодів розвитку організаційних мереж у державному управлінні; моделювання та абстракції – для логічно-схематичної побудови процесної моделі механізмів реалізації мережевого управління у діяльності органів державної влади; герменевтичний та порівняльний – для уточнення понятійно-категоріального апарату дослідження та визначенні нових дефініцій. Відбір наукової інформації за темою роботи здійснено шляхом комплексного аналізу літературних джерел, застосування статистичного методу. Інформаційну базу дисертаційного дослідження складають: закони та підзаконні акти України, США та країн ЄС, інформаційні, статистичні та аналітичні матеріали Міністерства цифрової трансформації України, Міністерства культури та інформаційної політики України, інтернет-джерела, праці українських і зарубіжних дослідників, результати власних досліджень.

Наукова новизна отриманих результатів полягає у здійсненні теоретичного обґрунтування механізмів реалізації мережевого управління у діяльності органів державної влади та наданні практичних рекомендацій щодо їх удосконалення шляхом застосування інформаційно-комунікативних технологій. Зокрема, у дисертації:

уперше:

- розроблено процесну модель механізмів реалізації мережевого управління у діяльності органів державної влади, яка складається з мети, принципів функціонування (співпраці та партнерства, спільного прийняття рішень, децентралізації та автономії, горизонтальних та вертикальних зв'язків), факторів (політичної волі, вироблення державної політики, ресурсів та фінансування, розвитку інституційної культури, наявності кваліфікованих

кадрів, міжнародних та геополітичних чинників, технологічних можливостей, готовності до змін), суб'єктів та об'єктів впливу (передбачає взаємодію між ними) та тристороннього алгоритму практичних заходів впровадження (*фасилітації* – залучення учасників до процесу для розуміння цілей їхньої участі, планування способів досягнення цих цілей і спільної роботи; *координації* – організації та синхронізації процесу спільної роботи всіх учасників для досягнення загальної мети; *адміністрування* – забезпечення виконання завдань, контролю, просування та підтримки функціонування мереж);

удосконалено:

- періодизацію еволюційних типів розвитку організаційних мереж, вважаючи їх початком *лінійні*, затим *функціональні* та *лінійно-функціональні* мережі, згодом – *дивізійні та матричні*, шляхом доповнення цього переліку новою організаційною структурою управління – *мережевою*, з огляду на стрімкий суспільний розвиток в умовах глобалізації та зростання інформаційно-комунікативних та цифрових зв'язків між органами державної влади та стейкхолдерами (беніфіцарами);

- підходи щодо застосування імітаційного (динамічного) моделювання ситуацій в мережевому управлінні шляхом імплементації адаптивних систем опису факторів та передумов виникнення можливих подій із використанням вихідних даних, що відображають умови і фактори прояву інформаційної окупації та подальшим аналізом негативного впливу зовнішньої пропаганди для визначення можливих наслідків, прийняття відповідних рішень органами державної влади та розробки відповідних заходів контрпропаганди з метою формування суспільної думки;

- класифікацію методів поширення інформації в соціальних мережах відповідно до загальних характеристик (розміщення інформації у власному співтоваристві або тематичному обліковому записі; промо-конкурси; спам – масове поширення інформації; несанкціоноване поширення повідомлень по «стінах» великих груп; розміщення платної контекстної реклами) шляхом

виокремлення нової складової – методу добровільного поширення власної, особистої та конфіденційної інформації, що стає об'єктом розвідки на основі відкритих джерел (OSINT), оскільки користувачі, зокрема державні службовці, самостійно у вільному доступі складають на себе «досьє» (автобіографічні дані, інформацію про професійну діяльність, власні уподобання, місцезнаходження, спосіб життя, присутність на фото та відео контенті тощо) та фактично інформацію про своє близьке оточення (список контактів, службові та родинні зв'язки), що може становити загрозу національній безпеці в умовах збройної агресії проти України;

набули подальшого розвитку:

– понятійно-категоріальний апарат дослідження шляхом введення у науковий обіг нових дефініцій: «механізми реалізації мережевого управління у діяльності органів державної влади – норми, правила, інструменти, методи, підходи та процедури, які використовуються для впровадження і функціонування мережевих структур у процесі управління та прийняття рішень з метою забезпечення співпраці й взаємодії між різними зацікавленими сторонами (органами державної влади, громадськими організаціями та приватним сектором)» та «управління мережею в державному секторі – процес впливу суб'єктів на об'єкти управління в межах організаційної мережі за допомогою відповідних механізмів (нормативно-правового, кадрового, організаційного, фінансово-економічного, технологічного, інформаційно-комунікативного та ін.) з метою досягнення запланованих результатів»;

– метод виявлення інформаційно-психологічних операцій у мережевому управлінні завдяки визначенню маркерів, які характеризують їх ознаки шляхом використання: соціально-загострених тем; нестандартної поведінки цільової аудиторії; інтуїтивних аргументів; стереотипів, узагальнень та кліше; дезінформації; спеціальних мовних конструкцій та експресивної лексики для виклику зайвих емоцій; соціальної інженерії (боти, фейкові профілі, штучні рейтинги та опитування в соціальних мережах);

спеціальних технічних засобів («озвучення» або «підсвічування» певних фрагментів відео або аудіо контенту).

Практичне значення отриманих результатів дисертаційного дослідження полягає у виробленні пропозицій щодо вдосконалення механізмів реалізації мережевого управління у діяльності органів державної влади України. Основні положення, висновки та рекомендації використано:

- у діяльності Департаменту захисту критичної інфраструктури Адміністрації Державної служби спеціального зв'язку та захисту інформації України, зокрема при розробленні проєкту постанови Кабінету Міністрів України «Про затвердження Плану взаємодії суб'єктів національної системи захисту критичної інфраструктури» враховано науково-обґрунтовані пропозиції дисертантки щодо застосування організаційних механізмів мережевого управління для забезпечення взаємодії суб'єктів національної системи захисту критичної інфраструктури в межах функцій та повноважень, визначених Законом України «Про критичну інфраструктуру» від 16 листопада 2021 року № 1882-IX (довідка № 07/01/02–7548/ВС від 17.11.2023);

- в навчальному процесі кафедри національної економіки та публічного управління Київського національного економічного університету імені Вадима Гетьмана при підготовці та викладанні навчальних дисциплін «Цифрові технології в публічному управлінні» та «Сервісна діяльність органів публічної влади», зокрема запропоновано науково-обґрунтовані підходи щодо досягнення максимального рівня ефективності діяльності ситуаційних центрів у сфері захисту критичної інфраструктури та реалізації кібербезпеки інформаційного середовища України (довідка № 103-л від 06.12.2022).

Особистий внесок здобувача. Дисертація є самостійною науковою працею, яка містить ідеї, висновки і пропозиції, які характеризуються науковою новизною і належать особисто авторці. У наукових працях,

опублікованих у співавторстві, використано тільки ті розробки, напрацювання та положення, які є результатом особистих досліджень авторки.

Апробація результатів дисертації. Основні положення та результати дисертаційної роботи оприлюднено авторкою на науково-практичних конференціях за міжнародною участю, а саме: «Публічне врядування в Україні: стан, виклики та перспективи розвитку» (Київ, 2018), «Теорія та практика публічного управління та адміністрування у XXI сторіччі» (Київ, 2018-2019), «Cyfrowe instrumenty zarządzania publicznego: Ukraina – Polska» (Київ-Вроцлав, 2019), «Україна 2030: публічне управління для сталого розвитку» (Київ, 2020), «Кібербезпека державних інституцій та подолання кризових станів» (Київ-Вроцлав, 2022) та «Політичні технології пропаганди та контрпропаганди у російсько-українській війні» (Київ, 2023).

Публікації. За результатами дослідження автором опубліковано самостійно й у співавторстві 12 наукових праць загальним обсягом 4,53 д. а. (особисто автору належать 4,07 д. а.), з них: 4 – у наукових фахових виданнях України, 8 – в інших виданнях.

Структура та обсяг дисертації. Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел і додатків. Загальний обсяг дисертаційної роботи становить 213 сторінок друкованого тексту. Робота містить 3 таблиці на 4 сторінках, 11 рисунків на 11 сторінках, 1 додаток на 1 сторінці. Список використаних джерел налічує 211 найменувань.

РОЗДІЛ 1

ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ФОРМУВАННЯ МЕРЕЖЕВОГО ПІДХОДУ У ДІЯЛЬНОСТІ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ

1.1 Науковий дискурс застосування технологій мережевої організації в державному управлінні

У сучасному технологічному та взаємопов'язаному світі мережева організація роботи для планування, проектування, розвитку послуг, розробки новітніх цифрових продуктів стала критично важливою як у державному, так і в приватному секторах, оскільки ефективність та результативність роботи суб'єктів управління більшою мірою стала залежати від якісної роботи мереж, аніж від окремих організаційних функцій. Державне управління усе частіше здійснюється у мережевому просторі, оскільки більшість країн тією чи іншою мірою децентралізовані, і значна кількість проблем виходять за межі адміністративних і географічних кордонів.

Мережі змінюють організаційний ландшафт сучасного державного управління. Світовий досвід засвідчує, що класична, вертикально організована система взаємодії між суб'єктами всередині держави обмежує можливості впровадження інноваційних технологій у практику управління та може спричинити уповільнення суспільно-політичного розвитку в сучасному динамічному середовищі. Пошук виходу з ситуації, що склалася, змушує сучасні уряди ухвалювати важливі рішення, які передбачають поєднання вертикальної координації з управлінською децентралізацією, ослаблення ієрархічних контактів, розширення горизонтальних, неформальних зв'язків з недержавними суб'єктами [111].

Іншими словами, відбувається докорінна зміна підходів до розуміння та організації процесів розробки й реалізації державних рішень, пов'язаних з формуванням мережевих структур, які разом з бюрократичними та

ринковими формами створюють новий тип організаційної діяльності органів державної влади.

Ця еволюція багато в чому вплинула на практику державного управління, відтак аналіз наукової полеміки щодо мережевих підходів у координації діяльності органів державної влади набуває актуального значення як для практиків, так і для дослідників.

Мережі сьогодні складаються з безлічі різнорідних складових, які мають різні ресурси і можливості, цілі, партнерів, програмні додатки, технічну інфраструктуру, готовність та персонал тощо. Відомо, що ефективність роботи та соціальна відповідальність суб'єктів управління визначаються не лише діяльністю окремої організації, а й їх колективним результатом. Таким чином, мережеве управління міжорганізаційною діяльністю та співпрацею є багатогранною та складною темою, яка по-різному досліджується науковцями та сприяє розвитку наукового дискурсу у різних галузях науки – державного управління, економіки, історії, політології та ін.

Важливою тенденцією в сучасних суспільствах є формування мереж організаційної співпраці або міжорганізаційних мереж. І приватні, і державні установи чи організації зазвичай беруть участь у мережах, щоб отримати доступ до знань, навичок та ресурсів інших установ, які за певних умов є недосяжними, або які вони не хочуть набувати (позбавлені можливості володіти) самостійно. Співпрацюючи в мережах, організації здатні досягти амбітних і складних цілей, яких вони не в змозі здобути самостійно. Окремі установи відіграють різні ролі в цих мережах в залежності від того, які організації долучаються або виходять з них. Таким чином, мережі є динамічними та схильними до змін.

Голландські дослідники Йорг Рааб і Патрік Кеніс (*Jörg Raab and Patrick Kenis*) стверджують, що зростаюча кількість існування міжорганізаційних мереж призводить до того, що світ стає «суспільством чистої праці» або «суспільством мереж». Вчені обґрунтовують, що світ рухається до

суспільства, в якому формальна вертикально інтегрована організація, яка домінувала в XX столітті, замінюється або доповнюється свідомо створеними та цілеспрямованими мережами з трьох і більше організацій (цілих мереж) [193].

Глобалізація, зростаюча конкуренція і постійна поява нових технологій, високі очікування споживачів адміністративних послуг, а також зростаючі вимоги до них ускладнюють успіх окремих суб'єктів управління. Вони, як правило, вступають у різні типи мережевої взаємодії з метою отримання доступу до знань, нових навичок, технічного обладнання та виробничих потужностей інших установ відповідної сфери управління [195].

Група зарубіжних вчених з США, Сінгапуру, Швейцарії зазначає, що інституції не будуть виконувати завдання всередині повної структури, якщо витрати на його виконання в межах однієї організації стають вищими, аніж це здійснюватиме залучений зовнішній актор. Зокрема, Е. Клемонс (*Eric K. Clemons*) та ін. стверджують, що інноваційні технології дозволяють зменшити витрати на координацію спільної мережевої роботи без ризиків у діяльності кожної організації. Науковці доводять, що дослідження соціальних комунікацій та мережевого співробітництва сьогодні мають велике значення в інформаційних системах, особливо для міждисциплінарних досліджень, у яких особлива увага приділяється темам, пов'язаним із стратегією, інформацією, технологіями, економікою та суспільством [146].

Непередбачувані кризи сучасного суспільства свідчать про необхідність прискорення розвитку таких мереж. У державному секторі діяльність урядових органів засвідчує, що ефективна та якісна державна політика для вирішення надзвичайно складних проблем та потреб громадян вимагає тісної співпраці з іншими суб'єктами публічного управління, громадськими та приватними організаціями. Крім того, такі розробки, як краудсорсинг, державно-приватна інфраструктура та партнерські проекти, прискорюють їх формування та розвиток.

Поширеність і необхідність міжорганізаційної мережевої співпраці як в бізнесі, так і в державному управлінні, породжують широке розмаїття мереж, що слугують різним цілям. До прикладу, вчені з Бернського університету прикладних наук А. Нейроні (*Alessia Neuronì*), М. Фрефель (*Marianne Fraefel*) та ін. зазначають, що у Швейцарії проблеми міжорганізаційної співпраці є наріжним каменем національної стратегії цифрового врядування. Спираючись на існуючі рамки, автори досліджують наукові погляди різних зацікавлених сторін щодо корпоративного управління в рамках федеральної системи Швейцарії. Інформаційна інфраструктура бізнесу та влади усе більше переплітається, що викликає потребу у координації їх функцій та зусиль для досягнення інноваційного руху вперед. Окрім того, науковці досліджують, як управління мережею сприяє продуктивності та досягнення кінцевих результатів. Управління мережами визнається цими вченими критичною змінною, яка значною мірою впливає на їх продуктивність та ефективність [183].

Кембриджський словник тлумачить термін «мережеве управління» як:

- систему з функцією моніторингу та управління різними аспектами мережі; цю функцію можна розділити на три категорії: управління відмовами, управління конфігурацією та управління продуктивністю; це велика система, що складається з багатьох подібних частин, які з'єднані між собою для забезпечення руху або зв'язку між (або вздовж) частин, або між частинами та центром управління;
- організаційний та управлінський підхід, який полягає в співпраці та координації різних стейкхолдерів (органів влади, громадських організацій, приватного сектору та інших зацікавлених сторін) для досягнення спільних цілей та розв'язання складних задач [182].

Таким чином, термін «мережеве управління» може вживатися в контексті публічного сектору, приватного сектору, некомерційних організацій та інших сфер та тлумачиться як підхід, що дозволяє ефективно

управляти складними ситуаціями та досягати спільних цілей через співпрацю та взаємодію різних учасників державного управління.

Перше застосування терміну «мережа» у контексті вивчення державної політики та управління було запропоновано Х'ю Хекло (*Hugh Heclo*) у 1978 р. [170].

Визначення мережевого управління, яке синтезує кілька попередніх тлумачень, запропоновано групою американських дослідників на чолі із К. Джонс (*Candace Jones*) у 1997 році, стосувалося переважно сфери бізнесу і приватного сектору та тлумачиться як управління певною мережею, що включає вибраний, постійний і структурований набір автономних компаній, зайнятих створенням продуктів або послуг на основі неявних і відкритих контрактів для адаптації до непередбачуваних обставин, а також для координації спільної роботи. Таким чином, мережеве управління визначається як впорядкована система механізмів підготовки, прийняття, реалізації та виконання управлінських рішень в організаційних мережах [164].

Мережевий підхід почав розвиватися в 70-х роках XX сторіччя групою європейських вчених, які заснували міжнародне товариство IMP Group (*Industrias Marketing and Purchasing Group*). IMP Group розвивала ідею, що роль взаємовідносин у поясненні поведінки організацій є визначальною у мережевих підходах в управлінні. Першим їх дослідженням було вивчення, узагальнення та аналіз взаємовідносин у промислових ланцюгах поставок в Європі. На сучасному етапі це товариство продовжує відігравати провідну роль у дослідженні мережевих взаємодій.

В подальшому було досліджено природу відносин між компаніями та самі відносини у мережах компаній. Дослідники IMP Group головну увагу зосередили не на операційних складових управлінських процесів, а на побудові клієнтоорієнтованої управлінської моделі, що започаткувало нову дослідницьку платформу – *маркетинг взаємовідносин* як управлінську діяльність із застосуванням низки інструментів (комунікації, обмін

пропозиціями, інструкції, стимули тощо), які мають певну цінність для партнерів, споживачів та суспільства в цілому.

Дана концепція передбачає вивчення і обґрунтування стратегій управління; різноманітних відносин в управлінських процесах; безпосередніх форм і методів комунікацій. Відтак, не дивлячись на відмінності підходів до дослідження мереж, вони не протиставляються один одному, а взаємно доповнюють і збагачують. Вивчення мережевої взаємодії компаній – це сфера міждисциплінарного характеру досліджень, який передбачає обмін ідеями та взаємне збагачення різних дослідницьких підходів, що дозволяє розробляти нові типи організаційних мереж, а також різні форми їх управління.

На початку 90-х років XX сторіччя Р. Майлз та Ч. Сноу (*Raymond E. Miles and Charles C. Snow*) розпочали дослідження мережевих структур, які вважалися ними як ефективне стратегічне організаційне рішення [177].

Науковці обґрунтували еволюційні періоди розвитку таких структур, вважаючи їх початком лінійні, затим функціональні та лінійно-функціональні мережі, згодом – дивізіональні та матричні. На сучасному етапі відбувається новий період суспільного розвитку в умовах глобалізації та стрімко формується нова організаційна структура публічного управління – мережева, розвиток якої став можливим завдяки зростанню інформаційно-комунікативних та цифрових зв'язків між органами влади (рис 1.1).



Рис. 1.1 Етапи еволюції організаційних структур публічного управління

Джерело: узагальнено та систематизовано автором за [48]

Дослідники обґрунтовували, що формування нової мережевої структури управління є новим періодом розвитку міжорганізаційної

мережевої співпраці, головною особливістю якої є використання унікальних/оригінальних активів різних суб'єктів управління, що перебувають на різних етапах власного розвитку для створення певної цінності, в той час як у традиційній моделі управління усі активи акумульовані в межах однієї структури (або у двох організацій відповідно до укладеного контракту).

Теоретичний підхід під назвою «принципал-агент» розглядає відносини між «принципалом» і «агентом», який заснований на розподілі праці, інформаційній асиметрії, навколишньому середовищі і поведінці партнера. У цьому аспекті науковці вважають, що фактор довіри у міжорганізаційних мережових відносинах відіграє вирішальну роль, впливаючи на результат та ефективність роботи. Американські вчені Р. Гулаті, Дж. А. Нікерсон (*Ranjay Gulati, Jack A. Nickerson*) розглядають довіру як певні очікування, що інша компанія не буде діяти опортуністично. Довіра між організаціями-учасниками стосується як неформальних відносин, так і механізмів формального управління, таких як угоди про рівень обслуговування, контракти та орієнтири. Міжорганізаційна довіра впливає на тип управління, що, в свою чергу, чинить вплив на ефективність взаємовигідних відносин [155].

Науковці зазначають, що помітними в цих соціальних відносинах є три види довіри:

- 1) довіра на основі обчислення спирається на раціональні рішення про організацію чи особу, якій слід довіряти;
- 2) довіра на основі ідентичності виникає із повторюваних взаємодій між учасниками; довіра, заснована на ідентичності, також виникає зі спільного членства в професії, команді, робочій групі або соціальній групі;
- 3) інституційна довіра спирається на соціальні структури та норми, такі як закони, угоди, контракти тощо.

Усі три види довіри можуть використовуватися задля забезпечення стійкості організаційних мереж, а також їх здатності вирішувати конфлікти

та управлінські проблеми.

У державно-політичному аспекті основна увага досліджень приділяється ролі влади, розглядаючи державні організації як політичні суб'єкти. Наприклад, вчені С. Командер та С. Пупакіс (*Simon Commander, Stavros Poupakis*) вважають, що національні уряди традиційно покладаються на внесок і співпрацю з суспільством у «політичних мережах». Державні установи потребують знання, ресурси та співпрацю з недержавними економічними та соціальними суб'єктами. У політичних мережах недержавні суб'єкти надають державним суб'єктам, з одного боку, інформацію, знання та досвід, а з іншого боку, підтримку у формуванні та реалізації державної політики. Натомість перші мають можливість впливати на державну політику, законодавство, розподіл державних фінансових ресурсів на вигідні для них напрями. Зміни відчуються одним або декількома мережевими акторами, які вносять нові ідеї в мережу, які потім передаються іншим акторам. Крім того, зовнішні зміни контексту призводять до змін у складі мережі, приходу нових акторів, а також до змін рівнів впливу існуючих акторів. Як наслідок, мережі повинні бути адаптивними та відображати такі зміни у своєму управлінні [147].

При цьому, учасники використовують свою владу для впливу на мережу і зміцнення власних позицій. Управління мережею створюється спільними цілями організацій, відповідальних за кожну групу заходів. Вони розглядають ці мережі як об'єкт безперервної боротьби за владу. Тому структури управління часто відображають розподіл влади в організаційній мережі. Ці дослідження певною мірою зосереджуються на аналізі позиціонування організацій, їх інтересів та можливостей реалізовувати владу. Реалізація влади може бути обмеженою в певних типах мереж через складні завдання, що мають певну специфіку завдань. Відтак, використання влади може бути контрпродуктивним. Крім того, за умови входу або виходу з мережі нової організації, баланс потужності може змінюватися. До того ж, нові технології здатні впливати на цей баланс потужності, оскільки деякі

завдання можуть втратити актуальність, а інші стати більш вагомими. З цієї точки зору спільні цінності та цілі можуть бути використані для управління діяльності учасників мережі [211].

У контексті державно-приватного партнерства дослідження стосуються співпраці державного сектора з комерційними та некомерційними організаціями, формуючи разом різні типи організаційних мереж, інноваційні мережі, державно-приватні мережі.

Фінська дослідниця Ю. Маджава (*Jukka Majava*) виділяє кілька типів мереж, таких як кластери, екосистеми, інноваційні центри, які відрізняються з точки зору членів, цілей, координації, кордонів, динамізму змін, характеру відносин та ролі знань. Зазвичай ці мережі включають постачальників послуг, клієнтів-споживачів, партнерів і навіть університети та державні органи, які співпрацюють з метою розробки, виробництва та просування інноваційних продуктів та послуг. Основною характеристикою цих мереж є те, що низка організацій працюють разом у нечітко пов'язаній структурі, яка може змінюватися з часом. Хоча існує спільна мета, яка мотивує формування мережі, ці організації мають власний інтерес для співпраці. На сьогодні мережі набувають вирішального значення в сфері державного управління, і конкуренція в багатьох галузях, як правило, відбувається більше між такими мережами, аніж серед окремих підприємств чи компаній [175].

Мережі, які перетинають державні та приватні сектори, вважаються важливою моделлю майбутньої організації та координації, яка може дозволити бізнесу, урядам та громадянському суспільству співпрацювати. У цих мережах компанії співпрацюють з національними урядами. Управління цими мережами вимагає комунікації, прийняття рішень, розподілу влади та координації механізмів. Дослідники з Нідерландів М. Янссен, Б. Клієвінк (*Marijn Janssen, Bram Klievink*) зазначають, що управління стикається з багатьма викликами, і процеси залежать від змін у культурних, нормативних та регулятивних структурах.

Всі ці форми мереж співпраці між державними установами,

приватними компаніями, громадянським суспільством і людьми критично покладаються на традиційні інформаційно-комунікативні технології (далі ІКТ), а також на Інтернет і соціальні медіа для своєї діяльності. Такі мережі потребують надійної цифрової інфраструктури для підтримки критично важливих функцій. Особливо транснаціональні мережі державного сектору можуть бути значно посилені «транснаціональними ІКТ», розвиток і управління якими, однак, стикаються зі значними проблемами [162].

Приватний та державний сектори розпочали надавати послуги, які вироблено в організаційних підрозділах, які називаються «центрами спільного обслуговування» та надають заздалегідь визначені сервіси кільком урядовим структурам, отримуючи значні вигоди від економії масштабу, зниження витрат, підвищення досвіду та якості послуг. Дослідник Р. Міннаар (*Reinald Minnaar*) з Університету бізнесу Ньєнроде (Нідерланди) визначає спільний сервісний центр як «окремий і підзвітний напіваавтономний підрозділ у (між)організаційній одиниці, який використовується для об'єднання дій і надання конкретних попередньо визначених послуг операційним підрозділам у цьому (між)організаційному суб'єкті, на основі узгоджених умов. Це призводить до передачі функцій іншим сторонам, що дозволяє організаціям зосередитися на своїй основній діяльності [178].

Мережі особливо важливі як певні канали для переміщення та обробки знань, і вони поступово стають основним місцем поєднання різноманітних знань та додаткових ресурсів, а також створення нових знань та інновацій на мережевому рівні. Мережі пропонують суттєві порівняльні переваги в координації наукомісткої діяльності на міжорганізаційному рівні; їхні соціальні механізми підвищують схильність учасників мережі обмінюватися актуальною інформацією, передавати знання через організаційні кордони та генерувати нові знання.

Ділові мережі набували особливої актуальності у сфері державного управління завдяки фундаментальним змінам у способі розробки та впровадження компаніями інновацій: якщо раніше це було внутрішнім

завданням, то в останнє десятиліття це все частіше стає більш «відкритим» і спільним процесом, що включає широку взаємодію з іншими співпрацюючими постачальниками, клієнтами, посередниками, а також органами державної влади. Участь державних органів у мережах забезпечує такі переваги, як доступ до додаткових ресурсів і можливостей, доступ до нових ринків і технологій, різноманітність знань, а також можливості досягти економії за рахунок масштабності, розділити витрати, інвестиції та ризики діяльності організації, а також впоратися з ринковими, продуктовими та технологічними складнощами.

Фахівець з комплаєнс-менеджменту, американська дослідниця Р. Надін (*Nadine Rivellese*) зазначає, що участь державних органів у таких мережах передбачає широкий обмін інформацією та знаннями між членами, а також вимагає широкої координації діяльності. Зокрема, відносини між приватними компаніями та державними органами вимагають конкретних координаційних дій на трьох рівнях:

- а) «зв'язки активності» (тобто взаємна адаптація в їх діяльності);
- б) «ресурсні зв'язки» (тобто технічні зв'язки та взаємні орієнтації їх фізичних та організаційних ресурсів);
- в) «соціальні зв'язки» (тобто соціальні взаємодії між індивідами та організаційними одиницями фірм, що співпрацюють). Ці координаційні дії вимагають широкого обміну інформацією, як структурованою, так і неструктурованою, яка може бути значною мірою підтримана шляхом використання відповідних ІКТ [194].

Новітня теорія державного управління охоплює також мережеві підходи у розвитку суспільних цінностей. Основна увага тут приділяється мережам громадських організацій, а іноді навіть системам публічних мереж, що співпрацюють інноваційними способами, які є вигідними у порівнянні з ієрархіями. Крім того, дослідники зосереджуються на координації цих мереж, включаючи роль мережевої адміністративної організації (*Network Administrative Organization – NAO*). NAO іноді називають мережевим

посередником, а її діяльність спрямовано на створення та координацію комплексу організаційних мереж [192].

Американська дослідниця Е. Остром (*Elinor Ostrom*) досліджувала концепт поліцентричного управління, яке може бути застосовано до органів державної влади. Поліцентризм є фундаментальним поняттям у її наукових пошуках. Цей термін вчена тлумачить як складну форму управління з кількома центрами прийняття рішень, кожен з яких діє з певним ступенем автономії. Підрозділи, що приймають рішення в поліцентричній структурі управління, характеризуються схожими функціями, однак, оскільки вони розташовані на кількох юрисдикційних рівнях (наприклад, на місцевому, регіональному та національному – обсяг їх відповідальності є різним). Структури також містять управлінські підрозділи спеціального призначення, які перетинають ці юрисдикції, формуючи горизонтальні зв'язки у мережі.

Наприклад, така багаторівнева конфігурація означає, що механізми управління, що демонструють поліцентричні характеристики, можуть бути здатними досягти балансу між централізованим і повністю децентралізованим управлінням у територіальній громаді. Хоча існування кількох напівавтономних центрів прийняття рішень може бути достатнім, однак це не гарантує достатньої координації між центрами прийняття рішень для її функціонування як поліцентричної системи управління.

Поліцентрична система управління може ефективно функціонувати, якщо центри прийняття рішень враховують один одного у конкурентних та кооперативних відносинах і здатні вирішувати конфлікти. Крім того, на сучасному етапі людська діяльність, як правило, взаємопов'язана на національному та глобальному рівнях через технологічний прогрес, зміни в системах державного управління та зростання ринків капіталу. Відтак, поліцентрична система управління повинна мати здатність відповідати наступним трьом характеристикам:

- а) адаптуються до соціальних та екологічних змін;
- б) забезпечують гарну інституційну придатність для складних систем

управління;

в) зменшують ризик інституційного провалу та втрат ресурсів через надмірні повноваження команди осіб, що приймають рішення та мають у розпорядженні різноманітні резерви (фінансові, матеріально-технічні, кадрові тощо) [185].

Група вчених на чолі з Джоном Брайсоном (*John M. Bryson*) здійснюють дослідження у галузі стратегічного планування та мережевого управління у громадській сфері. Вони досліджують способи, якими органи державної влади і некомерційні організації можуть співпрацювати в мережових структурах. У роботі «Міжсекторальний спільний розвиток у громадській сфері» (*Cross-Sector Collaboration in the Public Sector*) автор вивчає співпрацю між громадським, приватним та некомерційним секторами та її вплив на державне управління. Тут розглядається динамічні багаторівневі системи управління, використовуючи як кількісні, так і якісні методи дослідження, особливо із застосуванням поздовжніх порівняльних тематичних досліджень [142].

Дж. Брайсон виокремлює декілька видів систем мережевого управління:

- багаторівневі або складнопідрядні одиниці управління, включаючи використання каскадних збалансованих систем управління для забезпечення узгодженості;
- управління стратегічними питаннями, включаючи статистику продуктивності;
- управління ланцюжка створення вартості;
- портфельні підходи у мережевому управлінні;
- моделі співпраці: основна (головна, провідна) організація, спільне мережеве управління;
- гібридні моделі управління (комбінації двох або більше систем, зазначених вище) [141].

Крістофер Коліба (*Christopher Koliba*), професор Вермонтського університету, спеціалізується на мережевому управлінні та суспільних інноваціях. Він досліджує, які фактори сприяють успішному мережевому управлінню в сфері суспільного врядування. Науковець акцентує, що зростання уваги до мережевої концепції, як руху у напрямі розвитку сфери державного управління, було пов'язане зі зміщенням акценту з майже виняткової уваги на уряд, як дійової особи, до багаторівневого, багатосекторального управління як новітнього процесу реалізації державної політики та надання адміністративних послуг.

Вчений окреслює низку спроб використовувати мережеві концепції для вивчення складних соціальних структур, що виникають при формуванні та реалізації державної політики у різних сферах публічного управління. Перше наукове обґрунтування залученості до державної політики поліцентричних мереж організацій було зроблено згадуваною вище Елінор Остром з групою дослідників у 1963 році [172].

Мережі державного сектору можуть досягати різних цілей, включаючи надання послуг та забезпечення реалізації державної політики. Мережі державних установ формуються для інтегрованого надання послуг, використовуючи модель «єдиного вікна», яка пропонує єдине фізичне або віртуальне місце для доступу громадян до кількох послуг, розроблених різними державними установами. Це спільні, міжорганізаційні мережі, які стали універсальним інструментом надання адміністративних послуг. Надання послуг може включати діяльність та підпроцеси, що виконуються різними організаціями, відтак виникає необхідність управління залежностями між діяльністю цих установ.

Мережі державного сектору також важливі для вирішення нагальних соціальних проблем, таких, як потреби дітей та людей з психічними захворюваннями, зменшення безробіття та розвиток робочої сили, регіональний економічний розвиток. Для створення мережі з громадськими організаціями та окремими громадянами органи влади також активно

використовують соціальні медіа з метою використання їхніх знань для розробки або вдосконалення державної політики та послуг, що призводить до поступового переходу до «спільного виробництва» управлінських послуг [171].

Група дослідників Центру технологій в уряді США – Ш. Доуз, М. Гараві, Г. Берк (*Sharon S. Dawes, Mohammed A. Gharawi, G. Brian Burke*), вивчаючи проблеми міждержавних мереж, зазначають, що однією із головних функцій цих мереж є обмін знаннями та інформацією через кордони з метою забезпечення потреб, з якими жодна організація чи юрисдикція не може самостійно впоратися. Такі мережі є комплексними і динамічними соціотехнічними системами, що містять взаємні відносини, політику, інформацію, знання, процеси і технології.

При цьому, також виникають транснаціональні мережі знань державного сектору, що дозволяє публічним інституціям однієї країни обмінюватися інформацією та знаннями з колегами інших країн для вирішення глобальних проблем, таких як: надзвичайні ситуації у сфері охорони здоров'я, забезпечувати захист навколишнього середовища, контролювати міжнародну міграцію тощо. Вони можуть пролягати між державними департаментами або міністерствами різних країн, багаторівнево або географічно за регіонами. У цих мережах кожна організація-учасниця працює в складних національних, організаційних та інформаційних контекстах.

Контекстуальні відмінності між учасниками створюють дистанції в культурі, політиці, намірах, організаційних факторах, стосунках, знаннях, ресурсах, географії та технології. Ці відстані впливають на їх здатність брати участь у процесах і взаємодіях, які є важливими для продуктивності мережі. Структура цих мереж може бути вертикальною або горизонтальною. Основна мета вертикальних мереж полягає в узгодженні національних і наднаціональних правил за допомогою різних способів їх виконання, тоді як горизонтальні мережі покладаються на обмін знаннями та інформацією, щоб

допомогти створити потенціал для розробки та дотримання глобальних правил і політики. Вертикальні урядові мережі є традиційною формою, але горизонтальні мережі є звичайною структурою для зв'язку провідних акторів у дезагрегованому світі [148].

Таким чином, управління мережами необхідне для вирішення широкого спектру завдань та ситуацій. Це можуть бути рішення оперативного характеру, але також можуть бути пов'язані з готовністю користуватися важливими даними один одного для врегулювання конфліктів та застосування спільних механізмів управління та вирішення широкого кола питань, що належить до тактичного рівня.

Вчені виділяють три основні рівні мережевого управління: централізований, децентралізований і кластерний, а також такі засоби реалізації: а) формалізована структура прийняття рішень, б) встановлений процес узгодження рішень та в) налагодження формальних комунікацій (рис. 1.2).

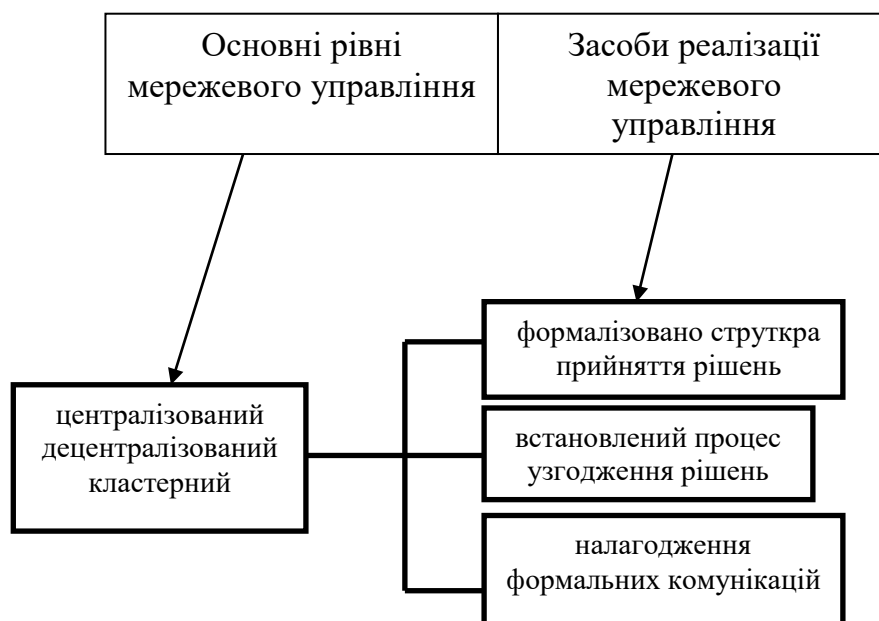


Рис. 1.2. Рівні та засоби реалізації мережевого управління

Джерело: складено автором за [201].

Зазначене послуговується використанням контрактів і угод, які необхідні для формалізації очікувань. Тим не менш, як зазначалось на

початку цього підрозділу, співпраця в мережевих роботах часто базується на довірі. Однак, контракти та формальні домовленості не замінюють довіри, оскільки не все може бути охоплено такими угодами, а надмірно суворі умови контрактів можуть призвести до стратегічно корисливої поведінки. Занадто багато деталей у контракті може навіть заблокувати, а не полегшити співпрацю.

Отже, наукові пошуки щодо вирішення проблем мережевого управління можна згрупувати за різними напрямками та підгалузями в залежності від специфіки досліджень та окреслити наступним чином (табл. 1.1):

Таблиця 1.1

Основні напрями досліджень проблем мережевого управління

Напрямок/Дослідники	Характеристика напрямку
Мережеве управління у публічному секторі (Jörg Raab and Patrick Kenis; Robert W. Rycroft, Don. E. Kash; Christopher Koliba)	Дослідження спрямовані на вивчення ефективності та результативності мережевого управління в громадському секторі, включають аналіз мереж співпраці між державними органами, агентствами, громадськими організаціями та іншими стейкхолдерами
Мережеве управління в державно-політичному аспекті (Elinor Ostrom; Sharon S. Dawes, Mohammed A. Gharawi, G. Brian Burke)	Дослідження впливу мережевого управління на суспільство, включаючи питання влади, довіри та рівності
Мережеве управління в бізнесі і приватному секторі (A. Neuron, M. Fraefel, R. Riedl)	Дослідження в цьому напрямі фокусуються на мережеве управління в корпораціях, міжнародних компаніях та інших приватних організаціях
Мережеве управління в некомерційному секторі (Ranjay Gulati, Jack A. Nickerson; John M. Bryson)	Дослідження цього блоку орієнтовані на мережеве управління в некомерційних організаціях, включаючи громадські організації, благодійні фонди та інші суспільні групи
Мережеве управління в інноваціях та технологіях (Eric K. Clemons, Rajiv M. Dewan, Robert J. Kauffman, Thomas A. Weber)	Дослідження стосується застосування мережевого управління для сприяння інноваціям та розвитку нових технологій
Мережеве управління в міждержавних відносинах (Simon Commander, Stavros Poupakis)	Наукові пошуки у цій царині пов'язуються із взаємодією та співпрацею між державами, міжнародними організаціями та глобальними акторами через мережеві структури

Джерело: узагальнено автором.

Кожен з цих напрямів має свої унікальні виклики та можливості, і дослідники аналізують теоретичні засади та розробляють практичні рішення для поліпшення управління та співпраці у різних сферах суспільного розвитку.

Усе вище окреслене дозволяє сформулювати основні принципи мережевого управління у діяльності органів державної влади, серед яких:

- *співпраця та партнерство*: мережеве управління передбачає співпрацю різних стейкхолдерів, які об'єднують свої зусилля для спільного розв'язання нагальних проблем;

- *налагодження зв'язків у мережевому управлінні*: горизонтальні відносини між стейкхолдерами або бенефіцарами на одному рівні (наприклад, між різними органами державної влади), так і вертикальні відносини між різними рівнями управління (наприклад, між місцевим, регіональним та державними рівнями);

- *забезпечення спільного прийняття рішень*: в мережевому управлінні стейкхолдери беруть участь у процесі прийняття рішень та розв'язання проблем, іноді шляхом консенсусу, поступок, компромісу;

- *децентралізація та автономія*: мережеве управління може передбачати високий рівень децентралізації та автономії для стейкхолдерів або бенефіціарів, що дозволяє їм самостійно приймати управлінські рішення та діяти;

- *фокусування на засадах громадянського суспільства*: акцентується на важливості залучення громадськості до процесів управління;

- *гнучкість і адаптивність*: мережеве управління вимагає гнучкості та здатності до адаптації до змінних умов та потреб стейкхолдерів/бенефіціарів.

Таким чином, підсумовуючи, зазначимо, що наукові пошуки щодо необхідності і доцільності запровадження мережевих підходів у діяльності

органів державної влади триває. Серед зарубіжних дослідників досліджувана тема продовжує активно обговорюватись та підтримується як спосіб поліпшення співпраці між державним та громадським сектором для досягнення спільних цілей. Доведено безапелляційність ефективності мережевого управління, а також значущість викликів, пов'язаних із збереженням довіри, ефективною координацією та прийняттям рішень у складних мережевих структурах.

1.2 Генеза правового формування механізмів мережевого управління у діяльності органів державної влади

Сучасний етап розвитку суспільства вимагає відповідних трансформацій у діяльності органів державної влади шляхом використання цифрових технологій, зокрема мережевого управління. Актуальність дослідження правового формування механізмів мережевого управління зумовлена, з однієї сторони, підвищенням активності застосування мережевих технологій у публічному управлінні та, з іншої – необхідністю удосконалення нормативно-правового забезпечення використання механізмів мережевого управління у діяльності органів державної влади.

Українське суспільство стрімко входить в епоху цифрових технологій, при цьому мережеве управління стає необхідним інструментом для суспільної комунікації між органами державної влади та громадськістю, модернізуючись в інструмент інформаційного впливу на населення [103].

О. Євсюкова пропонує здійснювати розвиток управління сервісної держави на основі мережевого підходу, адже саме в мережах відслідковується тісний взаємозв'язок та взаємовплив органів публічної влади, бізнес структур та громадян. Зокрема, автор пропонує віднести мережевий конструкт організаційної структури суспільства, в якому суб'єкти системи публічного управління перебувають у стані системної взаємодії, до

переліку ознак сервісної держави [21].

Відомо, що завдяки нормам права врегульовуються суспільні відносини у відповідній сфері діяльності, тож і законодавчого врегулювання потребують суспільні відносини у сфері мережевого управління. Успішна діяльність органів державної влади неможлива без впровадження механізмів мережевого управління з їх постійним розвитком у правовому полі.

Поняття «генеза» [від гр. genesis – походження] – синонім «генезис», у словниках та енциклопедичних виданнях означає виникнення, походження [127]; походження, зародження, виникнення, процес утворення [6].

Тому, актуальним є вивчення генези, а саме виникнення, формування, становлення та процесу розвитку механізмів мережевого управління у діяльності органів державної влади, а також визначення особливостей розвитку та чинників, що зумовили цей процес на відповідних стадіях (етапах) історичного виміру.

Виходячи з вищенаведеного, дослідження генези правового формування механізмів мережевого управління включають правові основи у сфері цифровізації та застосування цифрових технологій, зокрема мережевого управління у діяльності органів державної влади.

Погоджуємося із А. Галуцько, що суспільні відносини у сфері правового регулювання механізмів мережевого управління мають новітню юридичну природу, тож дослідження генези правового формування у цій сфері необхідно здійснювати на основах норм міжнародного права і Конституції України в розрізі прав і свобод людини [132].

Таким чином, виникає необхідність у проведенні аналізу сукупності нормативно-правових актів, які врегульовують суспільні відносини в інформаційній сфері, з виокремленням міжнародно-правового та національного рівнів формування законодавства у досліджуваній сфері.

Так, стосовно здійснення ефективних комунікацій між органами

державної влади та громадськістю у Конституції України 1996 року (стаття 38) передбачено, що громадяни України «мають право брати участь в управлінні державними справами». А статтею 40 визначено, що «усі мають право направляти індивідуальні чи колективні письмові звернення або особисто звертатися до органів державної влади, органів місцевого самоврядування та посадових і службових осіб цих органів» [42].

Також, Конституція України надає громадянам «право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір» [42].

Рішенням Конституційного Суду України 2012 року у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України здійснено офіційне тлумачення вищезазначених конституційних положень [101]. Так, Цивільним кодексом України у статті 302 визначено, що «фізична особа має право вільно збирати, зберігати, використовувати і поширювати інформацію» [119].

Отже, це означає, що законодавством передбачено для фізичних осіб мати право на інформацію та визначено, у який спосіб громадяни можуть реалізувати це право, яке узгоджено із нормами міжнародного права.

Зокрема, Міжнародним пактом про громадянські і політичні права, прийнятого 16 грудня 1966 року Генеральною Асамблеєю ООН, який ратифіковано Указом Президії Верховної Ради Української РСР № 2148-VIII від 19 жовтня 1973 року, передбачено право на вільне вираження своїх поглядів, яке «включає свободу шукати, одержувати і поширювати будь-яку інформацію та ідеї, незалежно від державних кордонів, усно, письмово чи за допомогою друку або художніх форм вираження чи іншими способами на свій вибір» [48].

Загальна декларація прав людини, прийнята і проголошена резолюцією 217 А (III) Генеральної Асамблеї ООН від 10 грудня 1948 року [23],

передбачає, що кожному належить «право на свободу переконань і на вільне їх виявлення», що заключається у свободі безперешкодного дотримання своїх переконань та вільний вибір на пошук, одержання і поширення інформації будь-якими засобами в незалежності від державних кордонів.

Конвенція про захист прав людини і основоположних свобод 1950 року [39; 91] також передбачає право на свободу вираження своїх поглядів, яке включає як і свободу дотримуватися своїх поглядів, так і вільний вибір щодо одержання і передавання інформації та ідеї без втручання органів державної влади в незалежності від кордонів.

Угода про співробітництво в галузі інформації 1992 року визначає учасників інформаційних обмінів, зокрема – це громадяни, їх об'єднання, редакції засобів масової інформації, державні й урядові заклади та ін. Угодою передбачено сприяння «всім формам співробітництва між різними засобами масової інформації своїх держав для забезпечення широкого вільного розповсюдження й обміну інформацією, включаючи створення спільних інформаційних структур» [117].

Окінавська хартія глобального інформаційного суспільства, прийнята на саміті G-8 в липні 2000 року [184], визначає інформаційно-комунікаційні технології, як один із найважливіших факторів, які впливають на формування суспільства XXI століття. Хартія передбачає активне сприяння діалогу з країнами, що розвиваються, міжнародними організаціями та іншими учасниками з метою удосконалення міжнародного співробітництва щодо формування політичного, нормативного та мережевого забезпечення та ін.

Хартія про збереження цифрової спадщини, прийнята у 2003 році [145], встановлює, що цифрова спадщина складається з унікальних ресурсів людських знань і вираження. Вона охоплює культурні, освітні, наукові та адміністративні ресурси, а також технічну, юридичну, медичну та інші види інформації, створені в цифровому вигляді або перетворені в цифрову форму з існуючих аналогових ресурсів.

Женевська Декларація принципів «Побудова інформаційного суспільства – глобальне завдання в новому тисячолітті» 2003 року [141] має на меті подолання цифрової нерівності, закликає до цифрової солідарності, як на національному, так і на міжнародному рівнях. Визначає спілкування як необхідну основу інформаційного суспільства, що є одним з основних соціальних процесів, однією з базових людських потреб і основою будь-якої соціальної організації. В документі зазначено, що створення відкритого для всіх інформаційного суспільства потребує нових форм солідарності, партнерства і співробітництва між державними органами та іншими заінтересованими сторонами (приватним сектором, громадянським суспільством та міжнародними організаціями).

Угода про асоціацію між Україною та Європейським Союзом (Угода про асоціацію) від 27 червня 2014 року встановлює принципи нормативно-правової бази для всіх електронних комунікаційних послуг та визначає й інші положення. Україна взяла на себе зобов'язання щодо забезпечення поступового приведення своїх чинних законів та майбутнього законодавства у відповідність до *acquis* ЄС [116]. В контексті вищенаведеного слід наголосити, що наразі Україна вже виконала 72% всіх зобов'язань, передбачених Угодою про асоціацію. У Звіті про виконання Угоди про асоціацію за 2022 рік 96% прогресу досягнуто у сфері статистики та обміну інформацією [142].

Продовжуючи дослідження генези правового формування механізмів мережевого управління в діяльності органів державної влади в законодавстві національного рівня, визначимо Закон України «Про інформацію» 1992 року, яким передбачено забезпечення права на інформацію такими заходами як [79]:

- реалізація права на інформацію шляхом створення відповідного механізму;
- вільний доступ до статистичних даних, архівних, бібліотечних і

музейних фондів, інших інформаційних банків, баз даних, інформаційних ресурсів шляхом створення таких можливостей;

- інформування громадськості та медіа про діяльність органів державної влади і прийняті ними рішення, як обов'язок суб'єктів владних повноважень;

- визначення спеціальних підрозділів або відповідальних осіб в органах державної влади для забезпечення доступу громадян до інформації;

- здійснення державного і громадського контролю за дотриманням законодавства про інформацію;

- визначення відповідальності за порушення законодавства про інформацію.

Законом України «Про доступ до публічної інформації» 2011 року забезпечується доступ до інформації через систематичне та оперативне оприлюднення інформації (в офіційних друкованих виданнях, на офіційних веб-сайтах в мережі Інтернет, на єдиному державному веб-порталі відкритих даних, на інформаційних стендах та у будь-який інший спосіб) та надання інформації за відповідними запитами [63], що і є однією з конституційних гарантій реалізації права на інформацію, зокрема права на вільне збирання, зберігання, використання та поширення інформації [101].

В контексті нашого дослідження необхідно виокремити законодавчі акти у сфері інформаційної, телекомунікаційної діяльності, діяльності друкованих засобів масової інформації (преси) та ін., які на сьогодні вже втратили чинність, але впливають на дослідження правового формування механізмів мережевого управління в діяльності органів державної влади.

Так, Закон України «Про телекомунікації» 2003 року (втратив чинність) [97] визначав повноваження держави щодо управління та регулювання телекомунікаційної діяльності, а також права, обов'язки та засади відповідальності фізичних і юридичних осіб, які брали участь у даній діяльності або користувалися телекомунікаційними послугами.

Закон України «Про друковані засоби масової інформації (преси) в Україні» 1992 року (втратив чинність) [64] створював правові основи діяльності друкованих засобів масової інформації (преси) в Україні, встановлював державні гарантії їх свободи відповідно до Конституції України, Закону України «Про інформацію» та інших актів чинного законодавства і визнаних Україною міжнародно-правових документів.

У Законі України «Про телебачення і радіомовлення» 1993 року (втратив чинність) [96] врегульовувалися відносини, що виникали у сфері телевізійного та радіомовлення на території України, а також визначалися правові, організаційні, економічні, соціальні умови їх функціонування, які були спрямовані на реалізацію прав громадян на отримання повної, достовірної та оперативної інформації, на відкрите і вільне обговорення суспільних питань та свободи слова.

На сьогодні вищевказані питання регулюються такими нормативно-правовими актами. Так, Закон України «Про електронні комунікації» 2020 року [66] визначає мету та завдання державного управління і регулювання у сферах електронних комунікацій, а також повноваження органів державної влади у сферах електронних комунікацій та радіочастотного спектра та регулює інші питання. Закон України «Про медіа» 2022 року [81] спрямований на забезпечення реалізації права на свободу вираження поглядів, права на отримання різнобічної, достовірної та оперативної інформації, на забезпечення плюралізму думок і вільного поширення інформації, на захист національних інтересів України та прав користувачів медіа-сервісів, регулювання діяльності у сфері медіа відповідно до принципів прозорості, справедливості та неупередженості, стимулювання конкурентного середовища, рівноправності і незалежності медіа та визначає правовий статус, порядок формування, діяльності та повноваження Національної ради України з питань телебачення і радіомовлення.

При формуванні механізмів мережевого управління у діяльності

органів державної влади важливим аспектом також є врегулювання відносин громадян, юридичних осіб, а також держави, що з'являються при створенні, отриманні, використанні та поширенні науково-технічної інформації. Так, метою Закону України «Про науково-технічну інформацію» 1993 року [82] є створення правової основи для отримання та використання науково-технічної інформації, а також визначення правових форм міжнародного співробітництва у цій сфері.

Отже, формування механізмів мережевого управління в діяльності органів державної влади відбувалося поступово з початком розвитку інформаційного законодавства.

Так, Законом України у 1998 році схвалено Концепцію Національної програми інформатизації [80], в якій передбачено основну мету Програми щодо забезпечення громадян та суспільства своєчасною, достовірною та повною інформацією на основі широкого використання інформаційних технологій, забезпечення інформаційної безпеки держави.

Національна програма інформатизації 1998 року [84], яка на сьогодні втратила чинність, визначала стратегію вирішення проблеми реалізації інформаційних потреб та інформаційної підтримки оборонної, екологічної, соціально-економічної, науково-технічної, національно-культурної та ін. сферах діяльності.

У 2022 році прийнято новий Закон України «Про Національну програму інформатизації», який визначає Національну програму інформатизації як «комплекс завдань, програм, проектів, робіт з інформатизації, спрямованих на розвиток інформаційного суспільства шляхом концентрації та раціонального використання фінансових, матеріально-технічних та інших ресурсів, виробничого і науково-технічного потенціалу держави, координації діяльності державних органів, органів місцевого самоврядування, а також підприємств, установ, організацій незалежно від форми власності» [85]. Одними із основних завдань

Національної програми інформатизації визначено реалізацію організаційних механізмів інформаційної взаємодії органів публічної влади за допомогою електронного документообігу, а також утворення систем інформаційної та аналітичної підтримки їх діяльності [85].

Указом Президента України від 31 липня 2000 р. № 928/2000 «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» [77] встановлено, що розвиток національної складової глобальної інформаційної мережі Інтернет (мережа Інтернет), забезпечення широкого доступу до цієї мережі громадян та юридичних осіб усіх форм власності в Україні, належне представлення в ній національних інформаційних ресурсів є одним з пріоритетних напрямів державної політики у сфері інформатизації, а також реалізацією конституційних прав громадян на інформацію, побудови відкритого демократичного суспільства та розвитку підприємництва.

Указом Президента України від 17 травня 2001 року № 325/2001 «Про підготовку пропозицій щодо забезпечення гласності та відкритості діяльності органів державної влади» [88] було сформовано робочу групу з підготовки пропозицій щодо забезпечення гласності та відкритості діяльності органів державної влади, завданнями якої було, враховуючи вітчизняний та міжнародний досвід, розробити законопроекти щодо формування правових основ з метою реалізації громадянами України конституційних прав на участь в управлінні державними справами та на вільний доступ до інформації про діяльність органів державної влади.

Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади, затверджений постановою Кабінету Міністрів України від 4 січня 2002 р. № 3 [90], визначає, що таке оприлюднення здійснюється для підвищення ефективності та прозорості діяльності органів державної влади через запровадження та застосування сучасних інформаційних технологій з метою надання громадянам інформаційних та

інших послуг, а також забезпечення впливу громадянського суспільства на процеси, що відбуваються у державі.

Таким чином, до 2007 року відзначався значно повільний темп створення інфраструктури для надання органами державної влади та органами місцевого самоврядування юридичним і фізичним особам інформаційних послуг з використанням мережі Інтернет. У зв'язку з цим і було прийнято Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», в яких було визначено перехід національної політики розвитку інформаційного суспільства в Україні до пріоритетного науково-технічного та інноваційного розвитку шляхом запровадження відповідних механізмів для надання інформаційних послуг через мережу Інтернет. У цьому законі також визначені основні засади законодавчого забезпечення розвитку інформаційного суспільства, запропоновано гармонізувати чинні нормативно-правові акти з нормами міжнародного права та здійснити кодифікацію інформаційного законодавства [87]. Зокрема, було запропоновано розробити та прийняти Інформаційний кодекс України (Кодекс України про інформацію) [99], який би визначив конкретний перелік суб'єктів інформаційних відносин, з урахуванням їх прав та законних інтересів, забезпечив би єдині підходи та принципи до регламентації відносин в інформаційному просторі.

Слід зазначити, що формування механізмів мережевого управління в діяльності органів державної влади пов'язана із оприлюдненням та поширенням інформації про їх діяльність.

Так, Закон України «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації» 1997 року [89], який на сьогодні втратив чинність, передбачав всебічне та об'єктивне висвітлення діяльності органів державної влади та органів місцевого самоврядування ЗМІ та інші положення законодавства про інформацію.

Закон України «Про доступ до публічної інформації» 2011 року [63], передбачає обов'язок суб'єктів владних повноважень – органів державної влади оприлюднювати інформацію, зокрема інформацію про організаційну структуру органу державної влади, його місію, функції, повноваження та основні завдання, а також напрями діяльності та фінансові ресурси

У Законі України «Про засади державної мовної політики» 2012 року [71], який визнано неконституційним, визначалося, що офіційна інформація про діяльність органів державної влади та органів місцевого самоврядування поширюється державною мовою, а у межах території, на якій поширена регіональна мова (мови), також і цією мовою (мовами).

Слід зазначити, що Законом України «Про забезпечення функціонування української мови як державної» 2019 року [70] передбачено, що нормативно-правові акти і акти індивідуальної дії органів державної влади оприлюднюються державною мовою у визначеному законодавством порядку.

Закон України «Про національну інфраструктуру геопросторових даних» 2020 року [83] встановлює обов'язок органів виконавчої влади та органів місцевого самоврядування оприлюднювати у мережі Інтернет усі геопросторові дані та метадані, окрім тих, які належать до інформації з обмеженим доступом.

Указ Президента України від 29 липня 2019 року № 558 «Про деякі заходи щодо поліпшення доступу фізичних та юридичних осіб до електронних послуг» [62] сприяє забезпеченню належного функціонування та захисту даних у національних електронних інформаційних ресурсах, доступності та зручності цифрових послуг для фізичних та юридичних осіб, а також запобігання корупції під час надання таких послуг.

Беручи до уваги те, що сучасний стан розвитку мережевого суспільства визначається як вітчизняними, так і зарубіжними науковцями як відповідні «процеси формування та реалізації механізмів мережевого управління в

діяльності органів публічної влади» та мають на меті покращити взаємодію з громадськістю, а також, погоджуючись з тим, що мережеве управління розглядається як процес залучення громадянського суспільства [8], пропонуємо дослідити становлення нормативно-правової бази, яка врегульовує питання реалізації державної політики щодо взаємодії органів державної влади та інститутів громадянського суспільства.

Створення ефективних організаційних та правових умов для формування ефективної взаємодії громадянського суспільства з органами державної влади стало метою прийняття Указу Президента України від 31 липня 2004 року № 854/2004 «Про забезпечення умов для більш широкої участі громадськості у формуванні та реалізації державної політики» [67].

Сучасний етап створення системи безперервного діалогу та взаємної співпраці органів державної влади та інститутів громадянського суспільства визначався шляхом прийняття таких Указів Президента України, як від 15 вересня 2005 року № 1276/2005 «Про забезпечення участі громадськості у формуванні та реалізації державної політики»; від 25 січня 2012 року № 32/2012 «Питання сприяння розвитку громадянського суспільства в Україні», а також розпорядженням Кабінету Міністрів України від 21 листопада 2007 р. № 1035-р «Про схвалення Концепції сприяння органами виконавчої влади розвитку громадянського суспільства», мета якої (Концепції) полягала у створенні сприятливих умов для подальшого розвитку громадянського суспільства та зміцнення демократії в Україні [69; 55; 95]. Ці нормативно-правові акти на сьогодні втратили чинність.

Закон України «Про громадські об'єднання» від 22 березня 2012 року [61] визначає основні засади взаємодії громадських об'єднань з органами державної влади шляхом залучення їх до процесу формування та реалізації державної політики, а також право громадських об'єднань брати участь у законотворчій діяльності, зокрема розроблення проєктів

нормативно-правових актів, які приймаються та видаються органами державної влади.

Впровадження сучасних форм та методів взаємодії органів державної влади та громадянського суспільства з використанням ІКТ, зокрема проведення опитувань, консультацій, здійснення громадських експертиз тощо, передбачено Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 9 січня 2007 року [87].

Постановою Кабінету Міністрів України у 2010 році затверджено Порядок проведення консультацій з громадськістю з питань формування та реалізації державної політики, який встановлює загальні вимоги щодо організації і здійснення органами виконавчої влади консультацій з громадськістю з питань формування та реалізації державної політики, а також Типове положення про громадську раду при міністерстві, іншому центральному органі виконавчої влади, обласній, Київській міській, районній, районній у м. Києві державній адміністрації, яке визначає основним із завдань громадської ради під час формування та реалізації державної політики сприяти врахуванню органом виконавчої влади громадської думки [68].

Указом Президента України у вересні 2021 року затверджено Національну стратегію сприяння розвитку громадянського суспільства в Україні на 2021-2026 роки, яка має на меті «створення сприятливих умов для розвитку громадської ініціативи та самоорганізації, формування та діяльності інститутів громадянського суспільства, налагодження взаємодії між громадянами, згаданими інститутами та органами державної влади, органами місцевого самоврядування, у тому числі для реалізації та захисту прав і свобод людини та громадянина, задоволення суспільних інтересів, забезпечення громадської участі у прийнятті та реалізації владних рішень» [86].

Правове поле та засади діяльності організацій громадянського суспільства у 2022 році зазнали значних змін з початком введення надзвичайного, а пізніше і воєнного стану. Органи публічної влади встановили багато обмежень щодо діяльності з проведення публічних консультацій стосовно обговорення проєктів нормативно-правових актів, а також щодо залучення організацій громадянського суспільства до участі у засіданнях органів виконавчої влади та органів місцевого самоврядування. Окрім цього, встановлено обмеження щодо подання інформації про діяльність органів державної влади на офіційних сайтах, а також обмежено доступ до публічних реєстрів, в тому числі і до Єдиного державного реєстру юридичних і фізичних осіб-підприємців та громадських формувань [57].

У цьому контексті важливим є здійснення під час воєнного стану міжсекторальної взаємодії між органами державної влади, органами місцевого самоврядування, громадянським суспільством та бізнесом, зокрема з таких питань як вирішення проблем жителів територіальних громад, підтримки ЗСУ, надання допомоги внутрішньо переміщеним особам та ін. Однією з форм такої взаємодії є мережі координаторів, які створюють громадські організації з метою розв'язання зазначених проблем шляхом здійснення ефективної комунікації з органами місцевої виконавчої влади та органами місцевого самоврядування [92].

Розпорядженням Кабінету Міністрів України від 14 лютого 2023 р. № 160-р затверджено план заходів до 2024 року [72] щодо реалізації Національної стратегії сприяння розвитку громадянського суспільства в Україні на 2021-2026 роки, яким визначено завдання та заходи міністерствам, іншим центральним та місцевим органам виконавчої влади щодо правового та організаційного забезпечення сприяння розвитку громадянського суспільства та діяльності громадських організацій, а також стандартизації публічних консультацій та ін.; строки їх виконання та відповідальних осіб; індикатори виконання цих заходів та очікувані результати.

Щодо реалізації вищезазначеної Стратегії місцевими органами державної влади, слід зазначити, що станом на 1 вересня 2023 року затверджено 16 Регіональних цільових програм сприяння розвитку громадянського суспільства та у місті Києві затверджено міську цільову програму [100].

Одним із механізмів реалізації цієї Стратегії є те, що органи виконавчої влади повинні інформувати громадськість про її реалізацію на офіційних вебсайтах та в соціальних мережах [86], що дає змогу зробити висновок про затребуваність застосування органами державної влади засобів мережевого управління у своїй діяльності.

На нашу думку, сьогодні реалізація механізмів мережевого управління у діяльності органів державної влади, пов'язана з цифровізацією, розвитком соціальних медіа та з удосконаленням зв'язків з громадськістю, перетворилась на актуальну вимогу часу. У зв'язку з цим, виникає необхідність проаналізувати правове забезпечення використання соціальних мереж у діяльності органів державної влади.

Соціальні мережі використовуються з метою розширення кола спілкування, відслідковування та моніторингу діяльності інших користувачів, зокрема органів державної влади, а також для викладу власної позиції з актуальних соціальних й суспільнозначущих проблем [53]. Соціальні мережі дозволяють підтримувати комунікаційні зв'язки на відстані одночасно із значною кількістю осіб, при цьому будь-яка онлайн-комунікація може втілитись в спільні масові заходи поза межами глобальної мережі.

Водночас при дослідженні механізмів дії соціальних мереж та способів поширення інформації порушується низка актуальних питань. Це, по-перше, ідентифікація користувачів мережі Інтернет, по-друге, посилення відповідальності за дотримання авторських прав, по-третє – цифрова безпека, кібергігієна та забезпечення безпеки доступу до баз даних, по-четверте – нормативно-правове врегулювання використання офіційної символіки у

соціальних мережах, по-п'яте – питання моралі і цензури (як груп у соціальних мережах, так і органів публічної влади, а також посадових осіб найвищої ланки, які мають акаунти в соціальних мережах) [103].

В Україні вже активно розробляється законодавство, яке стосується сфери цифровізації. Однак ці нормативно-правові акти опосередковано стосуються питань використання соціальних мереж у діяльності органів державної влади та формування механізмів мережевого управління.

Так, метою Закону України «Про електронні довірчі послуги» є врегулювання відносин у сферах надання електронних довірчих послуг та електронної ідентифікації. Також цим законом визначено поняття «веб-сайт» як «сукупність програмних засобів, розміщених за унікальною адресою в обчислювальній мережі, у тому числі в мережі Інтернет, разом з інформаційними ресурсами, що перебувають у розпорядженні певних суб'єктів і забезпечують доступ юридичних та фізичних осіб до цих інформаційних ресурсів та інших інформаційних послуг через обчислювальну мережу» [65].

Концепція розвитку цифрової економіки та суспільства України на 2018-2020 роки визначила, що одним із напрямів цифрового розвитку є подолання цифрового розриву через розвиток цифрових інфраструктур, зокрема зазначається, що: «Національний план розвитку широкосмугового доступу до Інтернету повинен містити відповідні показники покриття широкосмуговим доступом до Інтернету території країни; технічні вимоги до самих послуг широкосмугового доступу до Інтернету; моделі використання наявних у державі фізичних інфраструктур (авто- та залізничні магістралі, газопроводи, лінії електропередач) з метою розвитку телекомунікаційних мереж, відповідні ініціативи та проекти з організації надання послуг широкосмугового доступу до Інтернету для територій, громад, домоволодінь та соціальної інфраструктури» [93].

В цьому контексті необхідно вказати, що Законом України «Про захист

персональних даних» [76] регулюються правові відносини, що пов'язані із захистом і обробкою персональних даних, а також визначаються повноваження Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних, який, окрім судів, здійснює контроль за додержанням законодавства про захист персональних даних у межах своїх повноважень.

Правові відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах регулює Закон України «Про захист інформації в інформаційно-комунікаційних системах» [75] та визначає, що об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки такої інформації.

Забезпечення формування та реалізація державної політики у сферах організації спеціального зв'язку, захисту інформації, кіберзахисту, активної протидії агресії у кіберпросторі покладено на Адміністрацію Державної служби спеціального зв'язку та захисту інформації України відповідно до Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 3 вересня 2014 р. № 411 [73].

Отже, процеси глобалізації та цифровізації дозволяють органам державної влади використовувати Інтернет та соціальні мережі з метою здійснення ефективних комунікацій з громадськістю засобами мережевого управління, а це вимагає необхідність формування правового забезпечення щодо цих питань.

Погоджуємось, що використання мережевих технологій у діяльності органів державної влади є одним із пріоритетних напрямів державної політики в період цифрових трансформацій та цифровізації всіх сфер життєдіяльності суспільства. Впровадження сучасних цифрових інструментів органами публічної влади є одним з універсальних механізмів формування

цифрового управління і прийомів прийняття управлінських рішень, а також одним з основних методів удосконалення сфери публічного управління, які мають бути спрямовані на конкретні зміни в діяльності органів публічної влади, введення нових форм і засобів роботи публічних службовців [104].

Слід наголосити на тому, що сьогодні в Україні керуються низкою нормативно-правових актів, які регулюють різні аспекти питання поширення інформації про діяльність органів публічної влади в мережі Інтернет, однак не існує жодного такого акту, яким врегульовуються всі відносини, пов'язані з поширенням інформації, зокрема в соціальних мережах. Відсутність такого уніфікованого акту тільки підвищує ймовірність використання інформації, опублікованої в соціальних мережах органами державної влади, не за призначенням.

Таким чином, досліджуючи генезу правового формування механізмів мережевого управління в діяльності органів державної влади, можна зробити висновок про те, що українське законодавство у сфері мережевого управління не сформовано, окрім регулювання окремих аспектів діяльності органів державної влади в інформаційній сфері та у сфері цифровізації, а також питань забезпечення зв'язків з громадськістю, розвитку громадянського суспільства (врегульовано у значній кількості нормативно-правових актів).

Одже, на основі дослідження генези правового формування механізмів мережевого управління у діяльності органів державної влади виокремимо етапи створення нормативно-правових актів, які врегульовують суспільні відносини в інформаційній сфері, у сфері цифровізації, застосування цифрових технологій, а також з позицій конституційного права на інформацію та його реалізації, участі громадськості в державних справах та розвитку громадянського суспільства.

Перший етап (1973 – 1996 рр.) розпочався ратифікацією Указом Президії Верховної Ради Української РСР у 1973 р. Міжнародного пакту про

громадянські і політичні права, який прийнято 16 грудня 1966 р. Генеральною Асамблеєю ООН, і яким передбачено право на вільне вираження своїх поглядів. Угода про співробітництво в галузі інформації 1992 р. визначила учасників інформаційних обмінів. У 1996 р. прийнято Конституцію України, в якій передбачено право на інформацію. Відбулося прийняття Закону України «Про інформацію» 1992 р., яким передбачено забезпечення права на інформацію. Цей етап характеризується врегулюванням відносин громадян, юридичних осіб, а також держави, що з'являються при створенні, отриманні, використанні та поширенні науково-технічної інформації (Закон України «Про науково-технічну інформацію», 1993 р.).

Другий етап (1998 – 2003 рр.) визначився прийняттям декількох міжнародних документів у сфері інформаційно-комунікаційних технологій (Окінавська хартія глобального інформаційного суспільства, 2000 р.); збереження цифрової спадщини (Хартія про збереження цифрової спадщини, 2003 р.); регулювання співробітництва між державними органами та приватним сектором, громадянським суспільством і міжнародними організаціями, а також щодо подолання цифрової нерівності (Женевська Декларація принципів «Побудова інформаційного суспільства – глобальне завдання в новому тисячолітті», 2003 р.). Цей етап пов'язується із схваленням у 1998 р. Концепції Національної програми інформатизації. В цей період були прийняті законодавчі акти у сфері інформаційної, телекомунікаційної діяльності, діяльності друкованих засобів масової інформації (преси), зокрема у 2003 р. – Закон України «Про телекомунікації». На цьому етапі на законодавчому рівні закріплено питання розвитку національної складової глобальної інформаційної мережі Інтернет; щодо забезпечення гласності та відкритості діяльності органів державної влади; механізми оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади;

Третій етап (2004 – 2015 рр.) характеризується встановленням

принципів нормативно-правової бази для всіх електронних комунікаційних послуг (Угода про асоціацію між Україною та Європейським Союзом, 2014 р.). Відбулося прийняття Закону України «Про доступ до публічної інформації» у 2011 р., що і визначило конституційні гарантії реалізації права на інформацію. У цей період було затверджено Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки, в яких визначено розвиток інформаційного суспільства в Україні шляхом запровадження відповідних механізмів для надання інформаційних послуг через мережу Інтернет, а також було розроблено проєкт Інформаційного кодексу України. Під час цього етапу відбувається становлення нормативно-правової бази, яка врегульовує питання реалізації державної політики щодо взаємодії органів державної влади та інститутів громадянського суспільства (прийнято низку підзаконних нормативно-правових актів та Закон України «Про громадські об'єднання», 2004-2012 рр.).

Четвертий етап (2016 р. – до тепер) характеризується прийняттям законодавства у сфері цифровізації та застосування цифрових технологій. Прийнято закони України «Про електронні комунікації», 2020 р. та «Про медіа», 2022 р. У 2022 році прийнято Закон України «Про Національну програму інформатизації». Крім цього, прийнято законодавство, що стосується сфери цифровізації (Концепція розвитку цифрової економіки та суспільства України на 2018-2020 рр. Цей етап формування механізмів мережевого управління в діяльності органів державної влади пов'язаний із механізмами оприлюднення та поширення інформації про їх діяльність (закони України «Про забезпечення функціонування української мови як державної», 2019 р. та «Про національну інфраструктуру геопросторових даних», 2020 р.); затверджено Національну стратегію сприяння розвитку громадянського суспільства в Україні на 2021-2026 роки. Особливістю цього етапу є встановлені у 2022 р. обмеження у взаємовідносинах органів державної влади та організацій громадянського суспільства у зв'язку із введенням воєнного стану.

1.3 Соціально-комунікативні імперативи реалізації мережевого управління

В сучасних умовах комунікація є невід’ємною складовою будь-яких форм суспільних відносин. Активний розвиток соціальних мереж, зумовили настільки швидкі темпи розвитку держави та суспільства в цілому, що використання нових засобів комунікації залишається недостатньо вивченими. Сучасні комунікаційні технології мають значний вплив на свідомість людини, що й актуалізує дослідження порушеного питання.

У філософському значенні поняття комунікація (лат. *communicatio*, від *communis* – «роблю спільним, пов’язую, спілкуюсь») розуміють у широкому сенсі як термін, що окреслює людську взаємодію у світі [126, с. 291], яка виникає з потреб людей у суспільному житті. У науковому полі існують різні тлумачення змісту поняття комунікація. Соціологи (П. Сорокін) розуміють під комунікацією взаємодії, тобто передачу соціальної інформації. Психологи (А. Леонтьєв) – процеси обміну продуктами психологічної діяльності, насамперед спілкування. Кібернетики (А. Урсул) – обмін інформацією між складними динамічними системами та їхніми частинами, здатність сприймати, накопичувати та переробляти інформацію [1]. Енциклопедія державного управління тлумачить комунікацію, як обмін інформацією з приводу тієї або іншої проблеми, інструменту і результатів дослідження [38; 292].

Таким чином, поняття комунікація розуміється як спілкування, передача інформації, процес інформування широкого кола осіб із використанням технічних засобів, засобів масової комунікації (преси, радіо, телебачення тощо), що зумовлюється досягненням соціальної спільності та взаємодії за умови збереження індивідуальності кожного її елемента.

Так, в межах цифровізації українського суспільства саме цифрові комунікації виступають прогресивно удосконаленим елементом в

публічному управлінні та відіграють надзвичайно важливу роль у встановленні взаємодії між органами влади та громадськістю

На думку А. Соколова, електронна комунікація – це новітній вид смислової соціальної комунікації, яка охоплює широке коло техногенних комунікаційних каналів, заснованих на дротовому та радіозв'язку, магнітному та оптичному записі інформації. В. Маркова вважає, що електронна комунікація є синтезом усної та письмової комунікацій на новому технологічному рівні. О. Гребнев розглядає електронну комунікацію як соціальну інформаційну комунікацію, де каналом є електронне (цифрове) середовище [126].

Сьогодні органами влади, для зменшення паперової роботи і збереження необхідної інформації, поряд з електронною поштою та електронними дошками оголошень для передачі рутинної інформації, використовуються й соціальні мережі. Серед іншого, використання комунікацій в публічному управлінні передбачає публікацію на веб-сторінках органу влади інформації про власну діяльність, ведення діалогу з основними цільовими аудиторіями та зосередженість на наданні електронних послуг.

З появою та стрімким розвитком інтернет-простору, істотного значення набуває поняття цифровізації як складової демократичного розвитку, оскільки впроваджується ціла низка реформ, які охоплюють всі сфери суспільного життя. Актуальність зазначеного обумовлено тим, що в демократичній державі органи публічної влади не можуть ефективно функціонувати без конструктивної взаємодії з громадянським суспільством. Веб-сайти стали механізмом надання актуальної інформації. Однак соціальні мережі стають все більш пріоритетним підґрунтям для спілкування між органами публічного управління та громадянами.

В основу реформ, що відбуваються та плануються, поставлено як самий розвиток цифрових технологій, так і різні методи їх ефективного застосування, які дозволяють вийти на новий рівень взаємодії держави та

суспільства у вирішенні соціально-економічних проблем. Одним із основних завдань держави є забезпечення доступу всієї української спільноти до інформації в інтернет-просторі, необхідною умовою якого є розвиток цифрового суспільства.

Підвищення швидкості та доступу до Інтернет-простору, поширення мобільних пристроїв й додатків формують нові можливості доступу до інформації шляхом використання соціальних мереж. Спілкування всередині країни, з іншими установами та організаціями, а також з громадськістю істотно змінилися з розвитком нових технологій і соціальних медіа [37, с. 64]. Соціальні медіа включають Facebook, Google plus, Twitter, блоги, вікі та YouTube, де всі вони побудовані на основі технології Web 2.0. Соціальні мережі визначаються як «мережева платформа, що охоплює всі підключені пристрої, які заохочують співпрацю з точки зору створення, організації, зв'язку та обміну вмістом» [190]. Нині функціонування соціальних мереж стало невід'ємною складовою публічного управління майже у всьому світі.

Соціальні мережі сприймаються як певний інструмент, що використовується з метою привернення уваги громадян до суспільно важливих питань та інформування про діяльність органів публічної влади.

Україна потребує трансформації багатьох суспільних процесів та встановлення дієвих механізмів публічного управління. Швидкий розвиток цифровізації публічного управління вимагає від публічних службовців використання сучасних цифрових технологій, реалізації нових механізмів прийняття управлінських рішень та створення позитивного іміджу органів публічної влади.

Інтернет активно модернізує суспільство та більш ґрунтовно інтегрує його в соціальне життя он-лайн. Сьогодні фактично не можливо уявити сучасний світ без соціальних мереж. Реалії сучасності потребують зміни форми роботи органів державної влади шляхом використання цифрових технологій, до яких належить Інтернет, і зокрема, соціальні мережі.

У зв'язку з активним використанням соціальних медіа українським суспільством органи публічної влади для налагодження ефективної комунікації із громадськістю почали доволі активно використовувати соціальні мережі з метою поширення необхідної інформації стосовно формування державної політики, механізмів її реалізації та проведення роз'яснювальної роботи щодо перспектив її розвитку тощо. Водночас вимоги до якості, актуальності та повноти інформації, яка розміщується органами державної влади на сторінках у соціальних мережах, чітко не визначені та потребують нормативно-правового врегулювання. Також залишається актуальним питання щодо оптимального вибору соціальних мереж на загальнодержавному рівні та нормативно-правового врегулювання механізмів ведення такої комунікації органами державної влади. Слід зазначити, що велика кількість державних інституцій мають свої сторінки в таких соціальних мережах, як «Фейсбук», «Ютуб», «Твітер» тощо.

Соціальні мережі стали дієвим інструментом управління в бізнесі, освіті, економіці, а також набули ознак повноцінних засобів масової інформації (соціальних медіа). В період розвитку інформаційного суспільства, активна імплементація соціальних мереж спостерігається як у повсякденному житті суспільства, так і в функціонуванні органів публічної влади.

Під соціальною мережею розуміємо інтернет-співтовариство користувачів, об'єднаних за будь-якою ознакою на базі одного сайту. Головним чинником об'єднання користувачів у соціальну мережу може бути будь-яка їх спільність – фінансове становище, стать, національність, професії та інше [114]. Такі об'єднання в Інтернет-просторі називають он-лайнними.

Процес цифрової трансформації публічного управління розкриває ряд переваг, однією з яких є використання цифрових інструментів у вигляді он-лайнних соціальних мереж, що значно полегшує взаємодію між органами публічної влади, бізнесу та громадськістю в процесі реалізації управлінських рішень.

Серед он-лайнних соціальних мереж виділяють такі види:

1. Власне соціальні мережі (найбільш поширені Facebook, Instagram, MySpace, Twitter та ін.);
2. Системи миттєвого обміну повідомленнями (інтернет-чати): спілкування з іншими користувачами через мережу в режимі реального часу (Skype, ICQ, MSN Messenger та ін.);
3. Інтернет-форуми: надають можливість створювати нові теми, коментувати і обговорювати повідомлення інших користувачів;
4. Веб-блоги – особисті он-лайн журнали окремих користувачів;
5. Вікі-довідники – портали, зміст яких може бути редагований відвідувачами (Wikipedia);
6. Інтернет-хости: розміщення відеоматеріалів на безоплатній основі (YouTube) [41, с. 38].

Питання нормативно-правового регулювання використання соціальних мереж у діяльності органів публічної влади наразі не отримали належної уваги у вітчизняній науці, хоча кількість користувачів соціальних мереж в Україні збільшується, що свідчить про актуальність досліджуваної теми, важливість її теоретичних і практичних аспектів.

Останнім часом у США та країнах ЄС соціальні мережі, такі, як «Твітер» та «Фейсбук», стали способами офіційної комунікації органів державної влади, бізнесу та суспільства. Так, соціальні мережі зазвичай використовуються як інструмент для впливу на суспільство, а також впливу кожної окремої особи на управлінські процеси, що й утворює нові форми комунікації в соціумі.

Термін «соціальна мережа» був введений в 1954 році соціологом з «Манчестерської школи» Джеймсом Барнсом в роботі «Класи і збори в норвезькій острівній парафії», який розвинув винайдений ще в 30-ті роки підхід до дослідження взаємозв'язків між людьми за допомогою соціограм, тобто візуальних діаграм, в яких окремі особи представлені у вигляді точок, а зв'язки між ними – у вигляді ліній [32, с.105]. Таким чином, соціальна

мережа (Social Network) – це соціальна структура, що складається з групи вузлів, якими є соціальні об'єкти (люди або організації) і зв'язків між ними [46, с.15]. З цього поняття випливає власне думка про те, що суспільство – це складне переплетіння взаємовідносин, починаючи з випадкових знайомств і закінчуючи тісними родинними вузлами.

Важливо зазначити, що науковці розглядають поняття «соціальна мережа» в кількох значеннях. Так, Т.Галіч трактує поняття соціальної мережі як структуру, що складається з вузлових елементів і зв'язків між ними – соціальної павутини [11].

Питання використання соціальних мереж в аспекті комунікацій в публічному управлінні розглядається Г.Почепцовим, який вивчає комунікацію в суспільстві, її види, механізми, особливості функціонування, зокрема у сфері вироблення державної політики, та шляхи досягнення поставлених політичних цілей, одним із яких, на його думку, є соціальні мережі, які здатні не лише суттєво впливати, а й створювати власне специфічне «поле спілкування» між органами державної влади та громадянами [58].

В.Бебик розглядаючи особливості комунікацій та інформаційного менеджменту в публічному управлінні, аналізує роботу вітчизняних пресслужб органів влади і вказує на важливість їх роботи щодо повноцінного висвітлення позиції цих органів з усіх питань із використанням доступних методів комунікації [1].

Крім того, соціальну мережу описують як віртуальний майданчик, що забезпечує своїми засобами спілкування, підтримку, створення, розбудову, відображення та організацію соціальних контактів, у тому числі й обмін даними між користувачами, а також обов'язково передбачає попереднє створення облікового запису [129].

У зв'язку з активним використанням інтернет-сервісів у суспільстві виникає питання щодо застосування соціальних мереж і в діяльності органів державної влади України, що робить їх діяльність більш публічною.

Враховуючи трактування поняття «соціальна мережа», використання соціальних мереж у публічному управлінні вирішує низку завдань:

- 1) вплив на формування громадської думки;
- 2) формування відповідальної громадянської позиції;
- 3) популяризація діяльності державних інституцій та створення їх позитивного іміджу;
- 4) привернення уваги до соціально важливих та проблемних питань суспільства;
- 5) формування та зміцнення інститутів громадянського суспільства.

Суспільство стрімко входить в епоху цифрових технологій, при цьому соціальні мережі стають необхідним інструментом для суспільної комунікації, модернізуючись в інструмент інформаційного впливу та маніпулювання масовою свідомістю. Зростання кількості користувачів соціальних мереж безпосередньо пов'язане з динамічним розвитком інтернету та доступу до такого способу зв'язку. За даними Світової статистики користувачів інтернетом, кількість людей, які використовували соціальні мережі, непинно зростає. Так, вже у 2019 р. в «Інстаграм» є найбільше передплатників платного контенту у світі (обчислюється у мільйонах), а «Фейсбук» є найбільшою соціальною мережею у світі з 2,45 млрд активних користувачів щомісяця. Тенденція до використання соціальних мереж поширена і на території України. Цифрова трансформація українського суспільства наближається до такого рівня, коли дії будь-якої людини або діяльність будь-якої організації важко буде уявити без акаунтів в соціальних мережах. Такі акаунти в соціальних мережах вже мають й більшість органів державної влади. Так, особисті сторінки в мережі «Фейсбук» мають і керівники органів публічної влади. Слід зазначити, що кількість передплатників усіх цих сторінок постійно зростає [103., с. 45-46].

Українська аудиторія в соціальних мережах збільшується рекордними темпами. Найбільшу популярність сьогодні в Україні отримали такі он-лайн соціальні мережі, як Fecesebook та Instagram. Лише у 2018 році

кількість користувачів соціальної мережі Fesebook зросла на 3 млн. або на 30 %, а за останні п'ять років – на 9, 8 млн. або на 306, 2 %. На початку 2019 року соціальну мережу Fesebook використовували 13 млн. українців.

Разом з тим, якщо у 2017 році соціальною мережею Instagram користувалися 3, 8 млн. осіб, то у 2018 році – уже 7, 3 млн. Так, у 2018 році кількість користувачів зросла на 50, 7 % – із 7, 3 млн. до 11 млн., у березні 2019 року соціальною мережею Instagram користувалися ті ж 11 млн. осіб [1]. Кількість користувачів соціальної мережі Fesebook динамічно зростає. Водночас, динаміка використання соціальної мережі Instagram в Україні свідчить про значне збільшення кількості їх користувачів, ніж у Fesebook.

Враховуючи суттєві зростання кількості користувачів, можна стверджувати, що соціальні мережі доцільно використовувати не лише, як платформу для реклами, розважальних програм, які забезпечують об'єднання людей у он-лайн спільноти за інтересами, а й як комунікативний інструмент публічного управління.

Аналізуючи інформацію, яку розміщують на сторінках у соціальних мережах органи державної влади та посадові особи найвищої ланки, можна зазначити, що така інформація стає відображенням та одночасно супроводом діяльності органу або відповідної посадової особи. Також у загальному розумінні така інформація відображає пріоритети суспільства та результати проведених реформ.

Як вже зазначалося на с. 60-61 при дослідженні механізмів дії соціальних мереж та способів поширення інформації порушується низка актуальних питань. Це, по-перше, ідентифікація користувачів мережі «Інтернет», по-друге, посилення відповідальності за дотримання авторських прав, по-третє – цифрова безпека, кібергігієна та забезпечення безпеки доступу до баз даних, по-четверте – нормативно-правове врегулювання використання офіційної символіки у соціальних мережах, по-п'яте – питання моралі і цензури (як груп у соціальних мережах, так і органів публічної

влади, а також посадових осіб найвищої ланки, які мають акаунти в соціальних мережах).

З огляду на зазначене виникає потреба у формуванні нової сфери права – цифрового права. В Україні вже активно розробляється законодавство, яке стосується сфери цифровізації. Однак, як вже зазначалося у підрозділі 1.2. ці нормативно-правові акти опосередковано стосуються питань упровадження соціальних мереж у публічному управлінні. На нашу думку, також доцільним є розроблення програми адаптації в публічному управлінні вже існуючих і впровадження нових додаткових можливостей мережі інтернет, зокрема соціальних мереж.

Статтею 1 Закону України «Про телекомунікації» (втратив чинність) визначалося, що Інтернет – всесвітня інформаційна система загального доступу, яка логічно пов'язана глобальним адресним простором та базується на інтернет-протоколі, визначеному міжнародними стандартами [98]. Так, мережу інтернет розуміють як інформаційний простір, який не має чітко визначених меж, що свідчить про можливість реєстрації інформаційного ресурсу резидента України на сервері, який орендується на території будь-якої іншої держави.

В той же час, згідно зі статтею 2 Закону України «Про електронні комунікації» мережа Інтернет (Інтернет) – глобальна електронна комунікаційна мережа, що призначена для передачі даних та складається з фізично та логічно взаємоз'єднаних окремих електронних комунікаційних мереж, взаємодія яких базується на використанні єдиного адресного простору та на використанні інтернет-протоколів, визначених міжнародними стандартами.

Відповідно до Указу Президента України від 31 липня 2000 р. № 928/2000 «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» розвиток національної складової глобальної інформаційної мережі інтернет, забезпечення широкого доступу до цієї мережі громадян та

юридичних осіб усіх форм власності в Україні, належне представлення в ній національних інформаційних ресурсів є одним з пріоритетних напрямів державної політики у сфері цифровізації, задоволення конституційних прав громадян на інформацію.

У зв'язку із цим основними завданнями щодо розвитку національного сегменту мережі інтернет та забезпечення до неї широкого доступу в Україні було заплановано:

- створити в найкоротші строки належні економічні, правові, технічні умови для забезпечення широкого доступу громадян, ЗВО, наукових установ і організацій усіх форм власності, органів публічної влади, суб'єктів підприємницької діяльності до мережі інтернет;

- розширити та вдосконалити подання в мережі інтернет об'єктивної політичної, правової, економічної, соціальної, екологічної, науково-технічної, культурної інформації про Україну, зокрема тієї, що формується в органах публічної влади, ЗВО, наукових установах та організаціях, архівах, а також бібліотеках, музеях, інших закладах культури, розширення можливостей для доступу в установленому порядку до інших національних інформаційних ресурсів, постійне вдосконалення способів подання такої інформації;

- забезпечити конституційні права громадян на вільне збирання, зберігання, використання та поширення інформації, свободу думки і слова, вільне вираження своїх поглядів і переконань;

- забезпечити державну підтримку розвитку цифрової інфраструктури надання інформаційних послуг; створення умов для розвитку підприємницької діяльності та конкуренції в галузі використання каналів цифрового зв'язку, створення можливостей для забезпечення потреб на пільгових умовах у зазначених послугах ЗВО, наукових установ та організацій, громадських організацій, а також бібліотек, музеїв, інших закладів культури, закладів охорони здоров'я, включаючи розташовані в сільській місцевості;

- здійснити розвиток та впровадження сучасних цифрових технологій у сфері публічного управління, фінансовій сфері, підприємницькій діяльності, освіті, наданні медичної та правової допомоги та інших сферах;

- гарантувати інформаційну безпеку держави, недопустити поширення заброненої законодавством інформації;

- удосконалити правове регулювання діяльності суб'єктів інформаційних відносин, виробництва, використання, поширення та зберігання електронної інформаційної продукції, захисту прав на інтелектуальну власність, посилення відповідальності за порушення встановленого порядку доступу до електронних інформаційних ресурсів усіх форм власності за навмисне поширення комп'ютерних вірусів [78].

Важливим напрямом розвитку законодавства є закріплення правових норм поширення інформації органами публічної влади в соціальних мережах.

Водночас відповідно до пункту 2 Порядку оприлюднення у мережі інтернет інформації про діяльність органів виконавчої влади, затвердженого постановою Кабінету Міністрів України від 4 січня 2002 р. № 3, оприлюднення в мережі «Інтернет» інформації про діяльність органів виконавчої влади здійснюється шляхом:

- розміщення і постійного оновлення міністерствами, іншими центральними та місцевими органами виконавчої влади інформації відповідно до вимог Закону України «Про доступ до публічної інформації» та цього Порядку на офіційних вебсайтах (вебпорталах);

- функціонування та модернізації Єдиного вебпорталу Кабінету Міністрів України, призначеного для інтеграції офіційних вебсайтів (вебпорталів) органів виконавчої влади та розміщення інформаційних ресурсів відповідно до потреб громадян [74].

Незважаючи на те, що на рівні ЄС була прийнята 24 жовтня 1995 р. Директива 95/46 про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних, а також інші специфічні документи, які доповнюють і гарантують право на захист даних на рівні ЄС, але оскільки

більшість постачальників послуг соціальних мереж (наприклад Фейсбук) постійно проживає за рамками ЄС, то вони не здійснюють своїх зазначених вище функцій регулювання [180].

Ураховуючи викладене вище, зазначимо, що використання мережевих технологій у публічному управлінні є одним із пріоритетних напрямів державної політики цифрового розвитку всіх сфер життєдіяльності суспільства. Впровадження сучасних цифрових інструментів органами державної влади є одним з універсальних механізмів цифрового врядування у процесі прийняття управлінських рішень, а також одним з основних методів удосконалення сфери публічного управління, які мають бути спрямовані на конкретні зміни в діяльності органів державної влади, введення нових форм і засобів роботи державних службовців.

Соціальні мережі – потужний та ефективний цифровий інструмент, що має величезні можливості, які потрібно використовувати в публічному управлінні.

Сьогодні не всі органи публічної влади позиціонують себе в соціальних мережах, хоча соціальні мережі й відіграють важливу роль у комунікації органів публічної влади в мережі інтернет, оскільки дають можливість у часовому інтервалі безперервно комунікувати органам державної влади з органами місцевого самоврядування, бізнесом та суспільством у цілому.

Фактичний стан використання соціальних мереж українськими користувачами, як інструменту реалізації мережевих технологій в публічному управлінні, зумовлює:

- вільний доступ до інформації, якою володіють органи державної влади;
- забезпечить оперативну поінформованість громадськості, що включає актуальність та достовірність інформації;
- забезпечить громадський контроль за діяльністю органів державної влади, а також взаємодію громадян, бізнесу та органів публічної влади.

Впровадження соціальних мереж в публічному управлінні має бути цілеспрямованим та керованим процесом, який передбачає взаємодію держави, бізнесу та суспільства у режимі он-лайн. Соціальні мережі виступають ефективним засобом он-лайн управління, а їх використання зумовлює глобальний розвиток цифрових технологій, що сприяє зручному та швидкому прийняттю управлінських рішень. Перспективним, на нашу думку, є подальший пошук нових ідей впровадження соціальних мереж у публічному управлінні.

Цифрова трансформація публічного управління є важливим фактором сучасного цифрового розвитку України. Таким чином, в умовах реалізації мережевих технологій в публічному управлінні важливим у процесі управлінської діяльності є не тільки впровадження комп'ютерних новацій, але і використання соціальних мереж, які сприяють інформуванню громадян та бізнесу, а також реалізації управлінських рішень. Необхідно враховувати переваги та загрози мережевої форми управління, різноманітність мережевих структур та форм їхньої організації.

Під час збройної агресії з боку рф наша держава в інформаційному протистоянні, намагаючись забезпечити належний рівень інформаційного суверенітету, успішно протидіє дестабілізуючим інформаційним впливам.

З розвитком цифрового суспільства, соціальні мережі сприяють зростанню можливостей впливу на соціум. Мережеві технології можуть використовуватись в якості інструменту інформаційного управління масовою свідомістю людей, більшість з яких не здогадується і не усвідомлює реальну і потенційну небезпеку використання даних, які вони поширюють у соціальних мережах. Так, всесвітня мережа інтернет ставить перед державою нові завдання, вирішення яких впливає на різноманітні сфери життя українського суспільства, відкриваючи принципово нові можливості для поширення інформації та організації спілкування між громадянами.

Світовий досвід використання інтерактивних технологій через створення цифрових інформаційно-комунікативних платформ (майданчиків)

між суспільством і владою, організацію онлайнового доступу до проектів та чинної нормативно-правової бази, перенесення активності органів публічної влади і окремих її представників у соціальні мережі кардинально змінює публічно-управлінський ландшафт [27, с. 63-64].

На сьогоднішній день в Україні, недооцінюють наскільки впливовими можуть бути соціальні мережі не тільки у спектрі спілкування та коментування он-лайн, але й в управлінському аспекті, соціальному та й взагалі в умовах глобальної цифровізації.

Соціальні мережі стали не лише засобом спілкування, а й засобом вираження активної громадянської позиції, формування суспільної думки, впливу на політичні рішення влади. З іншого боку, соціальні мережі є одним з найбільш небезпечних інструментів інформаційно-психологічного впливу й маніпулювання масовою свідомістю і становлять загрозу стабільності та національній безпеці будь-якої країни, в тому числі України [47, с.47].

Сьогодні соціальні мережі надають користувачам широкий спектр обміну інформацією, їх відвідує чимала кількість он-лайн аудиторії у всьому світі. Вони займають передові позиції за популярністю он-лайн категорій після пошукових та інформаційних порталів, програмного забезпечення. Таким чином, переваги використання соціальних мереж полягають у вільному та швидкому доступі до інформації. При системному розгляді різних методів поширення інформації в соціальній мережі відповідно до загальних характеристик виділяють:

- розміщення інформації у власному співтоваристві або тематичному обліковому записі за максимальним рівнем популярності серед безкоштовних методів поширення інформації в соціальній мережі. Так, високий ступінь довіри користувачів до інформації, що публікується, дозволяє залучати більшу кількість користувачів, що підвищує її пошуковий індекс;

- конкурси в соціальній мережі – інноваційний метод поширення інформації в соціальній мережі, що передбачає проведення промо-конкурсів для залучення користувачів. Так, висока швидкість розповсюдження і довіра

до інформації з боку користувачів спонукає їх постити її серед друзів (у відсилаємому повідомленні якраз міститься поширювана інформація і запрошення взяти участь у конкурсі);

– спам – частково неконтрольований та безкоштовний метод поширення інформації в соціальній мережі. Так, даний метод передбачає поширення інформації шляхом розсилки особистих повідомлень користувачам, тобто користувач може поширювати будь-яку інформацію, у тому числі й протизаконну. Однак адміністрація соціальної мережі бореться з цим явищем шляхом блокування акаунтів, встановлення спам-фільтрів, обмеження обсягу вибірки за запитом тощо;

– несанкціонована розсилка повідомлень по «стінам» великих спільнот є максимально ефективнішим методом поширення інформації в соціальних мережах на відміну від розсилки особистих повідомлень. Так, даний метод не схильний до модерації з боку адміністрації соціальної мережі, що дозволяє охопити більшу аудиторію, не зважаючи на це все однозахистом спільноти від нелегітимної інформації займаються адміністратори спільноти;

– контекстна реклама – платний, але високоефективний метод поширення інформації в соціальних мережах, що дає можливість вибору цільової аудиторії по ряду параметрів (демографія, географія, інтереси, освіта, робота тощо). Так, даний метод дозволяє демонструвати рекламні оголошення на особистій сторінці користувача і в додатках соціальної мережі згідно з обраними параметрами. Однак поширювана інформація має обмеження, які встановлено адміністрацією соціальної мережі та проходить модерацію перед розповсюдженням.

Розглянувши наведені методи поширення інформації в соціальних мережах, вважаємо за доцільне додатково виокремити новий неконтрольований та безкоштовний метод поширення інформації в соціальних мережах – власна, особиста та конфіденційна інформація. Так, даний метод має різноплановий, а в ряді випадків й завершальний характер, оскільки користувач фактично сам складає на себе «досьє» (автобіографічні

дані, відомості про професійну діяльність, особисті уподобання, спосіб життя, відмічає своє місцезнаходження, свою присутність на фотографіях тощо), та фактично повні відомості про своє оточення (список контактів, із повним досьє на кожного суб'єкта). Така інформація про користувача, зокрема державного службовця або високопосадовця, стає об'єктом розвідки на основі відкритих джерел (OSINT), що може становити загрозу національній безпеці в умовах збройної агресії проти України.

У разі обробки, систематизації та аналізу інформації, розміщеної користувачем, за різноманітними пошуковими реквізитами, можна отримати майже ідеальний для будь-якої спецслужби, діяльність яких перебуває поза межами правового регулювання нашої держави, пошуково-довідково інформаційний масив для виявлення осіб, які становлять інтерес, їх вивчення та розробки тощо [60, с. 76].

Доречно зауважити, що з метою попередження таких проявів має бути задіяна низка складових структурних елементів державного механізму з урахуванням сформованої стратегії технічного захисту інформації та стратегії безпеки захищеної інформації, а також спільної роботи власників, розробників та користувачів мережі, а також уповноважених державних органів. Становлення цифрового суспільства призвело до загальної цифровізації та впровадження цифрових технологій в усі сфери життя. В результаті комплексного підходу до вивчення порушеного питання, можна зробити висновок, що власна конфіденційна інформація, як об'єкт поширення в соціальних мережах, досі не досліджувався, а проблематика захисту інформації користувачів в соціальних мережах залишається актуальною.

Роль соціальних мереж, незважаючи на існуючі проблеми, набуває змістовного значення, як феномена інформаційного обміну під час процесу цифровізації суспільства. Вони стають пріоритетним майданчиком для прийняття управлінських рішень органами влади та комунікації з громадянами. Варто зазначити, що на сьогодні не існує єдиних механізмів

використання соціальних мереж органами державної влади, що пов'язано з відсутністю як законодавчого врегулювання даного питання, так і наявністю постійного розвитку й трансформацій самих мереж, що підкреслює актуальність даної теми та вимагає більш ґрунтовних подальших досліджень.

Інформаційно-комунікативні технології та породжувані ними численні медіа-комунікації утворили покоління так званих «нових медіа», які ґрунтуються на цифровому відтворенні інформації. Вони стали не лише засобами виконання безпосередньо комунікативних та інформаційних функцій, але й спричинилися до формування культурних феноменів та практик [17, с. 136].

Сьогодні поняття соціальної мережі дещо модернізувалось та асоціюється з Інтернет платформами для віртуальних комунікацій. Тобто, термін соціальні мережі можна розуміти як віртуальну (онлайн) платформу, веб-сервіс, веб-сайт або портал в Інтернеті, що об'єднує велику кількість людей, надаючи їм все більше можливостей для цифрової комунікації між собою. Масова комунікація впливає на формування суспільної свідомості групи й особистості, на формування громадської думки та створення соціальних стереотипів. Тут же приховані можливості маніпулювати й управляти суспільною свідомістю, фактично здійснювати функцію соціального контролю [18, с. 66]. Як спосіб маніпуляції свідомістю використовують фейки шляхом висвітлення неточної інформації або частини інформації, спотворення контексту з метою підштовхування суспільства до дій або формування думок, які потрібні маніпулятору.

Враховуючи те, що майже кожному громадянину, в тому числі й публічному службовцю, відомо про соціальні мережі, розглянемо основні психологічні та соціальні аспекти використання облікових записів в соціальних мережах, які можуть впливати на масову свідомість суспільства, а саме:

– більшість користувачів мережі Інтернет відвідують веб-сайти органів публічної влади чи інші офіційні сторінки тільки в разі потреби, а

соціальні мережі – багато разів на день, що свідчить про поширення інформації на більшу аудиторію;

- соціальні мережі долають психологічні бар'єри та забезпечують доступ до інформації, в тому числі й про діяльність та комунікацію органів публічної влади, більш доступним для суспільства;

- у соціальних мережах оперативніше розповсюджується інформація, викликаючи більшу зацікавленість користувача, який може підписуватись на конкретно визначений обліковий запис з метою отримання необхідної інформації і не виключено, що така інформація може містити недостовірні дані;

- у соціальних мережах публікується інформація із зазначенням посилання на інший обліковий запис чи неофіційне джерело, які у подальшому можуть коментуватися користувачами. Крім цього, таке повідомлення на облікових записах органів публічної влади може містити недостовірну або неповну інформацію;

- на підставі індивідуальних ознак, які характеризують підписників облікових записів в соціальній мережі (наприклад, вік, стать, освіта, частота коментування тощо), розпорядники облікових записів, власне й всі інші користувачі соціальної мережі, зможуть аналізувати рівень актуальності та важливості інформації для суспільства, а також рівень зацікавленості у такій інформації. Однак, якщо такі індивідуальні ознаки містять недостовірну інформацію, це унеможлиблює правдивість та повноту таких даних.

Поширення фейкової інформації в соціальних мережах здійснюється з метою впливу на масову свідомість, непомітного нав'язування певних думок та використання такої інформації на підсвідомості під час віртуального (онлайн) спілкування.

Спілкування здійснюється за допомогою інформації, яка в процесі комунікації завжди впливає на психіку особистості. Соціопсихологічна інформація визначає поєднання знань, повідомлень та фактів про ситуацію,

функціонування та тенденції розвитку об'єктно-суб'єктних, суб'єктно-об'єктних і суб'єктно-предметних відносин, що виникають в суспільстві. Тобто, певний систематизований та обґрунтований масив такої інформації ґрунтується на системних знаннях про потреби, інтереси, почуття, настрої, думки, мотивації та поведінку людей [167, с. 27].

З огляду на викладене, слід наголосити, що використання соціальних мереж є дієвим процесом, який дозволить аналізувати процес масової цифрової комунікації, здійснювати прогнозування формування громадської думки та виявляти приховані можливості маніпулювання й управління суспільною свідомістю. При цьому, важливим залишається питання комунікації реальної (фізичної) з віртуальною (онлайн) активністю органів державної влади з громадянами та бізнесом з метою врахування висловлених в соціальних мережах пропозицій, зауважень, ініціатив тощо. Перспектива такої взаємодії передбачає виокремлення переваг використання соціальних мереж у виробленні державної політики України.

На стадії свого становлення соціальні мережі в основному використовувалися лише для спілкування та розваг. Сучасні комунікаційні технології дозволяють створювати соціальні спільноти (Інтернетком'юніті) з практично будь-якими заданими характеристиками – освітніми, професійними, віковими. Вони формуються на тлі акселерації соціального часу і посилення динаміки комунікаційних форм у процесі суспільного відтворення [20, с. 56].

Соціальні мережі співставні в сучасній соціокультурній ситуації із засобами масової комунікації, тому вони виконують всі функції засобів масових комунікацій. За критерієм періодичності, доступності, фінансовим критерієм, мережева комунікація є найбільш ефективною в сучасному комунікативному просторі. Традиційні засоби масової комунікації виступають в якості центрів, спочатку акумулюють інформацію, потім її сортують і розповсюджують. Соціальні мережі характеризуються потенційно нескінченним числом незалежних центрів акумуляції і поширення

інформації, що визначає її глобальність, демократичність, але й безконтрольність. Ці характеристики закладають нові смислові конструкти в організації комунікативного простору сучасного суспільства.

Науковці, розглядаючи феномен соціальних мереж у контексті становлення і розвитку мережевого суспільства, стверджують, що вони стають все більш популярними, більш мобільними і більш закритими для «не членів соціальної групи» [20, с. 58].

Розвиток соціальних мереж у сфері державного управління включатиме технологічні та стратегічні зміни, спрямовані на поліпшення комунікації, ефективності та взаємодію всіх учасників, зокрема можна виділити такі шляхи:

- *посилення мобільності*: соціальні медіа платформи будуть оптимізовані для зручного використання та отримання доступу державних службовців до необхідної інформації та комунікацій у будь-якому місці їх розташування;

- *використання алгоритмів штучного інтелекту*: інтеграція інтелектуальних технологій сприятиме технологічній оптимізації процесів взаємодії органів державної влади, покращенню персоналізації, аналітики, оцінювання та прогнозування соціальних платформ;

- *провадження кібербезпеки*: з урахуванням зростання важливості соціальних мереж у публічному управлінні, будуть впроваджені технології захисту важливої інформації та забезпечення конфіденційності державних службовців;

- *розширення сфери застосування*: вдосконалення комунікації між різними рівнями адміністрування, а також залучення громадян до процесів прийняття рішень;

- *розвиток внутрішніх месенджерів та корпоративних мереж*: органи державної влади будуть сприяти розвитку як внутрішніх, так і зовнішніх мереж корпоративних комунікативних платформ для поліпшення

співпраці між різними структурними підрозділами та партнерами в інших публічних секторах;

– *покращення зворотної комунікації*: спрямованість на ефективну взаємодію з громадянами сприятиме розробці інструментів зручного отримання зворотного зв'язку, висловлення думок та участі в процесах державного управління.

Так, особливо зворотний зв'язок може сприяти значному підвищенню ефективності обміну управлінською інформацією. Обмін інформацією між учасниками комунікативних відносин можна поліпшити, створивши системи зворотного зв'язку, регулюючи інформаційні потоки, впроваджуючи управлінські дії для формування різноманітних гілок інформаційного обміну, розгортаючи системи збору пропозицій, друкуючи матеріали інформаційного характеру для використання всередині суб'єкта чи об'єкта таких відносин, застосовуючи сучасні інформаційні технології тощо [51].

Отже, соціальні мережі стають сучасною цифровою платформою, яка є альтернативою засобам масової інформації і може досить продуктивно використовуватись в публічному управлінні. Аналізуючи вплив мережевих технологій на соціум, слід акцентувати увагу на важливому значенні мережевих технологій як на локальному, регіональному, так і на більш масштабному, глобальному рівні. Інтернет – це всесвітня система локальних і глобальних, приватних, публічних, академічних, ділових і урядових мереж, пов'язаних між собою через використання різноманітних дротових, оптичних і бездротових технологій. Інтернет становить фізичну основу для розміщення інформаційних ресурсів і послуг, зокрема гіпертекстових чи мультимедійних документів, електронної пошти та інших засобів цифрового зв'язку [126].

Доречно зауважити, що з точки зору діяльності державного управління, соціальні мережі необхідно застосовувати як інструмент реалізації державної політики, як середовище формування громадянського суспільства та як засіб поінформованості суспільства з урахуванням виконуваних ними функцій.

Висновки до розділу 1

Проведено дослідження стану наукових пошуків з питань застосування технологій мережевої організації у державному управлінні. Аналізом встановлено, що науковий інтерес до досліджуваної теми залишається актуальним і широким. Застосування технологій мережевої організації в державному управлінні розглядається як один із шляхів покращення якості та ефективності управління, сприяння взаємодії між різними державними органами та стейкхолдерами/беніфіцарами, а також підвищення ступеня прозорості та відповідальності.

Доведено, що мережеве управління може сприяти забезпеченню більш сталого розвитку, балансуючи економічні, соціальні та екологічні аспекти діяльності. Використання мережевого підходу здатне покращити прозорість та відкритість в державному управлінні, що сприятиме зменшенню корупції та підвищенню відповідальності. Наукові розробки зосереджуються на вивченні різних аспектів, таких як впровадження інформаційних систем та цифрових технологій, створення механізмів співпраці між органами влади, розвиток цифрового врядування, аналіз впливу технологій на прийняття рішень та взаємодію з громадськістю.

Констатовано, що застосування технологій мережевої організації у державному управлінні дозволяє краще адаптуватися до змін в оточуючому середовищі, включаючи економічні, політичні та соціокультурні зміни. У глобальному контексті мережева організація діяльності може сприяти співпраці між різними країнами та міжнародними організаціями для вирішення глобальних проблем, таких як зміна клімату, боротьба з пандемією, міграція та інші. Зважаючи на швидкі зміни у сфері інформаційно-комунікативних технологій і їхній вплив на суспільство та управління, досліджувана тема лишається актуальною, привертає увагу науковців та практиків у галузі державного управління та потребує подальших наукових пошуків.

Систематизовано еволюційні періоди розвитку типів організаційних мереж, вважаючи їх початком лінійні, затим функціональні та лінійно-функціональні мережі, згодом – дивізіональні та матричні; обґрунтовано, що на сучасному етапі відбувається новий період суспільного розвитку в умовах глобалізації та стрімко формується нова організаційна структура управління – мережева, розвиток якої став можливим завдяки зростанню інформаційно-комунікативних та цифрових зв'язків між органами державної влади, приватними компаніями та громадянами.

Проаналізовано закони та підзаконні акти України у сфері реалізації мережевого управління у діяльності органів державної влади, що дало змогу встановити їх суб'єктивність розподілу на відповідні групи (ВРУ, Президент України, КМУ): закони, Укази Президента України, постанови та розпорядження Кабінету Міністрів України. Визначено генезу правового формування механізмів мережевого управління у діяльності органів державної влади, яка ґрунтується на історико-правовому підході і має власну періодизацію. Визначено 4 етапи правового формування механізмів мережевого управління у діяльності органів державної влади, зокрема: перший етап (1973 – 1996 рр.); другий етап (1998 – 2003 рр.); третій етап (2004 – 2015 рр.) та четвертий – (2016 р. – до тепер).

Нагальним залишається питання нормативно-правового врегулювання використання соціальних мереж органами державної влади, вирішення якого потребує комплексного підходу з урахуванням наукових досліджень у цій сфері. Встановлено, що власна (конфіденційна) інформація, як об'єкт поширення у соціальних мережах, досі окремо не досліджувався, а тому проблематика захисту інформації про користувачів в соціальних мережах залишається актуальною.

Встановлено, що роль соціальних мереж, незважаючи на існуючі проблеми, набуває змістовного значення, як феномена інформаційного обміну під час процесу цифровізації суспільства, що стають пріоритетним майданчиком для прийняття державно-управлінських рішень органами влади

та потужним засобом комунікації з громадянами різних цільових аудиторій. Варто зазначити, що на сьогодні не існує єдиних механізмів використання соціальних мереж органами державної влади, оскільки це пов'язано з відсутністю законодавчого врегулювання особливостей їх функціонування, а також з постійним розвитком та трансформаціями самих мереж, що підкреслює актуальність даної теми та вимагає системних та ґрунтовних подальших досліджень.

Наголошено, що використання соціальних мереж дозволить аналізувати процес масової цифрової комунікації, здійснювати прогнозування формування громадської думки та виявляти приховані можливості маніпулювання й управління суспільною свідомістю. При цьому, важливим залишається питання комунікації реальної (фізичної) з віртуальною (онлайн) активністю органів державної влади з громадянами та бізнесом з метою врахування висловлених в соціальних мережах пропозицій, зауважень, ініціатив тощо. Перспектива такої взаємодії передбачає виокремлення переваг використання соціальних мереж у формуванні та реалізації державної політики.

Визначено тенденції розвитку соціальних мереж у сфері державного управління, які охоплюватимуть технологічні та стратегічні зміни, спрямовані на поліпшення комунікації, ефективність та взаємодію всіх учасників, а саме:

- *посилення мобільності*: соціальні медіа платформи будуть оптимізовані для зручного використання та отримання доступу державних службовців до необхідної інформації та комунікацій у будь-якому місці їх розташування;

- *використання алгоритмів штучного інтелекту*: інтеграція інтелектуальних технологій сприятиме технологічній оптимізації процесів взаємодії органів державної влади, покращенню персоналізації, аналітики, оцінювання та прогнозування соціальних платформ;

- *провадження кібербезпеки*: з урахуванням зростання важливості соціальних мереж у публічному управлінні, будуть впроваджені технології захисту важливої інформації та забезпечення конфіденційності державних службовців;
- *розширення сфери застосування*: вдосконалення комунікації між різними рівнями адміністрування, а також залучення громадян до процесів прийняття рішень;
- *розвиток внутрішніх месенджерів та корпоративних мереж*: органи державної влади будуть сприяти розвитку як внутрішніх, так і зовнішніх мереж корпоративних комунікативних платформ для поліпшення співпраці між різними структурними підрозділами та партнерами в інших публічних секторах;
- *покращення зворотної комунікації*: спрямованість на ефективну взаємодію з громадянами сприятиме розробці інструментів зручного отримання зворотного зв'язку, висловлення думок та участі в процесах державного управління.

Основні результати розділу 1 опубліковано в наукових працях автора: [103; 106; 108; 109; 110, 197].

РОЗДІЛ 2

УКРАЇНСЬКИЙ ТА ЗАРУБІЖНИЙ ДОСВІД ЗАСТОСУВАННЯ МЕРЕЖЕВОГО УПРАВЛІННЯ У ДІЯЛЬНОСТІ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ

2.1 Практика організації мережевих структур державного управління в Україні

В Україні триває активний процес формування інформаційного простору та інтеграція до нього всіх основних галузей суспільної діяльності, найголовнішим об'єктом якої є інформація та знання, а також шляхи доступу до них.

Світ увійшов до якісно нової історичної епохи – епохи цифровізації, коли суттєво нового значення набуває мережа інтернет і все, що з нею пов'язано.

Важливим аспектом підвищення ефективності державного управління в сучасному інформаційному суспільстві є цифрова трансформація традиційних галузей суспільного життя, розвитку цифрової інфраструктури, а також впровадження цифрових технологій. В умовах розвитку цифрового суспільства та в сучасних конкурентних умовах для функціонування органів державної влади необхідним є пошук ефективних шляхів прийняття управлінських рішень. Особливого значення при цьому набуває впровадження нових мережевих технологій у сфері державного управління, що визначено одним із пріоритетних завдань на сучасному етапі державного розвитку.

Процес глобалізації в державі визначає нові напрями наукових досліджень та призводить до загострення існуючих і виникнення нових розбіжностей, які мають різні форми.

Розвиток сучасного суспільства обумовлено комплексним впливом сукупності найважливіших тенденцій та факторів, що впливають на процес

цифровізації. Використання мережевих технологій в державному управлінні розширює можливості органів влади, які спрямовані на швидке інформування населення про їх діяльність та прийняті управлінські рішення, двостороннього зв'язку із суспільством. Таким чином, громадяни мають змогу брати участь у реалізації державної політики, пропонувати альтернативні шляхи вирішення тих або інших питань та отримувати якісні управлінські послуги.

Сучасне громадянське суспільство стає все більш залежним від цифрових технологій, відбувається «цифровий перехід» від систем і процесів індустріальної економіки і інформаційного суспільства до «цифрової» економіки та «цифрового» суспільства. Така трансформація приводить до появи нових, унікальних систем і процесів, що становлять їх нову ціннісну сутність [45, с. 7]. Водночас, прикладне застосування цифрових технологій є інструментом для досягнення цілей, що пов'язано з різними сферами життєдіяльності людини та країни. Таким чином, цифровізацію варто розглядати як інструмент, а не як самоціль [123].

На думку науковців, цифровізацію (digitalization) у широкому розумінні слід трактувати як процес впровадження цифрових технологій для вдосконалення життєдіяльності людини, суспільства і держави [45, с. 7].

Крім цього, поняття «цифровізація» застосовується у Концепції розвитку цифрової економіки та суспільства України на 2018 – 2020 роки, схваленої розпорядженням Кабінету Міністрів України від 17.01.2018 № 67-р [6], яке визначається як насичення фізичного світу електронно-цифровими пристроями, засобами, системами та налагодження електронно-комунікаційного обміну між ними, що фактично уможливорює інтегральну взаємодію віртуального та фізичного, тобто створює кіберфізичний простір.

Враховуючи зміст поняття «цифровізація» необхідно зауважити, що розвиток відповідної технічної бази не вирішить усіх проблем у системі державного управління, але може істотно підвищити ефективність роботи. Адже застосування новітніх технічних засобів супроводжується

оптимізацією організаційних процедур, що робить їх більш простими і логічно витриманими [40]. Ефективність роботи системи державного управління залежить від рівня взаємодії держави з громадянами і бізнесом, якості роботи кожної установи, взаємодії органів влади між собою.

Забезпечення ефективності державного управління в сучасних умовах розвитку цифрового суспільства не може бути досягнуто без реалізації цифрових технологій у цій сфері. Це свідчить про беззаперечну перевагу функціонування цифрового врядування, підґрунтям якого є запровадження в органах державної влади автоматизованої системи документообігу. Однак, паралельно з функціонуванням цифрового документообігу в деяких органах державної влади ще досі використовується система паперового документообігу, яка є досить повільною, призводить до значних ресурсних втрат, що потрібні для роботи поштових служб, канцелярій, які змушені реєструвати вхідні і відправляти вихідні документи. Зазначені обставини зумовлюють необхідність забезпечення процесів додаткової реєстрації відомостей про документ і сканування тексту для включення його до бази документів. Тобто використання застарілих методів роботи у цьому випадку тільки ускладнює робочий процес замість того, щоб його спрощувати.

З огляду на викладене, важливим аспектом є не лише цифрова реєстрація первинної або вихідної документації, якості цієї інформації, її повноти, своєчасності й подальшого використання, а й права отримання інформації, черговості й пріоритету її використання. Так, кадрові ресурси державних установ (від рядових співробітників до керівників вищої ланки) все більше поповнюються працівниками, які вміють працювати з цифровими технологіями. «Цифрове» робоче місце сприяє гнучкості у методах виконання роботи, стимулює спільну роботу та взаємодію з іншими працівниками, підтримує децентралізовані, мобільні робочі середовища та передбачає вибір технологій особисто працівниками. Серед переваг «цифрових» робочих місць – зниження витрат на апаратне забезпечення, офісні приміщення, відрядження. Окрім цього, «цифрові» середовища більш

конкурентоспроможні при пошуку працівників завдяки можливості запропонувати сучасну, інноваційну корпоративну культуру, кращий баланс між роботою та особистим життям і соціальний стиль роботи [40].

Цифрові системи органів державної влади є сукупністю взаємопов'язаних програмно-технічних елементів та відповідного організаційного, нормативно-правового, лінгвістичного і технологічного забезпечення для здійснення їх інформаційно-комунікативної діяльності [27, с. 292]. Також слід врахувати, що функціонування системи цифрового врядування, як взаємодії органів державної влади з громадянами та бізнесом, для підвищення якості надання управлінських послуг має відбуватися на всіх рівнях ієрархії влади.

Як наголошує М.Я. Швець [125, с. 93], цифрове врядування необхідно розглядати передусім, як форму організації публічного управління, яка характеризується застосуванням цифрових (інформаційно-комп'ютерних) технологій на кожному рівні та етапі такого управління. І.Б. Коліушко [36, с. 138] також звертає увагу на використання в органах державної влади сучасних технологій, у тому числі й інтернет-технологій.

Цифрове врядування є одним з інструментів розвитку цифрового суспільства, запровадження якого сприятиме створенню умов для відкритого і прозорого функціонування органів державної влади. Так, цифрове врядування складається з трьох важливих елементів взаємодії: взаємодії держави і громадянина; взаємодії держави та бізнесу; взаємодії органів влади між собою.

Мережеві технології не є вирішенням проблеми взаємодії органів державної влади з громадянами та бізнесом, але з їх допомогою можливо істотно підвищити ефективність такої взаємодії та реалізації цих трьох елементів. При цьому, громадяни отримують доступ до публічної інформації, якісні електронні довірчі послуги, мають можливість впливу на прийняття і реалізацію важливих управлінських рішень. Бізнес отримує спрощений, більш швидкий доступ до органів державної влади, що в свою чергу

допоможе більш ефективно і результативно співпрацювати бізнесу і владі. Органи влади – отримують можливість координувати свої дії, більш ефективно і оперативно вирішувати ті чи інші завдання, підвищити якість надання адміністративних послуг, бути відкритими та прозорими, чіткими та гнучкими до вимог громадян та бізнесу.

Реалізація мережевих технологій призведе до оптимізації організаційної функції державного управління, роблячи її більш простою і логічною. Запровадження цифрового врядування означає трансформацію усіх форм діяльності органів влади, зміну їх структури та принципів виконання завдань і функцій. Успіх цього переходу залежить від правильної стратегії і тактики, координації та ефективної взаємодії усіх учасників цього процесу, а саме: законодавчої, виконавчої та судової гілок влади, бізнесу та громадськості.

Реалізація мережевих технологій спрямована на розвиток цифрового врядування в Україні задля досягнення європейських стандартів, відкритості та прозорості влади для громадян, представників бізнесу та суспільства в цілому. Однак, до цього також додається низька якість управління розробкою, впровадженням, підтримкою функціонуванням та розвитком інформаційно-комунікаційних систем та ресурсів органів державної влади. Такі системи й ресурси часто створюються в результаті окремих ініціатив, для вирішення окремих поточних завдань і часом навіть не узгоджуються між собою.

Порядок впровадження стратегії цифровізації суспільства є абсолютно реальним завданням держави, яке створює правове поле для реалізації основних завдань і програми цифровізації, в основі яких лежить не подальше насичення технікою, а формування правових, організаційних, науково-технічних, економічних, фінансових, методичних і гуманітарних передумов розвитку цифрового суспільства. Це головне в реалізації та розвитку сучасних цифрових технологій у відповідних сферах суспільного життя, формуванні системи національних інформаційних ресурсів, створенні

загальнодержавної мережі цифрового забезпечення сфери державного управління, науки, освіти, культури, охорони здоров'я тощо, створенні загальнодержавних систем інформаційно-аналітичної підтримки діяльності органів державної влади.

Функціонування автоматизованої системи документообігу в органах державної влади є кроком до реалізації програми цифровізації. Однак, законодавством не визначено процедуру, спрямовану на окреслення дій органів державної влади, які не мають автоматизованої системи документообігу. На нашу думку, варто врахувати можливість взаємодії органів влади між собою за допомогою мережевої системи електронної пошти. У цьому контексті така система потребуватиме встановлення комплексної системи захисту інформації та доповнення додатковими елементами, такими як засоби роботи з формами, використання кваліфікованого електронного підпису (далі – КЕП) тощо.

Також, актуальною є й проблема недостатнього захисту інформації в інформаційно-комунікаційних мережах органів державної влади. До того ж подальший розвиток і поширення систем цифрового врядування лише посилюватимуть значимість безпекової складової серед питань забезпечення їх поточного функціонування. Для цифровізації суспільства в Україні потрібні ефективні механізми впровадження державної політики цифрового розвитку, одним із ключових елементів якої є реалізація мережевих технологій у сфері державного управління.

Глобальна цифровізація суспільства є реакцією на здійснення четвертої індустріальної революції. Основним драйвером першої індустріальної революції була механізація ручної праці, другої – застосування електроенергії та масовість виробництва, третьої – електроніка та автоматизація процесів управління через використання інформаційних технологій (виникає поняття «інформатизація», а згодом «електронне урядування»), натомість четвертої – цифровізація (цифрова трансформація), яка пов'язана із впровадженням кіберфізичних систем, які поєднують за

допомогою мережевих комунікаційних технологій реальні (матеріальні, біологічні) та віртуальні об'єкти [2; 59]. Таким чином, досягти в Україні належного європейського рівня цифровізації, а також подолати наявні проблеми, дозволить реалізація мережевих технологій у діяльності органів державної влади.

Створення стійкого цифрового суспільства – це також питання національної безпеки, незалежності держави, конкуренції українських компаній і, насамперед, ефективного прийняття державно-управлінських рішень. На сьогодні цифрові технології виступають основою для реформування державного управління, економіки, бізнесу, соціальної сфери і всього суспільства, а реалізація мережевих технологій є інструментом для ефективного їх розвитку.

Формування глобального кіберпростору створює численні ризики для безпеки держави, загрожують її фінансово-економічній стійкості, спроможності та незалежності урядів. Щоб керувати цими кіберзагрозами, країна повинна мати відповідні оціночні інструменти аналізу загального розвитку кібербезпеки.

Сучасним глобальним інструментом оцінювання кібербезпеки є Національний індекс кібербезпеки (National Cyber Security Index, NCSI), який починаючи з 2016 року вимірює готовність країн запобігати кіберзагрозам і керувати кіберінцидентами. Цей індекс є практичним інструментом для створення потенціалу національної кібербезпеки, розвитку безпечних цифрових суспільств в країнах, що розвиваються, оцінюючи їх поточну ситуацію з кібербезпекою, визначаючи прогалини в потенціалі та обмінюючись рекомендаціями.

Основними кіберзагрозами, що оцінює NCSI, є неможливість надання електронних послуг через їх недоступність, порушення цілісності даних через їх несанкціоновану зміну, а також порушення конфіденційності даних через розкриття таємниці. Ці загрози безпосередньо впливають на стабільне функціонування національних інформаційно-комунікаційних систем та

електронних послуг. Оцінка кіберзагроз здійснюється на основі чотирьох груп показників, які характеризують 1) розробку політики кібербезпеки, 2) кіберзагрози та інформацію, 3) освіти та підвищення кваліфікації та 4) внесок у глобальну кібербезпеку.

Останні дані щодо кібербезпеки показують дві суттєві риси. По-перше, високий рівень кібербезпеки простежується у високорозвинених країнах світу, які мають також високі конкурентні позиції. По-друге, існує тісна кореляція між рівнями національної кібербезпеки та цифрового розвитку, що показано на рис. 2.1.

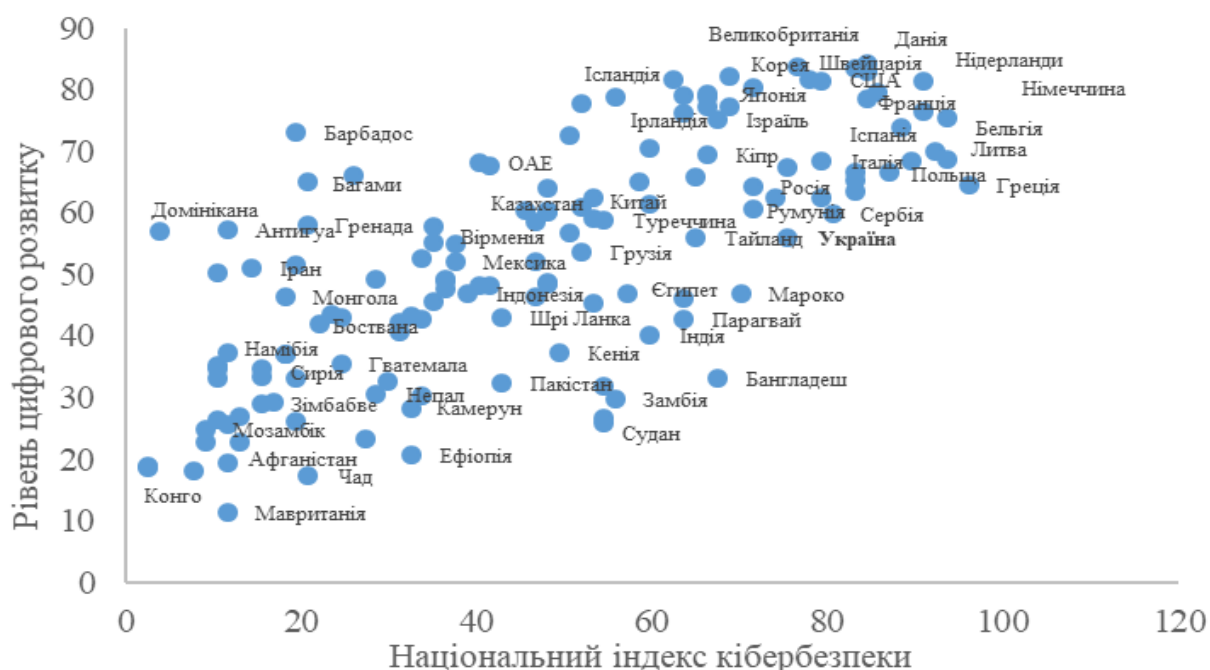


Рис. 2.1. Розподіл країн за рівнем кібербезпеки та цифрового розвитку

Примітка: побудовано за даними Національного індексу кібербезпеки 2021 р. Рівень цифрового розвитку – це середній відсоток від Індексу розвитку ІКТ та Індексу готовності до мережі.

Останні тенденції стану реалізації кібербезпеки 2020 – 2022 демонструють, що фокус зосереджено на запобіганні кіберзлочинності та

захисті персональних даних, eID та довірчих послугах, реагуванні на інциденти, освіті та розробці політики. Формування національних систем кібербезпеки більшою мірою орієнтовано на реакційну політику, а не проактивну, втім існують певні регіональні закономірності. Так, зокрема, зусилля країн Африки зосереджуються на захисті персональних даних, запобіганні кіберзлочинності та освіті, при цьому не вистачає навичок кризового управління та захисту основних і цифрових послуг. Натомість, кіберполітика країн Океанії зосереджена на реагуванні на кіберінциденти, аналізі кіберзагроз та боротьбі з кіберзлочинністю, але меншою мірою орієнтується на захист послуг та управлінні кіберкризовими ситуаціями. В країнах Азії тенденції кібербезпеки найбільше зосереджуються на боротьбі з кіберзлочинністю, реагуванні на кіберінциденти та освіті, водночас є проблеми із захистом цифрових і основних послуг та персональних даних. В країнах Америки влада зосереджується на боротьбі з кіберзлочинністю, реагуванні на інциденти, захисті персональних даних, електронному ідентифікаторі (eID), а також на довірчих послугах та освіті. Натомість, країни Європи представляють збалансовані зусилля з точки зору аналізу кіберзагроз, управління кіберкризами, кібервійськових операцій та глобальних зусиль і співпраці.

У ландшафті кібербезпеки, що швидко розвивається, постійно з'являються нові загрози. Технічні рішення є лише частиною багатопланової кібербезпеки урядів. Провідна роль на національному рівні сьогодні належить розробці державної політики у сфері кібербезпеки, оцінці кіберзагроз, освіті та підвищення кваліфікації, а також участі у забезпеченні глобальної кібербезпеки.

Війна, яка відбувається на фоні збройної агресії Росії проти України, вимагає від нашої країни створення потужного механізму протистояння. Війна в Україні розпочалась локально ще з лютого 2014 року на територіях Криму, Донецької та Луганської областей України та набула повномасштабного характеру з 24 лютого 2022 року. За цей період

пропаганда російських медіа набула масштабного поширення не лише на території Росії та України, але і в усьому світі. На сьогодні світова спільнота опинилась в умовах інформаційної російської окупації, тому разом з Україною її завданням є протистояння пропагандиським діям агресора, які спотворюють суспільну думку та становлять інформаційну загрозу засадам глобальної безпеки, миру та демократії. Україна наразі пропонує світу новий механізм інформаційного спротиву – «Інформаційний Рамштан» [26], який стане новим об'єднанням всіх країн цивілізованого світу з метою зміни стратегічних підходів та спільній протидії дезінформації Росії. Водночас, завданням нашої держави є не лише узгодження об'єднаних дій та створення міжнародної коаліції інформаційного протистояння російській пропаганді, але і використання з цією метою ефективних сучасних управлінських інструментів для координованого прийняття антикризових рішень.

Сучасним інструментом, що використовується органами влади як на міжнародному рівні, так і на рівні окремих країн світу для організації оперативного реагування на кризові виклики національній безпеці, зокрема й інформаційній, є ситуаційні центри (наприклад в Україні це «CERT-UA» – підрозділ у складі Держспецзв'язку, створений для реагування на комп'ютерні надзвичайні події), що функціонують на засадах мережевого управління. Їх діяльність спрямована на ефективне прийняття рішень у сфері управління динамічними ситуаціями на основі виявлення та всебічного аналізу інформації щодо їх змін, а також прогнозування їх подальшого розвитку.

Як зазначає М. Ендслі, ситуаційні центри усвідомлюють ситуацію через сприйняття елементів навколишнього середовища у просторі та часі, розуміння їхнього значення та прогнозування їх стану в найближчому майбутньому [151].

ЄС є стратегічним партнером України у вирішенні проблеми російсько-української війни, який надає потужну підтримку не лише через фінансування, але і через участь у спільній організації та реалізації різних

суспільно-політичних проєктів протидії російській агресії та ліквідації її наслідків. Тому пріоритетним для України стане також залучення інституцій ЄС до створення спільного моніторингового ситуаційного центру, який би забезпечував ефективне оперативне вирішення питань безпеки та оцінював ризики стратегічного управління. Під час проєктування такого ситуаційного центру варто враховувати досвід вже існуючих мереж ситуаційного управління.

В ЄС наразі сформувалася диверсифікована система платформ, проєктів та мереж ситуаційного управління з доволі різнобічним функціоналом. Так, наприклад, Гаазьким центром стратегічних досліджень (The Hague Centre for Strategic Studies) розроблена спеціалізована база даних і знань StratBase Datalab, яка використовується для здійснення геостратегічного аналізу та дослідження країн, які знаходяться в зоні ризику на основі відкритих даних [188, с. 9-10]. При цьому, що особливо важливо для України, в центрі уваги перебувають внутрішньодержавні конфлікти та громадянські війни. В проєкті Datalab застосовується система прогнозних економетричних моделей, останні з яких використовують системи штучного інтелекту для створення прогнозів конфліктів на субнаціональному рівні з часовим горизонтом від 1 до 24 місяців. Моделі нового покоління Datalab визначають причинно-наслідкові зв'язки під час виникнення конфліктів та спрямовані на роз'яснення різних конфліктних патологій і ефектів взаємодії між різними чинниками виникнення конфліктів.

База даних StratBase та моделі DataLab застосовуються у політиці ЄС щодо запобігання конфліктам та забезпечення миру у різні способи, серед яких:

- застосування прогнозних моделей для здійснення ситуаційного аналізу;
- виявлення характеристик конфлікту на основі побудови причинно-наслідкових моделей мережевого управління;

– розробка сценарних моделей застосування окремих політичних інструментів для врегулювання конфліктних ситуацій тощо.

Таким чином, ЄС має практично корисний для України досвід мережевого управління, впровадження якого під час розбудови нової моделі колективного інформаційного спротиву, який пропонує Україна, може забезпечити її довгострокову спроможність за рахунок аналітичного обґрунтування управлінських рішень.

Визначення та узгодження Україною заходів інформаційної безпеки та колективної протидії вірусній російській пропаганді на засадах мережевого управління може передбачати адаптацію існуючих моделей ситуаційного аналізу та подальшу розробку нових моделей з урахуванням нових міжкраїнових домовленостей та викликів. Застосування динамічного моделювання ситуацій із використанням вихідних даних та подальшим аналізом ситуацій щодо пропаганди є необхідним для визначення можливих наслідків прийнятих рішень щодо контрпропаганди та їх впливу на суспільну думку. Варто імплементувати також адаптивні системи, які використовуються для опису факторів та передумов виникнення можливих ситуацій за допомогою імітаційного (динамічного) моделювання. Їх завданням має бути визначення вихідних даних, що відображають умови і фактори виникнення інформаційної окупації задля розробки заходів щодо запобігання їх появі у майбутньому.

2.2 Зарубіжний досвід функціонування мережі ситуаційних центрів органів влади (на прикладі країн ЄС та США)

Виникнення загроз національній безпеці України, які були спричинені збройною агресією РФ сформували кризові виклики, які потребують не лише ефективного оперативного реагування, але і постійного відстеження ситуації, прогнозування можливого розвитку подій, обміну інформацією та взаємодію для прийняття рішень. У світовій практиці з цією метою напрацьовано досвід

створення та функціонування мережі спеціальних ситуаційних центрів оперативного реагування, які оснащують високотехнологічним обладнанням та забезпечуються кваліфікованим персоналом для аналізу ситуацій у критично важливих сферах, де можуть виникати загрози національній безпеці, спричинені різними чинниками. Тому вивчення дієвих та ефективних практик прийняття рішень в мережі ситуаційних центрів є передумовою успішної розбудови в Україні мереж антикризового реагування для органів державної влади.

Дослідженню принципів, механізмів та секторальних особливостей розвитку мережі ситуаційних центрів присвячені численні праці таких іноземних дослідників як М. Амановіч [136], С. Ван Бален [206], В. Драгос [150], Р. Лежчина [208], В. Овенс, Н. Павлов [189], П. Пілоцці, Дж. Пітерс, Т. Уолліс [208] та ін. У своїх публікаціях автори розкривають особливості функціонування ситуаційних центрів, симуляційних систем, платформ, командно-контрольних систем, віртуальних середовищ, баз даних у різних секторах управління об'єктами, таких як прикордонний контроль, морський нагляд, енергетична безпека, кібербезпека, семантичний аналіз, а також міжнародне співробітництво у сфері моніторингу ситуацій та обміну даними. Серед вітчизняних дослідників проблематика розвитку мережі ситуаційних центрів відображена у працях В. Вишневського [7], В. Горбик [15], Г. Кузьменка [44], А. Морозова [44], В. Пристайка [59], В. Тютюника [115], О. Яценка та інших. Авторами, зокрема, висвітлено еволюцію процесів автоматизації мережевого управління об'єктами в Україні, сутнісні характеристики, організаційні аспекти формування та особливості функціонування ситуаційних центрів на різних стадіях розвитку надзвичайних ситуацій, принцип мережево-центричності у функціонуванні ситуаційних центрів, а також особливості обґрунтування експертами антикризових рішень щодо функціонування органів державної влади.

Ситуаційні центри є ефективним інструментом прийняття рішень у сфері мережевого управління ситуаціями, які динамічно розвиваються, що

дозволяє виявляти на основі послідовного та всебічного аналізу базові тенденції, що визначають динаміку ситуації, а також прогнозувати її подальший розвиток [199]. Діяльність мережі ситуаційних центрів у зарубіжній практиці доволі часто пов'язують з функцією «усвідомлення ситуації» (англ. «situational awareness»), яку визначають як сприйняття елементів навколишнього середовища у відповідному просторі та часі, розуміння їхнього значення та прогнозування їх стану в найближчому майбутньому [152]. На практиці ситуації є спрощеними представленнями складної системи суб'єктів, організацій, подій і дій, що супроводжуються гіпотезами про можливі їх наслідки. Основним завданням ситуаційних центрів є моделювання ситуацій, які виникають у відповідній предметній області прийняття державно-управлінських рішень.

Як свідчить аналіз світової практики, мережі ситуаційного моделювання можна розділити на три основні види [199]:

- спеціалізовані та адаптивні мережеві системи моделювання динамічних ситуацій;
- моніторингові ситуаційні мережеві системи (центри ситуаційного відображення; розподілені системи відображення ситуаційної інформації);
- аналітичні ситуаційні мережеві системи (системи ситуаційного управління; аналітичні ситуаційні центри; експертні системи реального часу).

Спеціалізовані мережеві системи динамічного моделювання ситуацій використовуються для вирішення безпосередніх завдань, суть яких впливає з вихідних даних з подальшим аналізом ситуацій, що виникають у системах відображення ситуаційної інформації та аналітичних ситуаційних системах. Водночас, адаптивні мережеві системи застосовуються для вирішення діаметрально протилежних управлінських завдань, а саме – для опису факторів та передумов виникнення можливих ситуацій за допомогою імітаційного (динамічного) моделювання. Їх завданням є визначення вихідних даних, що відображають умови і фактори виникнення певних ситуацій.

Застосування аналітичних ситуаційних мережевих систем здійснюється з врахуванням того, що кількість можливих станів цільової системи є значною, водночас, кількість можливих рішень є обмеженою. Таким чином, поєднання системного підходу, який дає повне уявлення про об'єкт мережевого управління та його функціонування в зовнішньому середовищі, із ситуаційним дозволяє ефективно керувати розвитком конкретної управлінської ситуації. При цьому, ефективні управлінські рішення приймаються з врахуванням вихідних умов та характеристик конкретної ситуації. Окрім того, важливо розрізняти зовнішні ситуаційні центри, чії функції пов'язані з оцінкою ситуацій взаємодії певної організації із зовнішнім середовищем, та внутрішні центри, що застосовуються для моделювання, аналізу, оцінки взаємодії та мережевого управління внутрішніми структурними підрозділами організації.

Ситуаційні центри використовуються при виробленні стратегічних державно-управлінських рішень на основі аналізу масиву вхідної інформації про ситуацію. Окрім того, вони сприяють формуванню коректного розуміння ситуації з урахуванням динаміки її розвитку, а також є інструментом системного пошуку релевантних управлінських рішень. Ситуаційні центри дають можливість відстежувати хід ситуації, її зміни, а також прогнозувати її ймовірні майбутні стани. Добре організована робота ситуаційного центру дозволяє економити час і ресурси, приймати обґрунтовані рішення, одночасно уникаючи численних управлінських помилок, що є наслідком застосування в практиці менеджменту принципу перевірки рішень з досвіду власних спроб і помилок.

Структура мережі ситуаційних центрів може відрізнятися залежно від їх цільового призначення та предметного поля діяльності. Відтак, структура є одним із найвагоміших критеріїв класифікації мережі ситуаційних центрів. Так, у загальному розумінні ситуаційним центром (пунктом або кімнатою) можна назвати приміщення, призначене для проведення спостереження або аналізу поточної ситуації. Проте така дефініція є надто широкою, оскільки

під її кваліфікацію підпадатиме будь-яке приміщення, оснащене телебаченням, радіо, телефонним зв'язком, комп'ютерною технікою та географічними картами. В такому випадку йдеться про персональний ситуаційний центр. При цьому, структура мережі професійних ситуаційних центрів, як правило, є складнішою та охоплює оперативний штаб, ситуаційний зал управління (нагляду), обладнаний потужним обчислювальним середовищем, а також інформаційні моделі складних динамічних ситуацій. Відмінною рисою будь-якого сучасного ситуаційного центру є наявність в ньому геоінформаційної системи.

Обов'язковими компонентами функціональної структури ситуаційного центру є три базові модулі, які відповідають за динамічне (імітаційне) моделювання поведінки зовнішнього, внутрішнього середовища та за оцінку їх взаємодії.

Структура ситуаційного центру, як інформаційної мережі, окрім функціональної складової включає ще й різні види ресурсного забезпечення – інформаційно-аналітичного, технічного, організаційного, кадрового, лінгвістичного тощо. Інформаційна інфраструктура (мережа) таких центрів складається з програмного забезпечення та інформаційних потоків, що у сукупності забезпечують роботу базових модулів і візуалізацію ситуаційного центру. Сюди можна віднести усі вищезгадані типи систем ситуаційного моделювання.

Типовим прикладом з категорії зовнішніх мережевих ситуаційних центрів є SITCEN НАТО, до функціональних обов'язків якого належить інформування Північноатлантичної ради та Військового комітету НАТО про ситуацію в світі як у мирний час, так і в часи криз та військових конфліктів. Ця мережа ситуаційних центрів використовуються для проведення міжнародних військових навчань північноатлантичного альянсу. SITCEN обробляє та поширює найактуальнішу інформацію, отриману як з внутрішніх, так і з зовнішніх ресурсів як відкритого, так і таємного характеру. SITCEN виконує функції мережевого зв'язку з подібними

установами в країнах північноатлантичного альянсу та міжнародними організаціями.

Зміст діяльності SITCEN полягає в обробці інформації з метою забезпечення ситуаційної обізнаності північноатлантичного альянсу, що дозволяє Північноатлантичній раді (North Atlantic Council, скорочено – NAC) та Військовому комітету (Military Committee, скорочено – MC) приймати обґрунтовані рішення. NAC є вищим органом НАТО, який приймає політичні рішення, водночас, MC є вищим військовим органом НАТО, який надає консультативну підтримку діяльності NAC та Групи ядерного планування НАТО. Розміщений у штаб-квартирі НАТО в Брюсселі (Бельгія) хаб SITCEN посідає унікальне місце в організаційно-мережевій структурі НАТО для взаємодії між цивільними та військовими підрозділами персоналу (рис. 2.2).

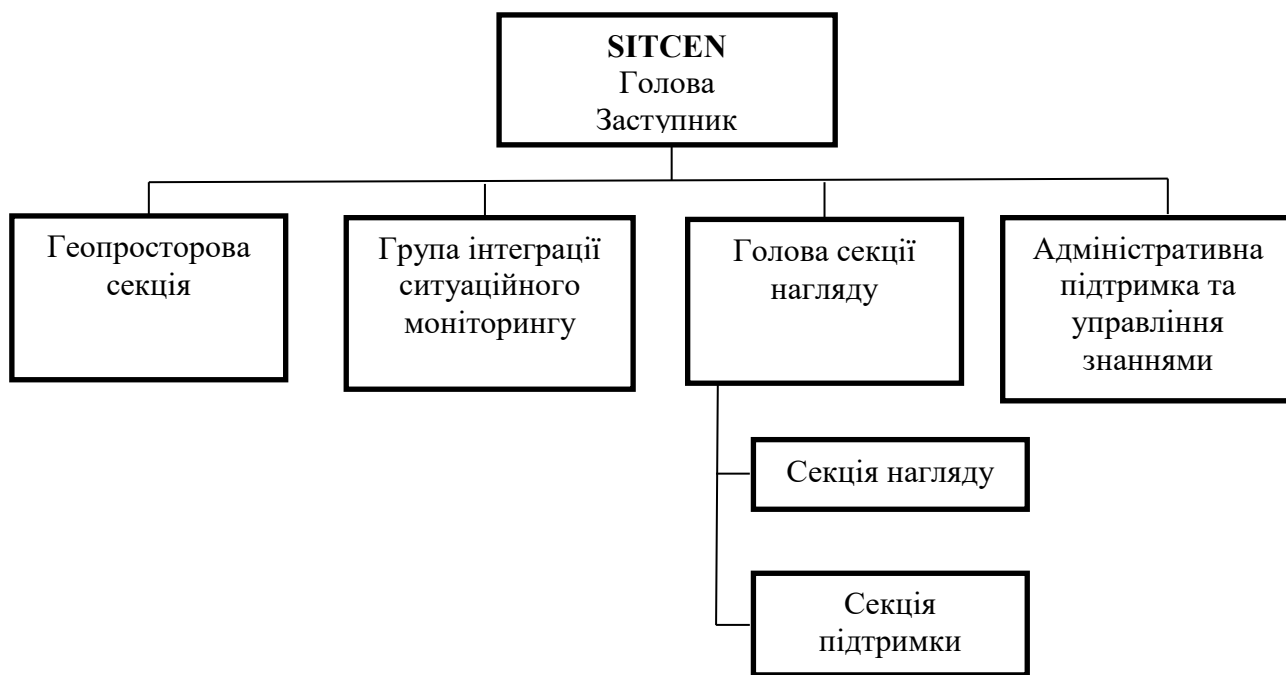


Рис. 2.2. Структура ситуаційного центру НАТО SITCEN

Джерело: складено автором за: [200].

Секція нагляду (SITCEN Watch) надає штаб-квартирі НАТО цілодобову ситуаційну інформацію щодо політичних, економічних, військових та терористичних подій у всьому світі. Персонал секції працює цілодобово 24/7

вахтовим методом, змінюючи вахту кожні 12 годин. Перелік функціональних обов'язків секції нагляду включає: надання оперативної інформації про події з використанням автоматизованої системи виклику; інформаційне забезпечення підготовки нарад та особистих брифінгів керівництва міжнародного військового штабу НАТО; моніторинг систем раннього попередження протиповітряної оборони від балістичних ракет; співпраця з Відділом громадської дипломатії НАТО з метою безперервного моніторингу інформації у пресі; підтримка діяльності організацій з врегулювання криз; сприяння Управлінню безпеки НАТО у здійсненні моніторингу за виконанням міжнародних місій персоналу НАТО, що знаходиться за кордоном.

Геопросторова секція SITCEN надає комплексні географічні послуги штаб-квартирі НАТО як у сфері наземного геопросторового спостереження, такі у сфері морського, повітряного та космічного спостереження.

Функціональні завдання секції є доволі широкими – від оперативного відображення місцевості до відтворення загальної оперативної ситуації для керівних органів НАТО. Окрім того, секція забезпечує мережеве управління геопорталами на різних мережевих доменах, а також займається створенням навчальних географічних сценаріїв для військових навчань. При цьому, у кризових умовах геопросторова секція розробляє геопросторові програми та стратегічні інформаційні панелі з геопросторовим контентом з метою забезпечення цілодобового ситуаційного аналізу, а також процесу прийняття управлінських рішень.

Група інтеграції ситуаційного моніторингу (Situational Awareness Integration Team – SAIT), створена в березні 2020 року, є відносно новим підрозділом SITCEN. Вона виконує роль системного інтегратора ситуаційного центру, розробляючи системне бачення глобального та регіонального середовища безпеки та його впливу на союзників і партнерів НАТО. Одним із головних завдань підрозділу є підготовка, координація та проведення нарад керівного персоналу штаб-квартири НАТО. SAIT також

проводить якісні та кількісні дослідження ситуацій, а також виконує роль посередника між усіма зацікавленими сторонами в межах НАТО.

У структурі SITCEN також є офіс адміністративної підтримки та управління знаннями (Administrative Support and Knowledge Management – АКМ), який є центральним пунктом інформаційного контролю та управління, а також професійного навчання та фінансового управління.

Доволі показовим прикладом сучасного етапу еволюції ситуаційних центрів є американський проект SANER (Situational Awareness for Novel Epidemic Response), що є національною мережею медичних ситуаційних центрів, яка має на меті революціонізувати застарілі процеси обміну даними у сфері охорони здоров'я, покращити рівень оперативної обізнаності про пандемічну ситуацію з COVID-19 у режимі реального часу, а також прогнозувати всі майбутні надзвичайні ситуації у сфері охорони здоров'я [169]. До мережі SANER залучено партнерів з державного та приватного секторів з метою автоматизації звітності щодо працездатності лікарень, моніторингу поточної ситуації у сфері охорони здоров'я під час катастроф, надзвичайного стану та інших форс-мажорних обставин.

Головною перевагою проекту SANER є автоматизація процесів звітності з використанням інструментарію прикладного програмування (API) на основі міжнародного стандарту обміну даними HL7® Fast Healthcare Interoperability Resources (FHIR®). Заклади охорони здоров'я, критичної інфраструктури та державні органи можуть використовувати ці стандарти для розкриття даних, які є критичними для контролю поширення хвороб та мережевого управління ресурсами системи охорони здоров'я у межах всієї країни. Завдяки такому стандарту обміну даними основні елементи інформації можна автоматично отримувати з цілого ряду джерел (баз даних) лікарень, серед яких: електронні медичні карти пацієнтів, система управління ліжко-місцями, система управління активами, інвентаризаційна звітність тощо. При цьому, елементи даних, що підлягають обміну в межах мережі, включають таку критично важливу інформацію, як кількість і статус

конкретних типів лікарняних ліжок, забезпеченість персоналом, кількість апаратів штучної вентиляції легень та іншого критично необхідного медичного обладнання. Цими даними у мережі можна поділитися з іншими лікарнями, місцевими, державними та федеральними органами охорони здоров'я та компетентними організаціями.

В Європейському Союзі наразі сформувалася диверсифікована система платформ мереж свого управління з доволі різнобічним функціоналом. Так, наприклад, Datalab – це спеціалізована база даних і знань, розроблена Гаазьким центром стратегічних досліджень (The Hague Centre for Strategic Studies), яка використовується для здійснення геостратегічного аналізу та дослідження країн, які знаходяться в зоні ризику на основі відкритих даних [189, с. 9-10]. При цьому, в центрі уваги проекту перебувають внутрішньодержавні конфлікти та громадянські війни.

У проекті Datalab застосовується система прогнозних економетричних моделей, що базуються на аналізі 50 факторів уразливості, пов'язаних з політичною нестабільністю. Моделі останнього покоління використовують системи штучного інтелекту для створення прогнозів конфліктів на субнаціональному (районному) рівні з часовим горизонтом від 1 до 24 місяців. Моделі нового покоління Datalab визначають причинно-наслідкові зв'язки під час виникнення конфліктів та спрямовані на роз'яснення різних конфліктних патологій і ефектів взаємодії між різними чинниками виникнення конфліктів.

Мережа HCSS StratBase Datalab передбачає аналіз більше 11 тисяч змінних із різних відкритих та приватних баз даних, більшість з яких мають кількісну природу (наприклад, економічні, фінансові, військові та інші дані), проте все частіше застосовується аналіз текстів, зображень, аудіо та відео. Набори даних обробляються за допомогою аналітичних алгоритмів, що дають змогу здійснювати картування досліджуваних ситуацій, а також відстеження глобальної геодинаміки, життєвих циклів конфліктів,

політичних ризиків та ризиків безпеки як в автономному режимі, так і в кіберпросторі.

Загалом, мережева база даних StratBase та моделі DataLab можуть застосовуватися у політиці щодо запобігання конфліктам та забезпечення миру різними способами, а саме: застосування портфелю прогнозних моделей для ситуаційного аналізу; виявлення конфліктних патологій на основі причинно-наслідкових конфліктних моделей; сценарні моделі застосування політичних інструментів для врегулювання конфліктних ситуацій тощо.

Ще більш комплексний підхід в сфері ситуаційного менеджменту, розроблений компанією «4C Strategies», застосовується у Швеції [189, с. 11- 12]. Exonaut – це мережева платформа керування ситуаціями, що базується на інтегрованих підходах до управління економічними ризиками та антикризового управління. Пакет програмного забезпечення дозволяє моделювати, оцінювати та відстежувати рівень організаційної готовності до кризових ситуацій. Наразі, платформа Exonaut фактично стала глобальним стандартом програмного забезпечення для проведення військових навчань та спеціалізованої фахової підготовки. Дана платформа дає змогу користувачам оцінювати, візуалізувати та використовувати навчальні дані для прийняття ефективних антикризових рішень. Зокрема, програмний додаток Exonaut Command and Control є комплексною системою мережевого управління надзвичайними ситуаціями, що охоплює весь спектр функцій – від диспетчерської до передової. Система дозволяє спостерігати за перебігом інцидентів на основі карти та інформаційних панелей, що дають змогу відстежувати стан та переміщення активів, створювати журнали інцидентів тощо. Система постійно удосконалюється з врахуванням вимог військових, поліцейських, пожежних та служб швидкої медичної допомоги.

Додаток Consular Online 2.0 забезпечує можливість спільного оперативного реагування на кризові ситуації та пройшов апробацію Європейською службою зовнішніх дій (EEAS) для реагування на консульські

кризи. Мобільна онлайн система Exonaut Incident and Crisis Manager включає дошки оголошень і сповіщень у режимі реального часу, інтерактивні карти посольств, лікарень, пунктів збору тощо, а також автоматизовані звіти про інциденти та спеціальні панелі інструментів. Критерії, набори запитань і цілі можуть бути зіставлені в системі з різними видами діяльності, які найбільше підходять для аналізу відповідних гіпотез або завдань. Окрім того, отримані об'єктивні та суб'єктивні дані можуть бути записані в систему майже в режимі реального часу та застосовуватися для інформування про подальший перебіг подій або для отримання визначених користувачем результатів.

Компанія MASA Group (Франція) розробила «MASA Synergy», що є мережевою системою підтримки прийняття рішень державними або приватними організаціями в умовах надзвичайних ситуацій, криз і катастроф. MASA Synergy дозволяє моделювати міжвідомчі кризові сценарії забезпечення громадської безпеки та операцій цивільного захисту на місцевому, регіональному та державному рівнях [131]. Перелік моделей «Synergy», зокрема, включає стихійні лиха (землетруси, повені, урагани, зсуви, посухи тощо), техногенні катастрофи (витоки хімікатів, забруднення, пожежі тощо), напади злочинців / терористів, операції з боротьби з натовпом, захист стратегічної інфраструктури, охорону велелюдних заходів тощо. Загалом MASA Synergy застосовується для підготовки персоналу кризових підрозділів, а також осіб, які приймають рішення. Система дозволяє оптимізувати процеси планування ресурсів, перевіряти ефективність планів на випадок надзвичайних ситуацій, а також оцінювати характер впливу катастроф на населення, майно та інфраструктуру.

Проект Effector (повна назва *англ.* «An End to end Interoperability Framework For MaritimE Situational Awareness at StrategiC and TacTical Operations») отримав фінансування у розмірі 5 млн євро на 18 місяців у жовтні 2020 року від програми ЄС з досліджень та інновацій «Горизонт 2020» за грантовою угодою № 883374 за тематичним пріоритетом «Демонстрація прикладних рішень для посилення прикордонної та

зовнішньої безпеки» (SU-BES03-2018-2019-2020), підтема 2 «Нові концепції підтримки прийняття рішень та інформаційних систем». Реалізація проекту здійснювалася консорціумом із 16 партнерів, що включав великі (NAVAL, THALES, ENG, CLS) та малі компанії (SATWAYS), дослідні організації (KEMEA, ICCS, INOV, IRIT), кінцеві користувачі, якими є державні органи країн-учасниць (Secreteriat General de la Mer; Hellenic Ministry of Maritime Affairs & Insular policy; Hellenic Police; Portuguese Navy; Bulgarian Executive Agency for Maritime Administration; Hellenic Ministry of Defense; Administration for Maritime Safety and Port Management of Montenegro).

Головною метою проекту EFFECTOR є розробка міжнародної системи морського спостереження та безпеки кордонів, що забезпечує моніторинг подій у морі, об'єднання та аналіз даних, а також підтримку прийняття рішень. Крім того, EFFECTOR забезпечує комунікацію та обмін інформацією між керівними органами країн-учасниць проекту на місці подій. Важливим технічним завданням в межах проекту є розробка структури сумісності національних систем моніторингу морської зони, а також надання пов'язаних з нею аналітичних послуг морського спостереження та безпеки кордонів. Складна система проекту включає цілу низку елементів, а саме: багаторівнева мережа даних і спільне середовище обміну інформацією для місцевих, регіональних і національних координаційних центрів; підсистема об'єднання і аналізу даних для надання послуг ситуаційної обізнаності; підсистема гармонізації даних для повної інтеграції систем морського та прикордонного спостереження, датчиків, платформ і джерел даних; підсистема звітності; підсистема морської семантики; підсистема інтеграції з європейськими мережами CISE та EUROSUR для транснаціонального обміну інформацією; безпекова підсистема.

Серед основних завдань проекту варто визначити:

- впровадження багаторівневої платформи «озера даних» для наскрізної взаємодії та використання даних, що сприятиме інтеграції

національних систем морського спостереження та взаємодії інформаційних систем на тактичному та стратегічному рівнях;

- здійснення обміну даними про ситуацію на місцевому, регіональному та національному рівнях з наднаціональним Спільним середовищем обміну інформацією в ЄС (CISE) та з Європейською системою нагляду за кордонами (EUROSUR);

- упровадження системи гармонізації даних та розроблення стандартів сумісності даних в середовищі морського спостереження;

- розроблення нових інструментів отримання знань, об'єднання даних, їх семантичного представлення та аналізу;

- перевірка прикладних рішень національними морськими органами, кінцевими користувачами та практиками;

- забезпечення повної відповідності діючій нормативно-правовій базі щодо захисту персональних даних та конфіденційності.

Багаторівнева мережа даних і спільне середовище обміну даними для місцевих, регіональних і національних координаційних центрів в межах проекту EFFECTOR було розгорнуто національних координаційних центрах трьох морських країн ЄС – Франції, Португалії та Греції. Вона підтримує національні та місцеві системи спостереження і складається з кількох взаємопов'язаних технологій з відкритим вихідним кодом великих даних, що забезпечує можливості отримання, перетворення та завантаження даних (Extract, Transform and Load – ETL) з метою:

- отримання, очищення та агрегування неоднорідних даних, зберігання необроблених даних та метаданих;

- забезпечення підтримки більшості існуючих стандартів обміну інформацією у таких сферах, як керування інцидентами, відстеження цілей, планування місій, розвідувальні рейди тощо;

- використання великих даних за допомогою останніх досягнень ІТ платформ в сфері агрегації великих даних, їх обробки, зберігання та розповсюдження;

– підвищення ефективності прийняття рішень шляхом ідентифікації контекстної інформації, багаторівневого злиття даних та їх семантичної аналітичної обробки.

Центри обміну та аналізу інформації (*англ.* Information Sharing and Analysis Centres, аббревіатура – ISAC) є об'єднаннями представників зацікавлених сторін з метою здійснення обміну інформацією про загрози та інциденти кібербезпеки в окремих галузях діяльності. За визначенням Агенції ЄС з інформаційної та мережевої безпеки (ENISA), центри обміну та аналізу інформації – це керована членами (які представляють як приватний, так і державний сектори) організація або група (формальна або неформальна), яка створена з метою підтримки захисту кібернетичної та фізичної безпеки її членів [159, с. 8]. Такі центри є некомерційними організаціями, які переважно забезпечують збір інформації про кіберзагрози для об'єктів критичної інфраструктури, а також двосторонній обмін інформацією між представниками приватного та державного секторів про основні інциденти, загрози та їх причини. Вони можуть бути орієнтовані як на окремий пріоритетний сектор (фінанси, енергетика, охорона здоров'я), так і на національному рівні слугувати центром збору та аналізу інформації про кібезагрози.

Центри обміну та аналізу інформації вперше були створені у США в 1997 році. Президент США Б. Клінтон створив Президентську комісію із захисту критичної інфраструктури після терористичних атак на Всесвітній торговий центр у 1993 році та Оклахома-Сіті у 1995 році. Основним завданням комісії стало дослідження можливостей співпраці між державним і приватним секторами у сфері забезпечення безпеки критичної інфраструктури країни. Під головуванням Р. Марша комісія представила доповідь з цілим рядом рекомендацій щодо підвищення рівня безпеки критичної інфраструктури США, найважливішою з яких стало створення центрів обміну та аналізу інформації з метою, в першу чергу, посилення співпраці між державною адміністрацією та промисловістю.

Наразі 25 галузевих центрів США об'єднані у Національну раду центрів обміну та аналізу інформації (National Council of ISACs – NCI), до функцій якої належить збір та аналіз даних стосовно кібернетичних та фізичних загроз, обмін інформацією з компаніями-членами, які представляють різні сектори американської економіки, а також розробка інструментів зниження ризиків і підвищення стійкості до загроз [132]. Оскільки сектори критичної інфраструктури доволі тісно взаємопов'язані, Національна рада відіграє критично важливу роль у міжгалузевій координації діяльності цих центрів, особливо під час стихійних лих та інших інцидентів, що становлять загрозу для фізичної чи кібернетичної безпеки. NCI також є форумом для обміну інформацією про загрози, а також служить інформаційним шлюзом для секторальних центрів, федеральних агентств та інших партнерів.

Мережа галузевих центрів обміну та аналізу інформації охоплює як в окремі сектори економіки США, так і критично важливу сферу суспільної діяльності, а саме: видобуток нафти та природного газу (Oil & Gas ISAC; Downstream Natural Gas ISAC), електроенергетику (Electricity ISAC), хімічну промисловість (American Chemistry Council), автомобілебудування (Automotive ISAC), авіакосмічну промисловість (Aviation ISAC; Space ISAC), транспорт (Surface Transportation, Public Transportation and OverThe-Road Bus ISACs), мореплавство та портову інфраструктуру (Maritime ISAC; Maritime Transportation System ISAC; Water ISAC), комунікації (Communications ISAC), інформаційні технології (Information Technology ISAC; Small Broadband ISAC), мас-медіа (Media & Entertainment ISAC), фінансові послуги (Financial Services ISAC), операції з нерухомістю (Real Estate ISAC), торгівлю та готельне господарство (Retail & Hospitality ISAC), охорона здоров'я (Health ISAC; Healthcare Ready), освіту та науку (Research & Education Network ISAC), регіональний розвиток (Multi-State ISAC), національну оборону (National Defense ISAC), управління надзвичайними ситуаціями

(Emergency Management & Response ISAC), інфраструктуру проведення виборів (Elections Infrastructure ISAC).

Більш ніж двадцятирічний досвід функціонування мережі центрів засвідчив їх високу ефективність у сфері забезпечення кібербезпеки, адже завдяки їх функціонуванню у США сформувалася стійка екосистема, що характеризується високим рівнем поінформованості її учасників про основні чинники та характер існуючих і потенційних загроз, інтенсивним обміном досвідом та знаннями, а також високим рівнем взаємної довіри між критично важливими операторами безпеки.

Європейські центри обміну та аналізу інформації мають відмінні від американських центрів функціональні особливості, адже вони, насамперед, зосереджені на розбудові партнерства між своїми учасниками та набагато більше покладаються на державну підтримку в сфері організації їх діяльності (формування секретаріатів) та забезпечення спеціальними знаннями (боротьба з кіберзлочинністю, обмін галузевою інформацією тощо). Участь державних органів в організації діяльності центрів надає їм більшої формальності та свідчить про увагу державного сектору до безпекових потреб відповідних галузей.

Загалом, в Європі сформувалося три моделі мереж центрів обміну та аналізу інформації – національна модель, секторальна модель та міжнародна колабораційна модель.

Діяльність мережі центрів, що належать до національної моделі, зорієнтована на територію всієї країни. Ідея такої моделі полягає в об'єднанні різних експертів та груп реагування на інциденти з комп'ютерною безпекою (CSIRTs) в межах єдиної національної ініціативи, що дозволяє підвищити ефективність аналізу та обміну інформацією про безпекові загрози. При цьому, взаємодія між експертами є доволі неформальною та переважно визначається самою спільнотою експертів та учасників центрів. Так, наприклад, метою Форуму обміну інформацією в Литві є об'єднання експертів з кібербезпеки задля обміну знаннями, досвідом та інформацією

про загрози. Він є волонтерською спільнотою експертів з індивідуальним членством, незалежно від організацій, які вони представляють. Тобто, якщо людина змінює роботу, то вона залишається членом форуму. Аналогічною є національна ініціатива CERT.LU, створена в Люксембурзі для обміну досвідом та знаннями між групами реагування на інциденти з комп'ютерною безпекою, яка підтримується Міністерством економіки.

Ще одним прикладом національної мережі обміну та аналізу інформації в Європі може слугувати заснована в 2008 році у Португалії Національна мережа груп реагування на інциденти з комп'ютерною безпекою (National network of CSIRTs). Дана ініціатива була започаткована 31 комп'ютерними групами реагування на надзвичайні ситуації (CERT) у співпраці з представниками груп реагування на інциденти з комп'ютерною безпекою (CSIRT) як державного, так і приватного секторів (енергетичний сектор, фінансовий сектор, телекомунікаційний сектор, академічне середовище та промисловість). Основними завданнями мережі є сприяння розвитку культури безпеки в Португалії, розробка показників стану безпеки та формування національної безпекової статистики, удосконалення проактивних і реактивних заходів протидії загрозам, створення необхідних превентивних інструментів, розробка сценаріїв координації дій в умовах масштабних інцидентів між групами реагування на інциденти з комп'ютерною безпекою та правоохоронними органами.

Секторальна модель мережі центрів обміну та аналізу інформації фокусується на безпеці секторальної критичної інфраструктури та життєво важливих секторів економіки. Метою діяльності таких центрів є обмін інформацією щодо безпеки в певному секторі економіки. Саме тому такі центри перетворюються на галузеві платформи спільних безпекових послуг, що надають цілу низку переваг для своїх учасників. При цьому, в межах секторальної моделі визначено два різних типи взаємодії: центрів обміну та аналізу інформації, які функціонують за підтримки представників відповідного сектору та секторальні центри, розвитку яких сприяє уряд.

Секторальні центри обміну та аналізу інформації, що функціонують за підтримки представників відповідного сектору зазвичай не отримують державного фінансування. Однак співпраця з державним управлінням все одно існує, наприклад, за конкретних обставин, таких як боротьба з кіберзлочинністю та обмін інформацією про безпекові інциденти. Цей тип кібербезпекових центрів притаманний переважно для великих країн, які мають потужний приватний сектор із чітко визначеними цілями у сфері кібербезпеки. Сьогодні оператори економічно розвинених галузей чітко усвідомлюють природу кіберзагроз, а також потребу у співпраці в їх подоланні, що зазвичай проявляється у збільшенні фінансування діяльності секторальних безпекових центрів і платформ.

Доволі показовими прикладами такого типу центрів є «Banking Cybersecurity Center» Польської асоціації банків та об'єднаний центр компетенції з інформаційної безпеки норвезького сектору охорони здоров'я «HealthCERT». Перший з них є платформою комунікації польських банків у випадку виникнення загроз безпеці, а також мережею обміну інформацією про вразливості та загрози банківській діяльності в країні. Наразі членами ВСС є 23 банки, що в сукупності представляють 83 % комерційного банківського сектора Польщі. Об'єднаний центр компетенції з інформаційної безпеки норвезького сектору охорони здоров'я об'єднує близько 400 членів. Центр проводить постійний моніторинг трафіку в ІТ-мережі охорони здоров'я Норвегії та сприяє обміну знаннями про загрози ІКТ та механізми захисту від них. Уряд Норвегії виділив фінансування та обладнання для «HealthCERT», а також визначив типи послуг, які він надає: сенсорна платформа, перевірка загроз несанкціонованого проникнення, оцінка вразливостей та сканування мережі.

Кібербезпекові центри, які функціонують за підтримки держави, зазвичай є спільними ініціативами представників приватного та державного секторів. При цьому, роль держави часто полягає у забезпеченні діалогу між учасниками центрів, а також в наданні фінансування (організація семінарів

тощо). Характерною ознакою цієї моделі є те, що державний сектор застосовує багатогалузевий підхід за яким центри обміну та аналізу інформації створюються у багатьох секторах з метою підвищення рівня кібербезпеки практично в усіх секторах. При цьому, держава прагне стимулювати обмін досвідом між центрами, які представляють різні сектори економіки. У зв'язку з цим, дана модель взаємодії центрів притаманна переважно для невеликих країн, в яких державі легше здійснювати міжсекторну координацію діяльності безпекових центрів. Так, наприклад, у Фінляндії Національний центр кібербезпеки «NCSC-FI» діє як єдина контактна точка та центр компетенції з питань кібербезпеки, який збирає, аналізує та поширює інформацію про загрози безпеці через різні канали, включаючи центри обміну та аналізу інформації. У Бельгії національний центр кібербезпеки займається створенням системи раннього попередження з метою забезпечення секторів критичної інфраструктури швидкими стандартизованими сповіщеннями про нові кіберзагрози та атаки. У Нідерландах національний центр кібербезпеки NCSC відіграє роль посередника та секретаріату для мережі центрів обміну та аналізу інформації.

Міжнародна колабораційна модель мережі організації центрів обміну та аналізу інформації об'єднує багато зацікавлених сторін з усієї Європи та світу. Існує загальне розуміння того, що кібербезпека не обмежена державними кордонами та потребує широкої міжнародної коаліції. Разом з тим, міжнародна співпраця у сфері кібербезпеки на європейському рівні, наразі, сформувалася у трьох пріоритетних секторах – фінансовому, енергетичному та авіаційному. При цьому, рушійною силою у формуванні, розвитку та забезпеченні таких міжнародних центрів є представники приватного сектору. Функцію секретаря зазвичай виконує один із членів, за умови, що інші партнери займаються маркетинговою стратегією, залученням нових членів та ін. Ця спільна відповідальність підтримує активність усіх зацікавлених сторін. Водночас, важливою перешкодою на шляху розвитку міжнародних центрів обміну та аналізу інформації є міжнаціональні

культурні відмінності, внаслідок яких представники різних держав мають різні точки зору та підходи до обміну безпековою інформацією.

Одним з таких центрів є заснований в ЄС у 2015 році Європейський центр обміну та аналізу інформації у сфері енергетики (*англ.* «The European Energy Information Sharing and Analysis Centre», аббревіатура – EE-ISAC). Головними завданнями EE-ISAC є секторальні дослідження вздовж всього ланцюжка створення доданої вартості в енергетиці, розширення складу членів мережі через залучення зацікавлених сторін енергетичного сектора, проактивна та заснована на довірі система обміну інформацією, підвищення організаційної стійкості та готовності членів мережі. З моменту свого створення і до сьогодні EE-ISAC перетворився на міжнародну галузеву мережу взаємної довіри у сфері обміну інформацією, став кібербезпековою платформою, яка об'єднує зацікавлених представників енергетичного сектору у процесі обміну даними про загрози, вразливі елементи, інциденти та можливі рішення у випадку настання порушень безпеки енергетичних систем [153].

В межах мережі EE-ISAC державні органи, комунальні підприємства (постачальники енергії, оператори транспортування та розподільники), охоронні організації, академічні установи, а також спеціалізовані громадські організації обмінюються між собою цінною інформацією про стан кібербезпеки та кіберстійкості в енергетичному секторі країн-учасниць платформи [208].

Обмін інформацією відбувається як під час фізичних зустрічей, так і за допомогою електронних засобів комунікації, включно зі спеціальною системою обміну інформацією. Наразі, система дозволяє обробляти лише вторинну інформацію, тобто таку, яка вже пройшла попередню обробку на національному рівні з відповідних первинних локальних першоджерел. Проте, наразі головним пріоритетом розвитку кіберплатформи є її інтеграція з платформою аналізу загроз, яка дозволить її учасникам отримувати первинну інформацію безпосередньо з місця інциденту, що призведе до

більшої ситуаційної обізнаності в режимі реального часу та значно підвищить ефективність і своєчасність прийняття управлінських та адміністративних рішень для реагування на такі інциденти.

Центр ЄС з обміну та аналізу інформації у фінансовому секторі FI-ISAC, заснований у 2008 році за ініціативою члена правління Агенції ЄС з інформаційної та мережевої безпеки ENISA, є самоокупною організацією з головою та секретарем, яка збирається двічі на рік. До складу центру входять представники фінансового сектору, національних комп'ютерних груп реагування на надзвичайні ситуації, а також правоохоронних органів. Окрім того, до складу учасників центру також входять ENISA, Європол, Європейський центральний банк, Європейська платіжна рада та Європейська Комісія. Місія FI-ISAC полягає в обміні інформацією про електронні та мобільні канали, картки, платіжні системи та інші питання, пов'язані з ІКТ, включаючи кіберзлочинну діяльність, що впливає на фінансове співтовариство, уразливості, технологічні тенденції та загрози. Такий обмін інформацією допомагає фінансовим установам підвищити обізнаність про потенційні ризики та забезпечує раннє попередження про нові загрози в Європі.

Європейський центр авіаційної кібербезпеки ECCSA було створено в 2017 році за ініціативою Європейської Комісії. Засновником центру стала Європейська агенція авіаційної безпеки EASA у співпраці з 12 європейськими партнерами – «Airbus», «Air France/KLM», аеропорт Брюсселя, Управління цивільної авіації Республіки Польща, «ENAV S.p.A.», EUROCONTROL, «Finnair», аеропорт Франкфурта, «Leonardo S.p.A.», «Lufthansa Group», «NAV Portugal» і «Thales Group». Центр є добровільним об'єднанням організацій авіаційного сектора з метою вивчення потенційних ризиків кібербезпеки в авіації, надання колективної підтримки у вирішенні інцидентів кібербезпеки, а також виявлення недоліків і несанкціонованих взаємодій, які потенційно можуть вплинути на стійкість і безпеку сектору. Основна мета ECCSA – створити сприятливе середовище для співпраці між

авіабудівними компаніями та експертами у сфері кібербезпеки задля підвищення їх стійкості до кібератак. ECCSA також сприятиме безпеці авіап перевезень, забезпечуючи високий рівень захисту систем навігації та авіаційної інфраструктури (від проектування до виведення з експлуатації літаків).

Членами ECCSA можуть стати будь-які компанії, організації або установи авіабудівного сектору ЄС, які здійснюють свою основну діяльність в одній із держав-членів Європейської агенції авіаційної безпеки. Крім того, до ECCSA можуть приєднатися організації з інших пов'язаних секторів, які є постачальниками продуктів чи послуг для авіабудівного сектору і можуть сприяти підвищенню загального галузевого рівня кібербезпеки.

2.3 Процесна модель механізмів реалізації мережевого управління у діяльності органів державної влади

Упродовж останніх десятиліть мережі стали основним способом для вирішення складних проблем і досягнень масштабного рівня. Дослідницький інтерес до мережевих структур підкріплюється зміною загальної парадигми в соціальних науках, новими розробками в галузі комунікаційних досліджень, організаційних відносин, а також державного управління.

Мережі завжди були притаманні державно-управлінській взаємодії, однак інституціоналізація мереж, як організаційної форми сучасного державного управління, є відносно новою на порядку денному. Цей процес відбувається на тлі зростання впливу і політичної ваги недержавних, громадських і міжнародних структур при прийнятті і реалізації стратегічних рішень, що вимагає від неї як розвитку нових функціональних напрямів, так і пошуку технологій управління, відмінних від традиційних. Активізація мереж неминуче призводить до значних трансформацій у структурі, функціях держави, методах і технологіях управління, характері професійної підготовки державних службовців тощо.

Мережі, як організаційна структура з об'єднаними учасниками (від місцевих коаліцій до міжнародних альянсів), мають спільні інтереси та працюють разом для досягнення загальної мети, існують в усьому світі для вирішення безлічі складних питань і проблем. Крім того, комунікативні технологічні підходи стають більш витонченими, оскільки грандіозні виклики перед глобалізованим суспільством стають усе більш складними. Незважаючи на зростання міжорганізаційних мереж як організаційної форми, вчені лише нещодавно почали досліджувати, яким чином та з якою ефективністю провідні організації забезпечують координацію різних суб'єктів мережі з різними цілями, обов'язками та можливостями.

Реалізація концепції мережевого управління у діяльності органів державної влади вимагає певних державних механізмів та підходів, які сприяють співпраці, координації та ефективному управлінню. Очевидно, що сучасне глобалізоване суспільство часто стикається із складними суспільними проблемами. Спроби впоратися з цими проблемами можуть призвести до тривалих процесів формування та реалізації державної політики. До прикладу, можна навести декілька сфер із складними процесами управління.

Організація інтегрованих медичних та соціальних послуг для людей похилого віку, що вимагає тісної співпраці між різними організаціями охорони здоров'я, соціального забезпечення, соціальними та житловими організаціями, які можуть бути державними, приватними чи некомерційними, фінансованими, наприклад, урядом або страховими компаніями.

Процеси реалізації державної політики або правозастосування, наприклад, у харчовій промисловості, де влада намагається регулювати складні ланцюги виробництва харчових продуктів, у яких різні сторони в умовах конкуренції можуть нехтувати безпекою харчових продуктів або іншими цінностями.

Експлуатація та підтримка об'єктів громадської інфраструктури

(наприклад, залізниць, доріг, аеропортів, водних проєктів, сміттєспалювальних заводів, електростанцій тощо), в яких влада стикається з великою різноманітністю зацікавлених сторін (приватні фірми, групи громадян, інші громадські суб'єкти, групи екологічних інтересів тощо).

Спроби формувати державну політику та бажаних досягти результатів у боротьбі зі злочинністю та покращенні соціального забезпечення потребують скоординованих зусиль різних державних організацій, таких як поліція, департаменти юстиції, екстрені служби, залучення організацій приватного сектору та громадян, а також співробітництво між органами влади різного рівня та між національними державами.

Процеси, спрямовані на запобігання та управління масштабними аваріями, кризами, стихійними лихами або соціальними заворушеннями та їхніми наслідками (наприклад спалахи пандемій, як COVID-19), вимагають ефективної координації для створення стійких мереж.

Спільним для цих прикладів є те, що вони стосуються складних питань, які потребують глибоких знань щодо їх природи та можливих рішень; однак вони також включають багато акторів, і це може призвести до хаотичного процесу з неочікуваними та небажаними наслідками, або процес може загальмуватись у тривалих та напружених дебатах і конфліктах, які нелегко вирішити.

Розвиток мережевого управління у державному секторі обумовлюється впливом різних факторів. До них відносять:

- політичну волю і підтримку розвитку мережевого управління;
- існування регуляторних законодавчих актів і політик, які визначають правила взаємодії між різними органами та стейкхолдерами;
- ресурси і фінансування: досягнення успіху в мережевому управлінні вимагає адекватного фінансування та інфраструктури;
- розвиток інституційної культури та її вплив на готовність до прийняття мережевого підходу;

- наявність кваліфікованих кадрів, які розуміють принципи мережевого управління та готові до їх впровадження;
- міжнародні та геополітичні чинники, особливо в контексті міжнародної співпраці та обміну досвідом;
- технологічні можливості: розвиток інформаційно-комунікативних технологій та нові інструменти взаємодії;
- готовність до змін та адаптації до нового підходу управління [122].

Як свідчать наукові роботи, емпіричному дослідженню мережевого управління у діяльності органів державної влади приділяється недостатньо уваги, що спричиняє обмежене розуміння. Відтак стає зрозумілим, що при створенні мережі необхідно чітко розуміння процесів та цілей з метою отримання вигід для організацій-учасників. Процес розвитку мережі є складним і вимагає часу для створення необхідних структур, визначення їх повноважень, процедур та механізмів співпраці, необхідних для функціонування механізмів державного управління, забезпечення узгодженості та високої продуктивності роботи [166].

Норвезькі дослідниці Р. Луннан, С. Макгогі (Randi Lunnan, Sara L. McGaughey) акцентують, що успіх великомасштабних проектів залежить від ефективного керівництва міжорганізаційних мереж, які співпрацюють разом для виконання загальної програми, незважаючи на різні цілі, обов'язки та можливості. Мережеве управління, визначене ними як процес аналізу та управління міжорганізаційними мережами, потребує реалізації за трьома етапами:

- по-перше, створення початкових зв'язків, створення легітимності та встановлення когнітивної та емоційної довіри;
- по-друге, управління мережами шляхом створення спільних і гнучких структур і встановлення чітких цілей;
- по-третє, моніторинг прогресу щодо цілей мереж.

Вчені доводять, що питанням побудови легітимності та довіри до

мережі приділено досить велику дослідницьку увагу, однак потребує аналізу проблема кращого розуміння механізмів, які включають початковий вибір форми, засобів, інструментів управління та подальший процес координації діяльності мережевої структури [174].

Відомо, що організаційні мережі не є статичними. Вони розвиваються разом зі змінами в технологіях, особливо в ІКТ, і стрімко розбудовуються у відповідності із світовим технічним та технологічним рухом вперед. Способи, якими ці фактори взаємопов'язані, визначають, яким чином може бути сформована мережа, як нею можна управляти, а також як управління впливає на продуктивність мережі.

Дійсно, у більшості сучасних суспільств державно-управлінські процеси пов'язані не лише з адміністративною ієрархією. Вони стосуються різних рівнів управління і, як правило, створюють всередині і поза ними мережі з багатьма учасниками поза офіційними ієрархіями. Невизначеність, зміни та досвід сприяють постійній еволюції в управлінні цими організаційними мережами [203].

Відтак, для побудови ефективної моделі функціонування механізмів мережевого управління в діяльності органів державної влади, пропонуємо застосувати тристоронній підхід до її реалізації, що містить такі складові:

- фасилітація, як спосіб залучення учасників до процесу для розуміння їхніх цілей, планування засобів досягнення цих цілей і спільної роботи;
- координація, як дія, яка допомагає усім учасникам плану чи діяльності працювати разом організовано, узгоджуючи дії для синхронізації зусиль та досягнення спільної мети;
- адміністрування, як процес забезпечення організації, виконання та нагляду за завданнями або діяльністю, спрямований на просування мережі до її цілей та підтримки її функціонування (рис. 2.3).

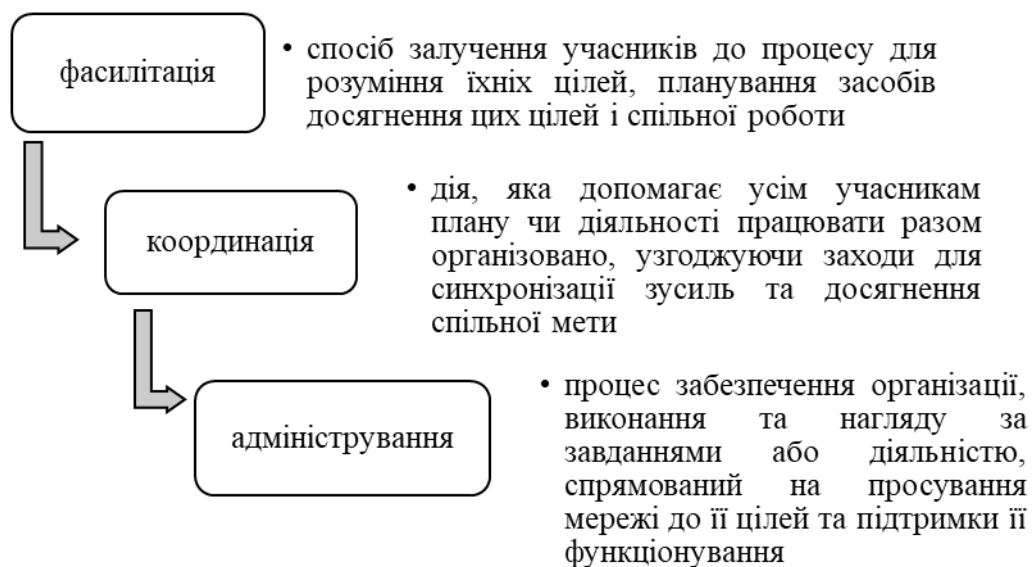


Рис. 2.3. Тресторонній алгоритм практичних заходів з впровадження механізмів реалізації мережевого управління у діяльності органів державної влади

Джерело: складено автором.

Фасилітація та координація тлумачиться як сприяння зв'язкам і мережевому управлінню процесами, що сприяють колективним діям членів – тих, хто об'єднався для досягнення спільної мети та яка резонує з ними. Щоб колективно досягти прогресу, вони повинні бути пов'язані один з одним, досягти консенсусу щодо пріоритетів, а також розробити та реалізувати спільну діяльність. Мережі потребують таке адміністрування, яке стосується виконання операційних і матеріально-технічних завдань, а також виступає основою для організації спільної діяльності.

Мережі забезпечують простір для встановлення зв'язків і колективних дій на основі співпраці, стосунків і спільної мети. Мережі часто потребують підтримки спеціального управління людьми, залученими для підтримки учасників у визначенні та досягненні спільних цілей. Незважаючи на те, що мережі різноманітні за своїми цілями, структурами та формальністю, вони часто потребують спеціальної підготовки відповідних фахівців різних рівнів

відповідальності та повноважень, аби мережі були ефективними та результативними [157].

Використовуючи запропонований вище практичний тристоронній підхід, мережеві фахівці мають можливість зберігати певний простір для побудови співпраці та розвитку відносин. Вони координують і сприяють діяльності членів та реалізації їхніх колективних проектів, підтримують бачення та стратегію, мобілізують ресурси для їх реалізації та здійснюють моніторинг та діагностику її ефективності.

Це підтверджується дослідженням китайських вчених Е. Заглул, Ц. Рень, Т. Лі (Ehab Zaghloul, Jian Ren, Tongtong Li), які обґрунтовують, що система діагностики визначає мережі як такі, що складаються з трьох основних компонентів – мережевих можливостей, мережевих функцій та організаційних функцій. Потужностями виступають елементи, які мережі повинні мати для ефективності роботи. Можливості мережі включають спільну мету, членство, лідерство, ресурси тощо. Функціями мережі дослідники вважають дії, які мережа здійснює через залучення та участь членів для досягнення спільної мети – наприклад, адвокація, ідейне лідерство або вирішення проблем [210].

Отже, управління мережею в державному секторі можемо тлумачити як процес впливу суб'єктів на об'єкти управління в межах організаційної мережі за допомогою відповідних механізмів (нормативно-правового, організаційного, кадрового, фінансово-економічного, технологічного, інформаційно-комунікативного та ін.) з метою досягнення запланованих результатів.

При цьому, забезпечуються виконання функцій сприяння, координації та адміністрування, які підтримують і зміцнюють мережу, дозволяючи учасникам проектувати, розробляти та впроваджувати заходи, спрямовані на досягнення спільної мети мережі.

Побудова взаємозв'язку та логіки управлінських процесів у мережевій структурі включає в себе створення системи взаємодії, співпраці та обміну

інформацією між стейкхолдерами та бенефіцарами для досягнення спільних цілей. У цьому зв'язку пропонуємо кореляцію основних завдань та заходів для побудови управлінських процесів у мережевій структурі (табл 2.1).

Таблиця 2.1

Основні завдання та заходи для побудови управлінських процесів у мережевій структурі

Основні завдання для побудови управлінських процесів у мережевій структурі	Основні заходи з реалізації
Визначення ролей та обов'язків	окреслення ролі та обов'язків кожного стейкхолдера та бенефіцара у мережі: розподіл відповідальності, повноважень щодо конкретних завдань та дій
Створення структури комунікації	розробка структури комунікації: визначає, яким чином інформація буде обмінюватися між стейкхолдерами та бенефіцарами: регулярні зустрічі, внутрішню пошту, спільні платформи для обміну інформацією тощо
Укладення угод та договорів	підготовка угод або договорів, які регулюють правила співпраці та обміну інформацією між стейкхолдерами та бенефіцарами (можуть включати умови щодо конфіденційності, відповідальності та інші аспекти співпраці)
Спільне прийняття рішень	узгодження процедури та механізмів для спільного прийняття рішень у мережі (консенсус, голосування, узгодження чи інші способи ухвалення рішень)
Моніторинг і оцінка	розробка системи моніторингу, аналізу та оцінки, яка дозволить стейкхолдерам та бенефіцарам відстежувати прогрес досягнення цілей, аналізувати та оцінювати ефективність управління
Взаємодія та координація	узгодження алгоритмів взаємодії між стейкхолдерами та бенефіцарами (регулярні наради, спільні проекти, робочі групи тощо); забезпечення відкритого та взаємного зв'язку між стейкхолдерами та бенефіцарами, щоб змінювати стратегії та дії, якщо це необхідно; розробка системи врегулювання конфліктів та вирішення розбіжностей у разі потреби

Джерело: складено автором.

Такий підхід може сприяти досягненню спільних цілей та оптимізації управлінських процесів у мережі. У цьому контексті практичні обов'язки учасників мережі пов'язані з підтримкою її можливостей і функцій. Будь який спеціаліст матиме власний конкретний портфель завдань і заходів. Команда

мережевих менеджерів та співробітники різних рівнів, швидше за все, виконуватимуть спеціалізовані ролі для підтримки діапазону можливостей і функцій мережі.

Підтримка можливостей мережі може включати сприяння спільному плануванню та постановці цілей або координацію процесів стратегічного планування. Залучення учасників поширюється на всі функції та можливості мережі, що включає в себе їхній зв'язок та співпраця один з одним, побудову та управління взаємодіями, а також забезпечення спільної роботи шляхом надання достатньо широкого діапазону можливостей, які вважаються доречними, значущими та залучають інтереси учасників. Забезпечення цього кола завдань вимагає широкого набору знань, вмінь та навичок від стратегічного системного мислення високого рівня до практичного потенціалу мережевого управління проєктами [163].

Роль державних механізмів у реалізації концепту мережевого управління вкрай важлива. Державні механізми створюють умови, визначають рамки та забезпечують необхідні ресурси для розвитку та функціонування мережеских структур у державному секторі.

Для реалізації мережевого управління важливо мати відповідний правовий фреймворк, який визначає законодавчу базу для співпраці між різними органами та стейкхолдерами. Державні органи відповідають за створення та підтримання такого фреймворку.

Для успішної реалізації мережевого управління потрібні відповідні державні ресурси, включаючи бюджетні асигнування, інфраструктуру та інші матеріальні та фінансові ресурси.

Фінансово-економічні механізми забезпечують розподіл ресурсів для мережеских ініціатив.

Механізм кадрового забезпечення сприяє розвитку професійного потенціалу для мережевого управління, включаючи навчання, тренування та розвиток навичок співпраці та комунікації.

Технологічний механізм пов'язується із використанням інноваційних

технологій та розвитком інформаційних систем для покращення взаємодії та обміну інформацією між органами.

Загальною метою механізмів реалізації мережевого управління є сприяння створенню умов для співпраці, взаємодії та досягнення спільних цілей між різними органами державної влади та зацікавленими стейкхолдерами/беніфіцарами.

Отже, механізми реалізації мережевого управління у діяльності органів державної влади можемо розуміти як конкретні норми, правила, інструменти, підходи та процедури, які використовуються для впровадження і функціонування мережевих структур у процесі управління та прийняття рішень з метою забезпечення співпраці й взаємодії між різними стейкхолдерами/беніфіцарами (органами влади, громадськими організаціями, приватним сектором та іншими зацікавленими сторонами), класифікацію яких наведено на рис. 2.4.

Загалом, державні механізми відіграють важливу роль у сприянні реалізації концепції мережевого управління, забезпечуючи правовий фундамент, координацію, технології, фінансово-економічні ресурси та кадри для ефективної діяльності органів державної влади.

Підсумовуючи, зазначимо, що управління мережами за своєю суттю є доволі складним. Суб'єкти, які беруть участь у мережах, наділені владою, мають встановлені соціальні та договірні відносини і можуть впливати на прийняття рішень.

Тим не менш, організації залежать один від одного, оскільки мережі є засобом досягнення своїх цілей і можуть бути ключем до їх виживання.

Співпрацюючи в мережах органи державної влади повинні не тільки управляти внутрішніми операціями, але також мають організовувати та скеровувати власну участь у багатоорганізаційних структурах, оскільки можливості для управління мережами відрізняються від тих, які необхідні для управління однією організацією чи установою.

Нормативно-правовий механізм	• закони та правові норми грають ключову роль у встановленні основних рамок для мережевого управління: регулюють структури, процеси та обов'язки учасників мережі; забезпечують захист прав та інтересів різних стейкхолдерів
Організаційний механізм	• органи влади можуть створювати спеціальні відділи або одиниці, які відповідають за розвиток та впровадження мережевого управління. Організаційні механізми також включають в себе визначення ролей та відповідальностей в урядових органах для забезпечення координації та співпраці
Фінансово-економічний механізм	• державні бюджети та фінансові ресурси важливі для реалізації мережевого управління. Фінансування проектів та програм, спрямованих на співпрацю, використовуються для створення інфраструктури для обміну інформацією та спільного прийняття рішень
Механізм кадрового забезпечення	• наявність кваліфікованих кадрів із знаннями та навичками є критично важливою. Державні установи (наприклад НАДС), можуть розвивати програми навчання та надавати підтримку для підвищення кваліфікації працівників, що беруть участь у мережевих структурах
Інформаційно-комунікативний механізм	• забезпечення доступу до інформації та ефективної інтерактивної комунікації між учасниками мережі є ключовими для успішної реалізації мережевого управління, що сприятиме обміну інформацією та забезпечуватиме інформаційну підтримку
Технологічний механізм	• використання спеціалізованих інформаційних систем та платформ; веб-порталу; системи моніторингу для збору даних про прогрес та результати діяльності; новітніх технологій, таких як штучний інтелект, блокчейн, інтернет речей (IoT) та інші

Рис. 2.4. Державні механізми реалізації мережевого управління

Джерело: складено автором.

Управління має справу зі складнощами, взаємозв'язками та динамікою між організаціями, що працюють у мережах.

Ці складнощі, взаємозалежності ускладнюють прийняття рішень, оскільки відповідальність може зміщуватися, а рішення, які прийняті однією організацією, можуть впливати на інші організації.

Наслідки таких рішень складно прогнозуються, а тому немає єдиного способу прийняття рішень на рівні мережі.

Державні механізми мережевого управління можуть бути різними і залежати від контексту. Основні суб'єкти мережевого управління повинні взаємодіяти один з одним, вирішувати можливі конфлікти та досягати разом бажаних результатів.

Хоча не існує формалізованих процесів мережевого управління для залучення нових гравців у мережу, мережі можуть розвиватися в міру приєднання нових організацій та виходу інших.

Таким чином, організаційна мережа розвивається з плином часу з усіма видами внутрішніх і зовнішніх змін.

Тому механізми мережевого управління використовуються для вирішення різноманітних питань з урахуванням змін, які можуть виникнути у процесі діяльності органів державної влади.

Виходячи з вищенаведеного, приходимо до висновку, що мережеве управління позиціонується як безперервний процес.

Рішення, яке приймається адміністраторами мережі, може бути остаточним, повідомленим та реалізованим за допомогою інших механізмів державного управління, або рішення може бути оскаржене і призвести до перегляду питань, і процес розпочнеться спочатку.

Аналіз наукової літератури свідчить, що в мережевому управлінні визначена структура та окреслені державні механізми можуть бути доповнені чи оновлені. Питома вага використання тих чи інших державних механізмів мережевого управління відрізняється залежно від ситуації [168].

Таким чином, існує процесний та безперервний цикл між переглядом порушених питань, повторним узгодженням рішень, використанням різного роду державних механізмів та інструментів мережевого управління, неформальними процесами та рішеннями, реалізацією та адаптацією інструментів та методів до нових обставин чи умов (рис. 2.5).

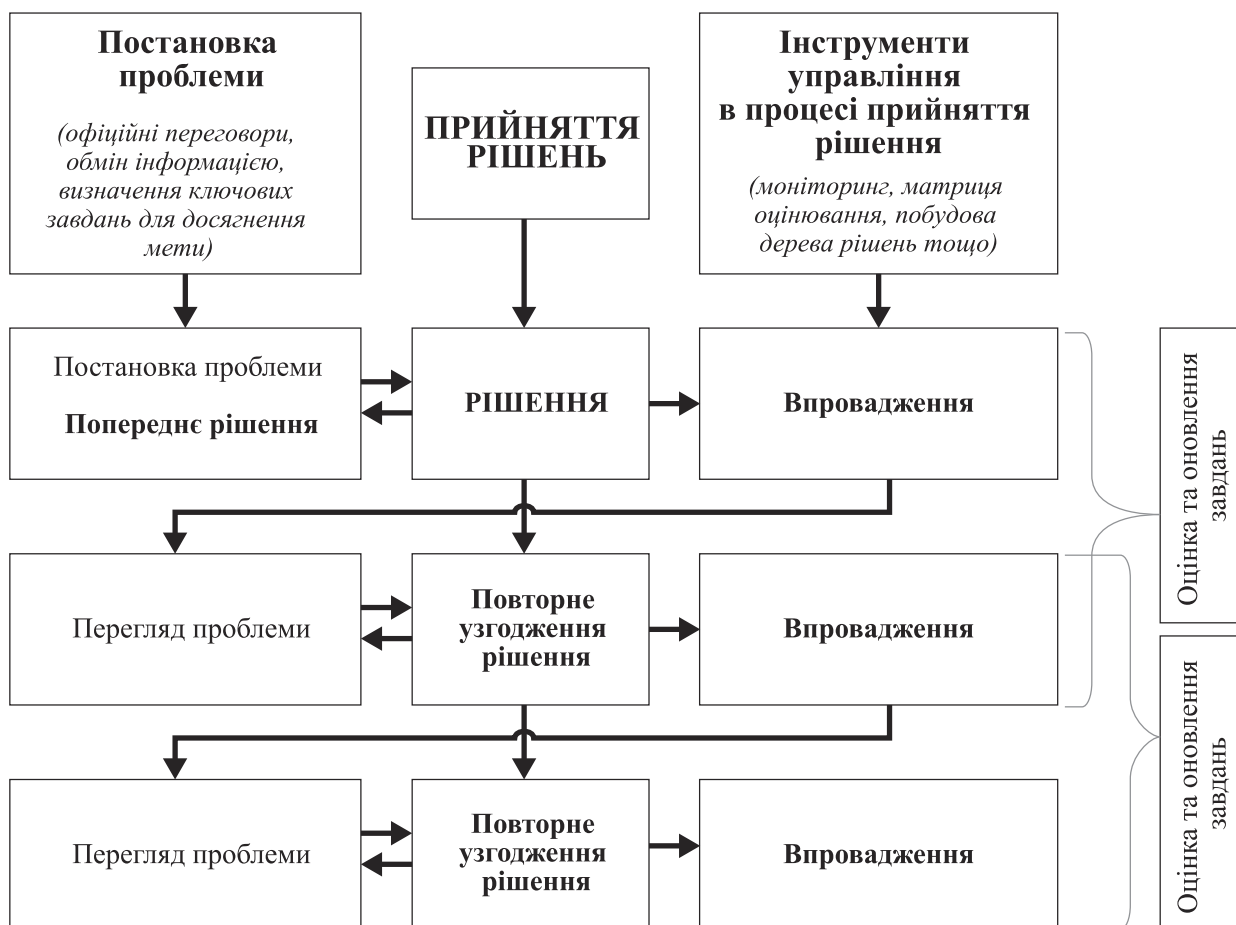


Рис. 2.5. Відображення процесного циклу у мережевому управлінні

Джерело: складено автором

Тим не менш, формальні механізми можуть залежати від таких змінних, як зрілість мережі, її призначення, використовувані програмні системи, екзистенція і форма лідерства та інші змінні. Крім того, в процесі впровадження рішення може стати зрозуміло, що певні державні механізми мережевого управління недостатні для вирішення деяких питань, що потребує певних змін. Таким чином, існує безперервний цикл оновлення заздалегідь визначеної структури мережевого управління, який, у свою чергу, досягається шляхом використання потрібних механізмів управління, що призводить до розвитку набору рекурсивних зв'язків.

Мережеве управління у діяльності органів державної влади може ставити перед собою різноманітні цілі, і вони можуть варіюватися в залежності від контексту, сфери та завдань конкретної мережі.

Окреслимо основні цілі мережевого управління, які полягають у наступному:

- забезпечення ефективності: мережеве управління має бути спрямоване на підвищення ефективності управління державними ресурсами та послугами шляхом поліпшення співпраці і координації між різними державними органами, агентствами та стейкхолдерами/беніфіцарами;
- збільшення відкритості і прозорості: мережеве управління повинно сприяти створенню більш відкритого та прозорого адміністрування, що підвищує довіру громадян до державних органів і сприяє боротьбі з корупцією;
- забезпечення потреб громадян: мережі державного сектору мають бути орієнтовані на забезпечення потреб громадян, налагоджуючи доступ до якісних адміністративних послуг і ресурсів;
- підвищення інноваційності: мережеве управління сприяє обміну ідеями та інноваціями між різними стейкхолдерами/беніфіцарами, що забезпечує розвиток нових і кращих підходів до вирішення проблем;
- сприяння сталому розвитку: мережеве управління сприяє забезпеченню збереження прав людини та природних ресурсів, екологічної стійкості; доступу до якісної освіти та охороні здоров'я; розвиток стійкої та резильєнтної інфраструктури; зміцнення міжнародного співробітництва тощо.

Запропонована процесна модель механізмів реалізації мережевого управління у діяльності органів державної влади наведена на рис.2.6



Рис. 2.6 Процесна модель механізмів реалізації мережевого управління у діяльності органів державної влади

Джерело: складено автором

Зазначене дало змогу стверджувати, що функціонування механізмів мережевого управління у діяльності органів державної влади

концептуалізується як динамічний соціотехнологічний процес, який здійснюється через сукупність правових норм, постулатів, стандартів, принципів, методів та інструментів, за допомогою яких держава створює умови для впровадження мережевого управління у різних сферах життєдіяльності сучасного глобалізованого суспільства.

Цей процес характеризується постійною взаємодією між учасниками, розвивається і керується завдяки виникненню проблем, які потребують вирішення, та коригується внутрішніми діями суб'єктів організаційної мережі.

Однак, при цьому варто зазначити, що незважаючи на популярність мережевої моделі управління, не можна сказати, що вона беззастережно міцно закріпилася в практиці державного управління в демократичних країнах. І пов'язано це не стільки з об'єктивними обмеженнями мережевої моделі, скільки з політичною специфікою самої держави. Держава не є монолітною, вона складається з різних підсистем, кожна з яких має свою специфіку (ключові суб'єкти, характер проблем, регулюючі інструменти, обсяг ресурсів і капіталу тощо). Використання конкретних силових та управлінських інструментів має відповідати функціям, які виконує держава в різних соціально значущих сферах, і має бути спрямовано на забезпечення адаптивної ефективності її інститутів.

Відповідно, в одних підсистемах доцільно використовувати традиційні бюрократичні та примусові методи, тобто нормативно-правові механізми, в інших – ринкові методи, як-то: надання окремих видів адміністративних послуг, в третіх – мережеві методи, які є найбільш витратні і складні у досягненні мети, такі як соціальний захист, забезпечення екологічної безпеки тощо. Принципове значення має і масштаб розв'язуваної задачі: чим вона вужча і конкретніша, тим менше підстав для використання мережевого управління, оскільки переваги такого управління демонструються за умови невизначеності і масштабності.

Таким чином, сучасна, інституційно стійка держава прагне

диверсифікувати свої управлінські моделі та інструменти, виходячи зі специфіки профілів своєї діяльності. Вона задає логіку взаємин акторів, окреслює межі взаємодії акторів, обмежуючи або розширюючи їх можливості для самоорганізації, пристосування до мінливих зовнішніх і внутрішніх умов середовища.

Висновки до розділу 2

Доведено, що реалізація мережевих технологій у діяльності органів державної влади дозволить досягти в Україні європейського рівня цифровізації суспільства. Формування стійкого цифрового суспільства є значущим фактором провадження національної безпеки, забезпечення незалежності держави, сприяння чесній конкуренції українських компаній, а також ефективного прийняття державно-управлінських рішень. Реалізація мережевого підходу є інструментом ефективного розвитку цифрових технологій, які є основою для реформування державного управління, національної економіки, приватного сектору, соціальної сфери, кібербезпеки. Констатовано, що у ландшафті кібербезпеки, що швидко розвивається, постійно з'являються нові загрози. Встановлено, що технічні рішення є лише частиною багаторівневої кібербезпеки держави, а тому основним завданням сьогодення на національному рівні є впровадження мережевого управління як інструменту реалізації державної кіберполітики у сфері аналізу та оцінювання даних та наявних кіберзагроз, професійного навчання та підвищення кваліфікації публічних службовців, а також участі органів державної влади у провадженні глобальної кібербезпеки.

Визначено, що сучасним інструментом оперативного реагування на кризові виклики інформаційної та кібербезпеки є ситуаційні центри, які функціонують на засадах мережевого управління та активно використовується органами державної влади (наприклад, CERT-UA у складі Державної служби спеціального зв'язку та захисту інформації України). Їх

діяльність спрямована на ефективне прийняття рішень у сфері управління динамічними ситуаціями (комп'ютерними надзвичайними подіями) на основі виявлення та всебічного аналізу інформації щодо їх змін, а також прогнозування їх подальшого розвитку.

Зазначено, що на міжнародній арені своєчасне визначення та узгодження Україною із країнами-партнерами заходів інформаційної безпеки та колективної протидії вірусній російській пропаганді на засадах мережевого управління може передбачати адаптацію існуючих моделей ситуаційного аналізу та подальшу розробку нових моделей з урахуванням нових міжкраїнових домовленостей та викликів. Застосування динамічного моделювання ситуацій із використанням вихідних даних та подальшим аналізом ситуацій щодо пропаганди є необхідним для визначення можливих наслідків прийнятих рішень щодо контрпропаганди та їх впливу на суспільну думку. Рекомендовано імплементувати адаптивні системи опису факторів та передумов виникнення можливих ситуацій за допомогою імітаційного (динамічного) моделювання, завданням якого має бути визначення вихідних даних, що відображають умови і фактори виникнення інформаційної окупації задля розробки заходів щодо запобігання їх появі у майбутньому.

На основі компаративного аналізу світового досвіду визначено основні засади діяльності ситуаційних центрів в міжнародних міжурядових організаціях та об'єднаннях на прикладі ситуаційних центрів SITCEN NATO, SANER, ISAC, NCI, а також мережевих платформ HCSS StratBase Datalab, Exonaut, MASA Synergy, Effector та центрів реагування на інциденти у сфері кібербезпеки CSIRT, CERT, NCSC-FI, ECCSA в США й окремих країнах ЄС (Швеції, Франції, Литви, Польщі, Португалії, Норвегії, Фінляндії, Нідерландів).

Узагальнено, що ситуаційні центри є інструментом постійного моніторингу, аналізу та оцінки даних, моделювання ситуацій для прийняття управлінських рішень в кризових ситуаціях, а також осередком здійснення результативної координації зусиль органів державної влади щодо протидії

військовим внутрішньодержавним чи міждержавним конфліктам, політичним кризам, кіберзагрозам, пандемічним ситуаціям у випадку поширення хвороб, стихійним лихам, техногенним катастрофам терористичним злочинам, загрозам стратегічної інфраструктури (зокрема, енергетичної, сільськогосподарської та ін.).

Визначено, що головною метою створення ситуативних центрів в умовах сучасних геополітичних викликів є забезпечення національних інтересів країни та/чи безпеки міжнародної діяльності в усіх її аспектах, концентруючись на протидії ризикам, пов'язаним як з діяльністю окремих осіб чи їх груп, так і з можливими надзвичайними ситуаціями, спричиненими природними явищами.

Діяльність ситуаційних центрів може передбачати їх спеціалізацію на окремих напрямках чи сферах, або охоплювати широке коли проблем, вирішення яких покладається на спеціально створену мережу. Прийняття рішень при цьому здійснюється на основі постійного моніторингу та збору ситуаційної інформації, яка обробляється (аналізується та оцінюється) спеціальними системами ситуаційного управління. Системи ситуаційного моделювання дозволяють оптимізувати процеси планування, покращити дієвість планів в умовах надзвичайних ситуацій, оцінювати характер впливу катастроф на населення, майно та інфраструктуру.

Обґрунтовано, що організація діяльності мережі ситуаційних центрів потребує широкого ресурсного забезпечення, яке охоплює широкий спектр інструментів (приміщень, матеріальних засобів, обладнання тощо) та відповідно підготовлений кваліфікований персонал. Зокрема, у світовій практиці спостерігається стійка динаміка до розвитку високотехнологічних спроможностей, які дозволяють максимально швидко відстежувати ситуацію, збирати інформацію та допомагати управлінцям приймати оперативні рішення, а також, здійснювати моделювання будь-якої проблемної ситуації, прогнозувати її наслідки та передбачати можливі варіанти її розвитку з використанням кількісної та якісної оцінки одержаної інформації.

Встановлено, що подальші дослідження діяльності ситуаційних центрів повинно спрямовуватися на винайдення шляхів адаптації та узгодження світового досвіду із українською практикою в контексті пошуку оптимальних організаційних, фінансово-економічних механізмів мережевого управління їх функціонування, а також на розробку сучасних цифрових інструментів, які б забезпечували оперативну взаємодію органів державної влади та ефективну розробку і реалізацію ними управлінських рішень щодо управління кризовими ситуаціями.

Доведено, що застосування механізмів мережевого управління та запровадження мережевої організації роботи у діяльності органів державної влади може привести до позитивних результатів, які в значній мірі залежать від специфіки контексту, якісної реалізації та підтримки такого підходу.

Визначено послідовність застосування мережевого підходу у державному управлінні, як процесу моніторингу, оцінки, аналізу та адміністрування міжорганізаційними структурами, що складається з трьох етапів реалізації:

- створення початкових зв'язків, легітимності, встановлення когнітивної та емоційної довіри;
- управління мережами шляхом створення спільних і гнучких структур і встановлення чітких цілей;
- досягнення прогресу щодо цілей мереж органів влади.

Відповідно до цього запропоновано тристоронній алгоритм практичних заходів з впровадження механізмів реалізації мережевого управління у діяльності органів державної влади: фасилітація; координація; адміністрування. Доведено, що мережевий підхід створює умови для покращення внутрішньої та зовнішньої координації роботи державних органів, що дозволяє вирішувати складні проблеми більш ефективно, оскільки внаслідок кращої взаємодії зникає дублювання завдань і ресурсів, що може заощадити час та бюджетні витрати. Загалом, впровадження

мережевої організації роботи в державних органах може покращити їхню ефективність, сприяти більш адаптивному управлінню та відкритості в діяльності, а також стимулювати інновації та сталий розвиток. Однак успішність такого підходу залежить від багатьох факторів, включаючи підтримку з боку влади, готовність до змін та якість управління процесами мережевої співпраці. Запропоновано кореляцію основних завдань та заходів для побудови управлінських процесів у мережевій структурі.

Розроблено процесну модель механізмів реалізації мережевого управління у діяльності органів державної влади, яка складається з мети, принципів функціонування (співпраці та партнерства, спільного прийняття рішень, децентралізації та автономії, горизонтальних та вертикальних зв'язків), факторів (політичної волі, вироблення державної політики, ресурсів та фінансування, розвитку інституційної культури, наявності кваліфікованих кадрів, міжнародних та геополітичних чинників, технологічних можливостей, готовності до змін), суб'єктів та об'єктів впливу (передбачає взаємодію між ними) та тристороннього алгоритму практичних заходів впровадження (*фасилітації* – залучення учасників до процесу для розуміння цілей їхньої участі, планування способів досягнення цих цілей і спільної роботи; *координації* – організації та синхронізації процесу спільної роботи всіх учасників для досягнення загальної мети; *адміністрування* – забезпечення виконання завдань, контролю, просування та підтримки функціонування мереж).

Практична реалізація моделі здатна призвести до покращення ефективності роботи органів державної влади через кращу координацію та співпрацю між ними та стейкхолдерами/беніфіцарами. Це може призвести до досягнення кращих результатів та більшої відповідності до цілей та потреб громадян; стимулюватиме залучення їх та зацікавлені сторони до процесів управління і прийняття рішень, що забезпечить більш глибоке розуміння потреб і очікувань громадськості; дозволить органам влади ефективно адаптуватися до змін в політичному, економічному та соціокультурному

середовищі; сприятиме обміну ідеями та навчанню від інших стейкхолдерів, що може призвести до стимулювання інновацій та креативності в роботі органів влади.

Основні результати розділу 2 опубліковано в наукових працях автора:
[102; 103; 105; 107].

РОЗДІЛ 3

РОЗВИТОК МЕХАНІЗМІВ МЕРЕЖЕВОГО УПРАВЛІННЯ У ДІЯЛЬНОСТІ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ УКРАЇНИ

3.1 Забезпечення розвитку економічного механізму реалізації мережевого управління у діяльності органів державної влади в Україні

Забезпечення розвитку мережі ситуаційних центрів органів державної влади в Україні на основі світових здобутків потребує застосування дієвого економічного механізму їх функціонування, який би дозволяв забезпечувати їх потреби у необхідних фінансових матеріально-технічних, кадрових, інформаційних та інших ресурсах. Згідно Рішення Ради національної безпеки та оборони України від 4 березня 2021 року «Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони» передбачено, що з метою «...підвищення ефективності інформаційно-аналітичного забезпечення прийняття управлінських рішень, взаємодії, координації і контролю за діяльністю органів виконавчої влади...» визнається за необхідне «...розширення та подальший розвиток єдиної мережі ситуаційних центрів...». На виконання цього рішення на Кабінет Міністрів України, Апарат Ради національної безпеки і оборони України, Службу безпеки України, а також Службу зовнішньої розвідки України покладається завдання щодо забезпечення подальшого розвитку мережі ситуаційних центрів, а також можливості розгортання резервних ситуаційних центрів у запасних пунктах управління.

Таким чином, наразі в Україні створено правові засади діяльності ситуаційних центрів органів державної влади, як мережі інформаційно-аналітичного забезпечення прийняття управлінських рішень органами державної влади. Водночас, їх економічне забезпечення потребує чітке визначення джерел їх фінансування, а також створення механізмів, які б гарантували узгодження цілей державної політики, на реалізацію якої

спрямовується їх діяльність, чітких результатів їх досягнення та відповідальності посадових осіб за цільове використання призначених бюджетних коштів.

Узгодження джерел ресурсування ситуаційних центрів з методами їх використання відповідно до визначених цілей їх функціонування, а також формування необхідної та достатньої матеріально-ресурсної бази, передбачає формування економічного механізму реалізації мережевого управління органів державної влади.

Поняття економічного механізму набуло доволі широкого обґрунтування у науковій літературі. Так, А. Бонарчук та Є. Бронська визначають економічний механізм як «систему економічних методів, які направлені на забезпечення функціонування, підвищення ефективності виробничої системи». Вчені також уточнюють його зміст, вказуючи, що це «комплекс взаємопов'язаних та чітко впорядкованих заходів, які реалізуються за допомогою різних методів господарювання і забезпечують раціональне протікання певних економічних процесів; додатково виділяють підсистеми оцінки та аналізу будь-якого виду діяльності, планування, контролю, мотивації та стимулювання» [113].

Як зазначає В. Ткач, економічний механізм є відкритою складною інтегрованою системою, яка «постійно розвивається та складається з комплексу взаємопов'язаних елементів». Останні спрямовані на ефективне використання ресурсів у процесі діяльності та забезпечення стійкого розвитку [112]. Економічний механізм за визначенням О. Брижака – «це сукупність методичних інструментів, які дають можливість моделювати варіанти прийнятих рішень, розробляти засоби їх аналізу й реалізації, чим підвищують їх обґрунтованість та знижують ризик від упровадження» [2].

О. Власюк звертає увагу на структуру економічного механізму реалізації стратегії і зазначає, що вона включає в себе розроблену «систему фінансового забезпечення та систему економічних інструментів, які спрямовані на перетворення соціальної активності ... у важливі ресурси

економічного розвитку ...» [2]. Натомість, Л. Валага та С. Бондаренко звертають увагу, що економічний механізм системи потрібно розглядати як спосіб взаємодії всіх їх елементів із притаманними йому формами і методами діяльності, який дозволяє досягнути мети діяльності організації [4].

Узагальнюючи такі наукові підходи та з урахуванням особливостей предмету нашого дослідження, зазначимо, що на нашу думку формування *економічного механізму реалізації мережевого управління у державному секторі*, яке реалізується через діяльність системи ситуаційних центрів, передбачає узгодження процесів визначення їхніх потреб, акумулювання та використання необхідних ресурсів (фінансових, матеріальних, людських, технологічних та ін.), а також оцінювання результатів їх роботи, що втілюються у створених ними продуктах (послуги, роботи) та суспільних ефектах, що вони спричиняють, відповідно до визначених цілей та принципів.

Схематичне представлення складових елементів економічного механізму реалізації мережевого управління в діяльності органів державної влади представлено на рис. 3.1.

Основу економічного механізму реалізації мережевого управління органів державної влади складають його цілі, які визначають головні напрями потреб його інституційних одиниць – ситуаційних центрів. Цілі формування економічного механізму мережевого управління органів державної влади повинні відповідати основним завданням діяльності ситуаційних центрів. Так, згідно з постановою Кабінету Міністрів України «Питання мережі ситуаційних центрів» від 11 липня 2023 року [54], основними завданнями ситуаційного центру Кабінету Міністрів України є експертно-аналітичне та інформаційне супроводження діяльності самого Кабінету Міністрів України, а також його прем'єр-міністрів та віце-прем'єр міністрів.

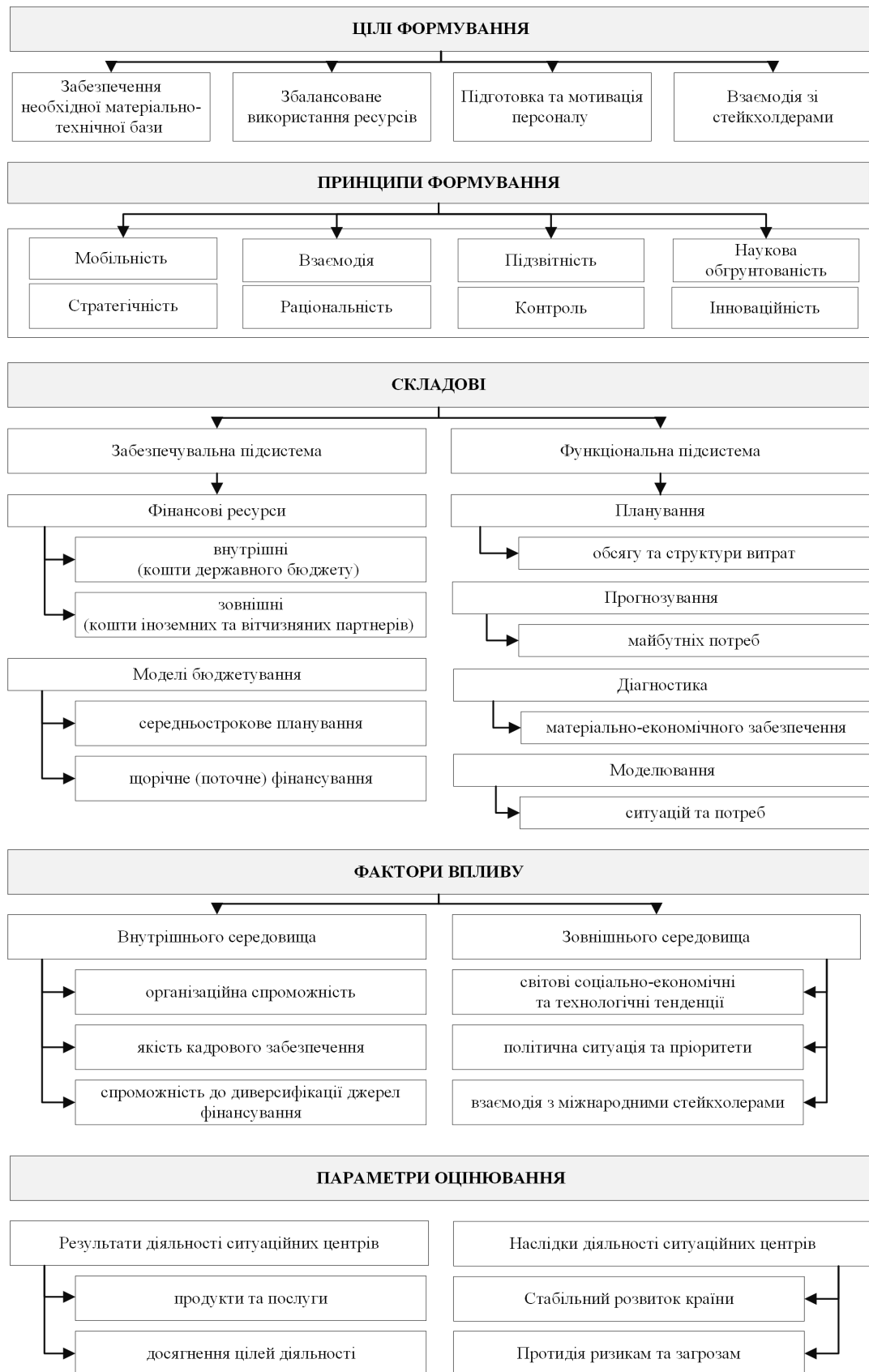


Рис. 3.1. Економічний механізм реалізації мережевого управління в діяльності органів державної влади

Джерело: розроблено автором.

Відповідно, цілями формування економічного механізму, на нашу думку, мають бути:

- забезпечення матеріально-технічної бази, необхідної для виконання покладених на ситуаційні центри завдань, зокрема інформаційно-комунікаційні системи, підсистеми зв'язку, комплекси технічного захисту, засоби електроживлення, програмне та апаратне забезпечення та ін.;

- збалансоване використання ресурсів, що передбачає їх розподіл відповідно до визначених стратегічних та оперативних завдань діяльності ситуаційних центрів;

- підготовка та мотивація персоналу ситуаційних центрів, зокрема основних фахівців, необхідних для виконання безпосередніх завдань ситуаційного центру (зокрема фахівців з обробки даних, аналізу та візуалізації даних, фахівців з обробки геопросторових даних, фахівців з цифрового захисту, забезпечення роботи цифрових комунікаційних мереж), так і допоміжного (обслуговуючого) персоналу (на кшталт фахівців з технічної підтримки роботи систем та програм, фахівців з комунікацій та взаємодії зі стейкхолдерами, фахівців з роботи з людськими ресурсами, фахівців з фінансового забезпечення та ін.);

- взаємодія зі стейкхолдерами вироблення державної політики, на реалізацію цілей і завдань якої спрямована діяльність ситуаційного центру органу державної влади, серед яких ситуаційні центри інших органів державної влади як на центральному та і на регіональному рівнях, інші органи державної та місцевої влади, виконавчі інституції у сфері реалізації державної політики, установи та організації публічного сектору, громадські організації, міжнародні партнери.

Формування економічного механізму мережевого управління органів державної влади повинно здійснюватися на засадах сучасних підходів організації системи державного управління із дотриманням його класичних принципів. Серед переліку принципів обґрунтованих, зокрема

Н. Шурою [125], відзначимо ті з них, що мають безпосередній прояв мережевого управління органів державної влади:

Таблиця 3.1

Принципи мережевого управління у діяльності органів державної влади

Прояв в діяльності ситуаційних центрів	Принцип	Зміст принципу
Безпосередній	верховенство права	діяльність органів державної влади повинна здійснюватись виключно згідно із законодавчими та нормативними актами
	об'єктивність	дотримання максимальної безкорисливості у прийнятті управлінських рішень
	пропорційність	масштаби управлінських рішень і способи їх реалізації мають відповідати цілям адміністрування
	службова співпраця	надання допомоги різними відомствами під час підготовки адміністративних рішень
	ефективність	економне використання ресурсів під час прийняття рішень з адміністрування, мінімізація витрат на прийняття рішень
	субсидіарність	рішення суб'єктів публічного управління мають реалізовуватись на тих рівнях, де їх виконання є найбільш ефективним
	пріоритет вироблення державної політики	політика служить формою узагальнення та вираження інтересів окремих соціальних груп чи суспільства загалом
	зворотній зв'язок	забезпечення зворотної взаємодії органів державної влади із громадянами
	системний підхід	організація державного управління як системи, забезпечення її функціонування та розвитку
Опосередкований	незловживання владою	діяльність суб'єктів державного управління має здійснюватись тільки у межах, визначених в чинному правовому полі
	єдиний сервісний доступ	підготовка інформації на замовлення громадян, прийом скарг, пропозицій, відповіді на них на одному робочому місці
	демократія	державне управління здійснюється за згоди тих, ким управляють
	централізм на демократичній основі	механізм делегування владних і управлінських повноважень на підставі розділення центрів влади і прийняття рішень
	соціальна справедливість	поєднання принципу свободи підприємництва з принципом соціальної допомоги бідним прошаркам населення

Джерело: складено автором на основі [128].

Таким чином, дотримання принципів державного управління є передумовою забезпечення успішності діяльності ситуаційних центрів органів влади. Водночас, на нашу думку, варто виокремити специфічні принципи, яких необхідно дотримуватись при формуванні економічного механізму реалізації мережевого управління в діяльності органів державної влади. Серед таких принципів, нами визначено (див. рис. 3.1):

- *мобільність*, що передбачає можливість просторового переміщення центрів прийняття рішень та їх функціонування в режимі дистанційного керування;

- *стратегічність*, що передбачає орієнтацію оперативної діяльності на вирішення стратегічних завдань ситуаційних центрів у відповідності до цілей державної політики, реалізацію якої здійснює керівний орган для такого центру державної влади;

- *взаємодія*, що передбачає взаємодоповнюваність, взаємне консультування та взаємну підтримку прийняття рішень в процесі мережевого управління органами державної влади, що дозволить покращити якість моніторингу об'єкту спостереження та прийняття управлінських рішень;

- *раціональність*, що передбачає формування необхідних для функціонування ситуаційних центрів ресурсів, у відповідності до потенційно отриманого результату;

- *підзвітність* щодо цільового використання отриманих фінансових ресурсів, зокрема за рахунок бюджетних коштів; при цьому необхідно враховувати обґрунтований рівень секретності та захисту даних для забезпечення цілей національної безпеки та оборони країни;

- *контроль*, який полягає у періодичному нагляді за використання наданих для ситуаційного центру ресурсів з точки зору їх цільового використання;

- *наукова обґрунтованість* прийнятих управлінських рішень, яка б дозволяла довести раціональність використання доступних ресурсів в діяльності ситуативного центру;
- *інноваційність*, що передбачає постійне оновлення матеріально-технічної бази у відповідності до суспільного прогресу, щоб розробляти управлінські рішення із застосуванням цифрових технологічних пристроїв та програм.

Системи застосування економічного механізму реалізації мережевого управління у діяльності органів державної влади із таких складових підсистем.

Забезпечувальна підсистема передбачає комбінацію фінансових ресурсів, якими є кошти державного бюджету (*внутрішні ресурси*) та донорські кошти вітчизняних та іноземних партнерів (*зовнішні кошти*), з прийнятною для органу влади моделлю бюджетування. Ситуативні центри, як інституційні одиниці, що знаходяться у підпорядкуванні органів державної влади, отримують пряме фінансування на забезпечення своїх потреб за рахунок видатків державного бюджету. Органи державної влади, які є головними розпорядниками бюджетних коштів, передбачають необхідні обсяги фінансування діяльності їх ситуативних центрів та розподіляють їх у відповідності до визначених завдань. При цьому, в практиці державного управління, напрацьовано дві ключові моделі бюджетування. Перша з них базується на програмно-цільовому розподілі бюджетних коштів на засадах середньострокового планування. Такий підхід передбачає, що бюджетні кошти призначаються для реалізації цілей державної політики, реалізацію якої здійснює орган державної влади. Планування обсягів фінансування здійснюється з урахуванням прогнозних потреб на 3 роки, втім можливими є коригування у випадках надзвичайних обставин.

Інша модель бюджетування, що поширена в практиці державного управління, передбачає щорічне фінансування у розрізі бюджетних функцій. Обґрунтування видатків здійснюється на основі «історичних даних», при

цьому оцінка їх доцільності та якості бюджетних послуг не враховується. Окрім того, за цієї моделі бюджетні кошти спрямовуються на утримання бюджетних установ чи їх мережі без встановлення чіткої відповідальності за результати їх діяльності.

Відповідно до діючої в Україні системи бюджетування діяльності органів державної влади, кошти на їх функціонування призначаються та використовуються згідно із затвердженими для даного органу влади бюджетними програмами. Такий підхід реалізується в Україні згідно з Концепцією застосування програмно-цільового методу в бюджетному процесі, схваленою розпорядженням Кабінету Міністрів України від 14 вересня 2002 р. №539-р. [43]. Згідно зі статтею 2 Бюджетного кодексу України програмно-цільовий метод у бюджетному процесі передбачає управління бюджетними коштами для досягнення конкретних результатів за рахунок коштів бюджету із застосуванням оцінки ефективності використання бюджетних коштів на всіх стадіях бюджетного процесу [3].

Натомість, в сьогоденній практиці розподілу видатків державного бюджету не передбачається спеціальних бюджетних програм на фінансування діяльності ситуаційних центрів органів влади. Це, зокрема, прослідковується у переліку бюджетних програм, що реалізуються Міністерством оборони України, а також іншими центральними органами виконавчої влади. Не передбачається використання бюджетних коштів на функціонування ситуаційних центрів також відповідно до діючого переліку бюджетних програм, затвердженого наказом Міністерства фінансів України від 20.09.2017 № 793 (із змінами від 29.12.2017 № 1181) «Про затвердження складових Програмної класифікації видатків та кредитування місцевого бюджету».

Таким чином, бюджетне фінансування діяльності мережі ситуаційних центрів органів державної влади здійснюється без конкретизації в рамках програмно-цільового методу. Це призводить до неможливості оцінювання ефективності використання коштів державного бюджету та визначення

результативності досягнення цілей державної політики з точки зору забезпечення потреб громадян.

Водночас, головними перевагами від застосування програмно-цільового методу бюджетування для фінансування діяльності ситуаційних центрів органів державної влади в Україні, на нашу думку, мають стати:

- узгодження мети ресурсного забезпечення ситуаційного центру з виконанням поставлених перед державними органами цілей і завдань;
- перенесення акценту з витрат бюджетних коштів на виконання державних функцій, здійснення діяльності та досягнення результатів;
- здійснення контролю безпосередніх показників діяльності та кінцевих показників;
- визначення очікуваних результатів, що забезпечують досягнення поставленої мети;
- обґрунтування обсягу видатків на основі визначених цілей здійснення видатків і показників ефективності та результативності
- кошти державного бюджету спрямовуватимуться на досягнення найбільш ефективних результатів;
- персональна відповідальність керівників органів державної влади за досягнення результатів бюджетних програм.

З огляду на це, вважаємо за необхідне запровадити спеціальні бюджетні програми для органів державної влади, які є головними розпорядниками бюджетних коштів, що відображали б узгодження бюджетних коштів, що виділяються на фінансування діяльності ситуаційних центрів, з цілями державної політики та результатами їх досягнення. Типовою назвою таких бюджетних програм може стати *«Забезпечення функціонування ситуаційного центру ... (назва органу державної влади)»*. При цьому, самі ситуаційні центри можуть стати виконавцями таких бюджетних програм, формувати перелік напрямів спрямування бюджетних коштів за погодженням з їх керівним органом державної влади та звітувати

про їх використання відповідно до визначених показників оцінювання бюджетної програми.

Важливу перспективну роль у забезпеченні фінансових ресурсів для ситуаційних центрів органів державної влади на додаток до цільових видатків з державного бюджету, можуть відіграти, на нашу думку, зовнішні джерела. Особливо актуальним розвиток такого джерела фінансування стає з огляду на хронічний дефіцит державного бюджету в Україні та його посилення в сучасних умовах російсько-української війни, що розпочалась з 2014 року та набула повномасштабного формату з 22 лютого 2022 року. Потреба у залученні додаткових фінансових коштів зумовлюється необхідністю виконання поточних видатків соціального та оборонного характеру, які суттєво обмежують можливості формування ситуаційних центрів на базі сучасного інноваційного технологічного обладнання. Тому виконання завдання органів державної влади щодо розвитку мережі ситуаційних центрів варто реалізовувати із залученням донорських коштів, що можуть бути отримані в рамках реалізації проектів з розвитку, програм фінансової допомоги та ін. Перелік потенційних суб'єктів, що можуть надавати донорську допомогу на розвиток мережі ситуаційних центрів в Україні, представлено на рис. 3.2.

Серед потенційних джерел отримання зовнішніх фінансових ресурсів відзначимо:

- міжнародні валютно-фінансові організації, такі як Міжнародний валютний фонд, що надає кредити для уряду;
- допомога від ЄС, як інтеграційного об'єднання, приєднання до якого закріплено в Конституції України та здійснюється на сьогодні в рамках виконання Угоди про асоціацію між Україною та ЄС;
- допомога від урядів країн-партнерів, зокрема від США як лідера на світовій політичній арені в рамках реалізації його цілей щодо досягнення миру та протидії тероризму на світовій арені;

- міжнародні та іноземні фінансові посередники, якими можуть стати інвестиційні фонди, банки інших держав, гарантійні товариства та ін.;
- міжнародні та іноземні благодійні фонди та краудфандингові платформи, роль яких може стати доволі суттєвою за умови дотримання принципів демократичності та зміцнення громадянського суспільства;
- приватні компанії та особи-благодійники, які можуть мати потенційно особистий інтерес у захисті їх приватної власності, що буде забезпечено як наслідок діяльності ситуаційних центрів у вирішенні питань національної безпеки та оборони.

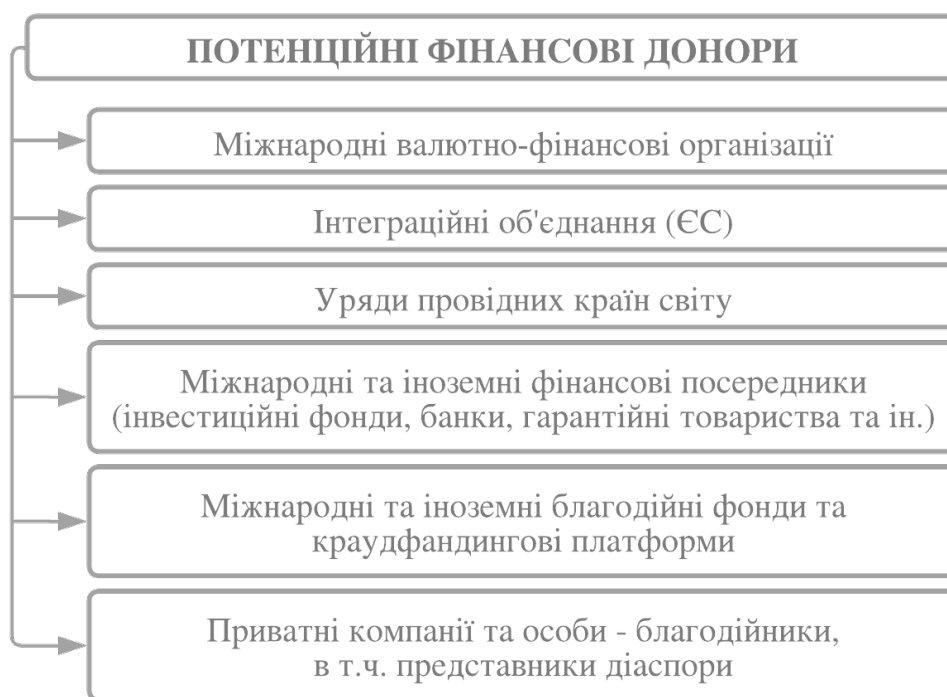


Рис. 3.2. Потенційні фінансові донори для забезпеченні потреб ситуаційних центрів органів державної влади

Джерело: розроблено автором.

Функціональна підсистема економічного механізму (див. рис. 3.1) мережевого управління органів державної влади доповнює вже описану нами забезпечувальну підсистему та передбачає здійснення фахівцями, що

відповідальні за забезпечення діяльності ситуаційних центрів, діяльності щодо:

- *планування* обсягів та структури витрат ситуаційних центрів з наявної ресурсної бази, аналізу її достатності та відповідності сучасному технологічному рівню;
- *прогнозування* майбутніх потреб ситуаційних центрів щодо розширення та/чи оновлення їх матеріально-технічної бази, програмного забезпечення, кадрового потенціалу та ін.;
- *діагностики* матеріально-економічного забезпечення ситуаційних центрів щодо їх відповідності сучасному технологічному рівню та спроможності забезпечити потреби фахівців центру в процесі здійснення ними завдань;
- *моделювання* ситуацій та потреб ситуаційних центрів залежно від зміни вихідних умов та можливого впливу ризик-факторів на їх спроможність у виконанні покладених на них функцій.

Успішність економічного механізму реалізації мережевого управління у діяльності органів державної влади визначається його адаптивністю та стійкістю до сприйняття впливу факторів, що формують спроможність та змінюють умови функціонування ситуаційних центрів.

Ключовими факторами впливу, які варто враховувати при формуванні економічного механізму реалізації мережевого управління у діяльності органів державної влади, нами визначено фактори внутрішнього та фактори зовнішнього середовища (див. рис. 3.1).

Факторами внутрішнього середовища можуть стати: організаційна спроможність ситуаційних центрів, що характеризується рівнем їх самодостатності у прийнятті рішень, який передбачено відповідно до визначених для них повноважень; якість кадрового забезпечення ситуаційних центрів, яка залежить від спроможності наявних трудових ресурсів виконувати покладені на них функції та повноваження; спроможність до диверсифікації джерел фінансування, що передбачає можливості залучення

органами державної влади додатково до бюджетних коштів також донорської допомоги для оперативного забезпечення ресурсних потреб ситуаційних центрів.

Факторами зовнішнього середовища, які мають вплив на формування економічного механізму реалізації мережевого управління у діяльності органів державної влади, на нашу думку, можуть стати: світові соціально-економічні та технологічні тенденції, зміна та динаміка яких зумовлює потребу в оновленні матеріально-технічної бази ситуаційних центрів; політична ситуація та пріоритети державної політики, що визначають перспективні напрями використання коштів державного бюджету та зміну пропорцій обсягів бюджетного фінансування, що спрямовуються на забезпечення потреб ситуаційних центрів; взаємодія з міжнародними стейкхолдерами, які своєю діяльністю здатні суттєво змінити як потреби ситуаційних центрів, та і їх ресурсні можливості.

Завершальним та невід’ємним етапом у формуванні економічного механізму реалізації мережевого управління у діяльності органів державної влади є *оцінювання його ефективності* (див. рис. 3.1). Така діяльність дозволяє не лише визначити результати функціонування ситуаційних центрів у відповідності до їх економічного забезпечення, але і запропонувати потенційно необхідні заходи щодо удосконалення їх діяльності з огляду на отримані результати. Окрім того, оцінювання ефективності діяльності ситуаційних центрів є невід’ємним елементом, що передбачається при здійсненні програмно-цільового планування державного бюджету, що базується на визначенні показників ефективності використання бюджетних коштів. Тому, на нашу думку, оцінювання діяльності ситуаційних центрів повинно здійснюватися на основі аналізу результатів їх діяльності, а також наслідків.

Результати діяльності ситуаційних центрів органів державної влади можуть бути визначені як перелік продуктів та послуг, що створюються ними в процесі виконання їх функцій, а також можуть вимірюватись у досягненні

цілей їх діяльності. Це, зокрема, втілюється у розроблених програмах з аналізу даних, відстеження ситуацій, організованих інформаційно-комунікаційних мережах та системах, налагоджених нових процесах та алгоритмах прийняття рішень, що відображають досягнення організаційних цілей. Натомість, *наслідки діяльності ситуаційних центрів* відображаються у їх зовнішньому впливові на оточуюче середовище, зокрема на стейкхолдерів державної політики, які впливають на органи державної влади, громадян країни, іноземних партнерів та глобальне середовище. Зокрема, серед позитивних наслідків діяльності ситуаційних центрів можуть бути стабільний розвиток країни, що забезпечується ефективною протидією ризикам та загрозам, що виникають в оточуючому середовищі. Водночас, кризові ситуації в країні, активність терористичних угруповань на території країни чи масштабні неконтрольовані руйнування на території країни внаслідок надзвичайних ситуацій можуть стати проявом негативних наслідків діяльності ситуаційних центрів.

Більш глибоке дослідження економічного механізму реалізації мережевого управління у діяльності органів державної влади дозволяє зробити висновок проте, що ключовим елементом у його формуванні є налагодження власної інституційної *моделі процесу ресурсування ситуаційних центрів*. Така модель передбачає виявлення ресурсних потреб ситуаційного центру, аналіз доступних джерел їх забезпечення та побудову відповідної системи ресурсного забезпечення, структура якої дозволяла б забезпечити успішне виконання завдань ситуаційного центру у відповідності до цілей державної політики, що реалізується відповідним органом влади. Процес формування інституційної моделі процесу ресурсування ситуаційного центру органу державної влади, на нашу думку, повинен розпочинатися зі збору та аналізу інформації щодо потреб та ресурсів, необхідних для їх забезпечення (див. рис. 3.2.).

При цьому, потреби ситуаційного центру можуть визначатися як поточними та регулярними функціями та завданням, виконання яких

покладається на нього, так заходами, що будуть здійснюватися у випадку складно передбачуваних надзвичайних ситуацій.

Тому аналітичні можливості ситуаційного центру повинні також передбачати можливості прогнозування їх діяльності у оперативній, середньостроковій та довгостроковій перспективі. Це дозволить врахувати можливі надзвичайні потреби та передбачити необхідний резерв ресурсів для їх врегулювання.

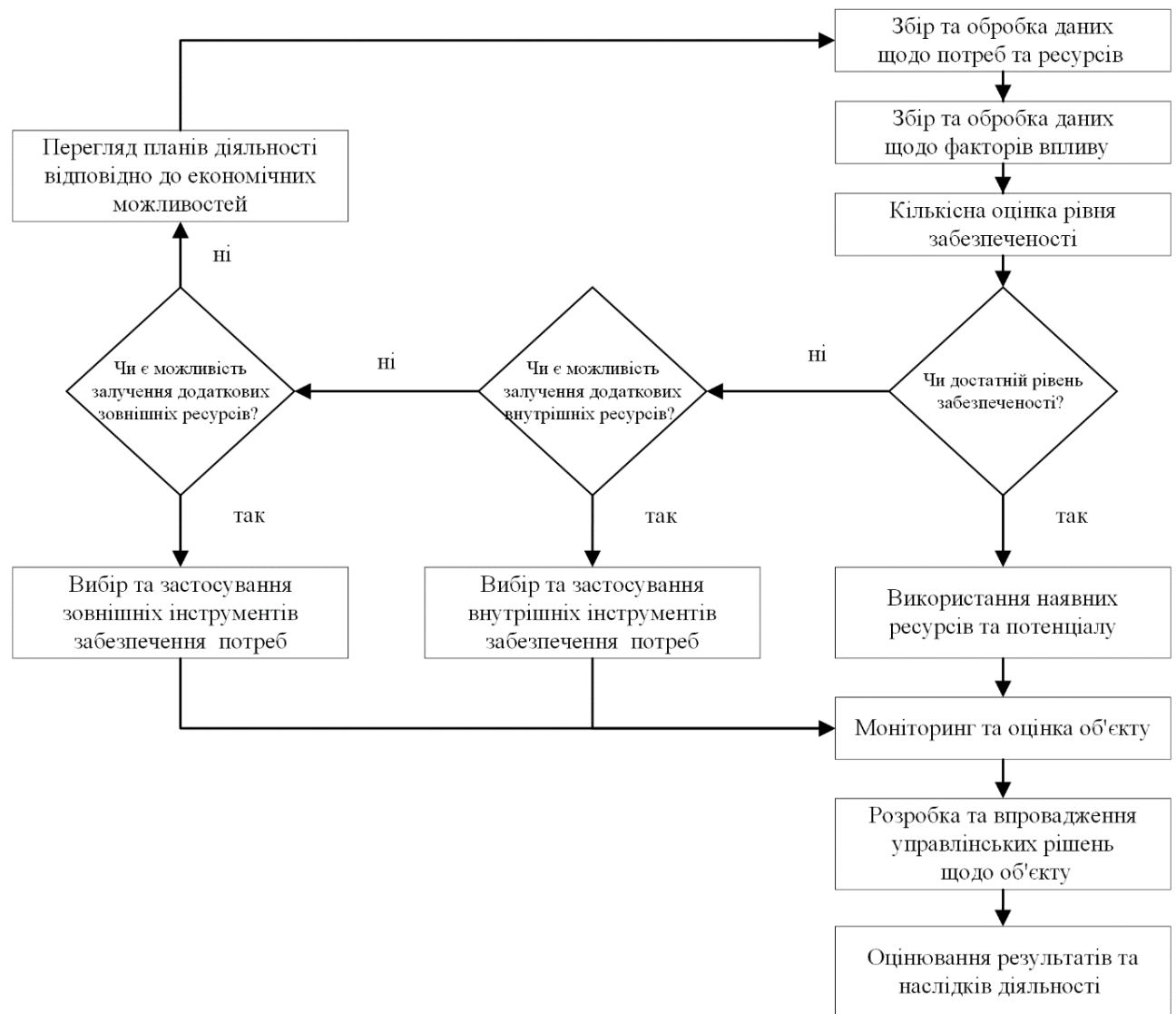


Рис. 3.3. Модель процесу ресурсування ситуаційного центру органу державної влади

Джерело: розроблено автором.

Наступним кроком в процесі ресурсування ситуаційного центру має стати збір та обробка даних щодо факторів зовнішнього та внутрішнього середовища, що мають вплив у поточному періоді та можуть змінювати потреби центру у майбутніх періодах. Водночас, варто враховувати їх вплив як з точки зору потреб, так і з точки зору доступності окремих видів ресурсів та їх структури. Зокрема, кризи суспільно-політичного характеру, безпекового, техногенного, фінансово-економічного, пандемії та інші зовнішні виклики з одного боку, обмежують можливості ресурсування ситуаційних центрів як з внутрішніх, так і зовнішніх джерел, а з іншого боку, – збільшують потребу у розширенні їх діяльності задля подальшого запобігання їх негативним наслідкам.

Результатом вивчення обсягів доступних ресурсів у співставленні з визначеними потребами із урахуванням потенційних впливових факторів має стати детальна кількісна оцінка рівня забезпеченості у доступних для ситуаційного центру ресурсах. На її підставі приймається рішення щодо параметрів та напрямів використання наявного ресурсного потенціалу, чи, у випадку необхідності, пошук додаткових внутрішніх та/чи зовнішніх джерел ресурсів. У випадку їх наявності, доступності та достатності приймається рішення щодо їх структури та напрямів використання в рамках виконання завдань та функцій ситуаційного центру у поточному та прогнозних періодах. Натомість, у випадку браку доступних для ситуаційного ресурсів, існує потреба в перегляді потреб, їх ранжування за пріоритетами та узгодження термінів їх задоволення з можливими періодами залучення додаткових ресурсів.

Після завершення формування структури ресурсів та джерел їх залучення, яка б задовольняла потреби ситуаційного центру, подальшими кроками можуть стати їх використання для здійснення функцій щодо об'єкту мережевого управління, на який спрямована діяльність центру. Зокрема, залучені ресурси використовуються на здійснення моніторингу та оцінки об'єкту мережевого управління, розробку та впровадження управлінських

рішень щодо об'єкту, а також оцінювання результатів та наслідків діяльності ситуаційного центру.

3.2 Удосконалення інформаційно-комунікативних механізмів реалізації мережевого управління

В розбудові інформаційно-комунікаційний механізмів мережевого управління в першу чергу варто визначити поняття впливу та протидії. Комунікативний вплив – це процес інформаційного впливу одного джерела інформації (людини або групи людей, структури, організації) на інших, з використанням засобів комунікації. Цей процес може бути здійснений різними способами, такими як мовлення, міміка, жест, тон голосу, а також використання мовних засобів, таких як аргументація, переконання, підкреслення тощо. Комунікативний вплив може мати різноманітні цілі, такі як зміна поведінки, переконань, думок або емоцій цільової аудиторії. Ключовим елементом комунікативного впливу є взаємодія між відправником повідомлення і отримувачем, яка сприяє процесу передачі інформації та взаєморозумінню між сторонами. Натомість комунікативна протидія – це процес, спрямований на запобігання або зменшення впливу комунікативного впливу на особу або групу людей. Комунікативна протидія може використовуватися для захисту від небажаних впливів, таких як маніпулювання, дезінформування, перекручення фактів та інші форми комунікативної агресії. Цей процес може бути здійснений різними способами, такими як використання логічного мислення, критичного аналізу, спостереження, аналіз поведінки тощо. Ключовим елементом комунікативної протидії є здатність розпізнавати та розуміти різні форми комунікативного впливу та ефективні методи їх протидії. Комунікативна протидія може бути корисною для підвищення свідомості та захисту від негативного впливу комунікативних технологій. Оскільки комунікативний вплив та протидія

засновані на використанні мовних засобів, конструктивні та деструктивні факторам відбувається в певному мовному просторі.

Для визначення інформаційно-комунікативних механізмів реалізації мережевого управління в умовах збройної агресії проти України в першу чергу варто розглянути основні інструменти деструктивного впливу на діяльність органів державної влади з метою здійснення відповідних заходів протидії.

Одним з проявів військової агресії РФ проти України є інформаційна війна складовою якої є інформаційні психологічні операції. Інформаційна війна, на відміну від кібервійни, ціллю якої є комп'ютери, програмне забезпечення та системи керування, передбачає використання та управління інформаційно-комунікативними технологіями у бойовому просторі для досягнення конкурентної переваги над супротивником. Інформаційна війна – це маніпулювання інформацією, якій довіряє ціль, без її відома, щоб ціль приймала рішення проти своїх інтересів, але в інтересах того, хто веде інформаційну війну [173]. Інформаційна війна, крім іншого, може включати поширення пропаганди або дезінформації з метою деморалізації або маніпулювання громадськістю, підриву якості інформації протиборчих сил і відмову протилежним силам у можливості збору інформації [143]. Більш широким розумінням «інформаційної війна», на рівні її ведення як з позиції планування та організації інформаційних операцій, так і з сторони побудови та реалізації інформаційної оборони є набір факторів, який, пов'язаний з використанням інформаційних технологій, які зосереджується на аспектах, пов'язаних з використанням інформації, включаючи (серед багатьох інших) аналіз соціальних мереж, аналіз рішень, і людські аспекти командування та контролю. Інформаційна війна описується як «використання інформації для досягнення наших національних цілей» [205]. Інформаційна війна це операція, яка проводиться з метою отримання інформаційної переваги над супротивником [176] та, в залежності від типу інформаційного поля й механізму впливу, може приймати різні форми [156].

В результаті інформаційних операцій в рамках інформаційної війни основні форми комунікації можуть бути спотворені з використанням інформаційних каналів, які в своїх комунікаціях використовують радіо, інтернет, включаючи месенджери та соцмережі та викрадення цих каналів для кампаній дезінформації. Крім того, можливі відключення або підроблення комунікативних мереж, зокрема соціальних онлайн-спільнот. Організоване використання соціальних медіа та інших платформ для створення онлайн-контенту може бути використано для маніпулювання громадською думкою та формування негативних стереотипів щодо національних інтересів України. Комунікаційний менеджмент та використання синтетичних носіїв також можуть вплинути на сприйняття громадськістю інформації [156].

Організаційною основою як проведення інформаційної війни, так і вибудовування інформаційної оборони є інформаційно-психологічні операції (ІПСО, англ. – Psychological Operations, PSYOP) – це планована та організована діяльність, яка включає в себе опрацювання інформації з метою отримання психологічної переваги в конкретній ситуації. Ця діяльність може бути використана для розв'язання різних завдань, включаючи соціальні, політичні, комерційні та інші. Основною метою інформаційно-психологічної операції є вплив на думки, переконання, почуття та поведінку людей. Метою інформаційно-психологічних операцій є спонукання або зміцнення поведінки, яка сприймається як сприятлива для цілей деструктивного впливу, так і для захисту від нього. Такі операції застосовуються як у мирний час, так і під час військових конфліктів. Розрізняють чотири основних види ІПСО: стратегічний, оперативний, тактичний та консолідуючий [5].

Стратегічні ІПСО проводяться на глобальній або регіональній основі на підтримку цілей і завдань країни та може приймати різні форми, щоб підвищити ефективність у досягненні мети. Плануються переважно поза ареною військових дій.

Оперативні ІПСО проводяться в певній географічній зоні з метою підтримки ефективності командування театру військових дій, кампаній та стратегій театру, або супроводжувати такі дії, через сучасні комунікаційні механізми. Ці операції спрямовані на підвищення рівня бойової здатності та ефективність виконання конкретних завдань в кризових ситуаціях та відкритих військових діях. Ці операції проводяться «до» та «під час» війни або конфлікту, а також після їх завершення.

Тактичні ІПСО зазвичай проводяться в поєднанні з іншими тактичними операціями проти, або для підтримки протиборчих сил або аудиторії. На цьому рівні такі операції зазвичай призначені для точкових дій та адаптовані на комунікацію в різноманітних медіа-форматах для різних категорій та цільових аудиторій. Деструктивний вплив може бути спрямованим, в тому числі, на активацію процесів невдоволення діяльністю органів державної влади, поєднуючи переконання з реальною погрозою, знижуючи здатність до супротиву та рівень підтримки дій влади.

Консолідаційні ІПСО спрямовані на посилення або консолідацію зусиль як в національному, так і в регіональному масштабі та можуть бути ефективними під час внутрішніх оборонних операцій, а також можуть використовуватися як протидія іншим типам інформаційно-психологічних операцій.

Інформаційно-психологічні операції можуть мати різноманітні завдання у залежності від контексту та мети їх використання в мережевому управлінні. Основними задачами інформаційно-психологічних операцій можуть бути:

- вплив на громадську думку та переконання людей: можуть бути використані для формування, зміни або підтримки думок та переконань у різних цільових аудиторіях;
- вплив на емоції та почуття: можуть використовувати різноманітні емоційні техніки для впливу на почуття та емоції людей;

- вплив на поведінку: можуть бути спрямовані на зміну поведінки людей у певних ситуаціях;
- створення образу: можуть бути використані для створення певного образу або іміджу будь-якої особи;
- роз'яснення та поширення інформації: можуть бути спрямовані на ефективне поширення та роз'яснення інформації в певних цільових аудиторіях;
- вплив на виборчий процес та результати голосування: можуть бути використані для впливу на вибір громадян у політичних виборах;
- підвищення громадської свідомості: можуть бути спрямовані на підвищення соціальної свідомості громадськості про певну проблему чи подію;
- комерційні цілі: можуть бути використані для просування товарів чи послуг, збільшення продажів та просування певного бренду.

Основні інформаційно-комунікативні механізми, які використовуються в мережевому управлінні можуть включати такі методи застосування ІПСО:

- переконання: використання різноманітних аргументів, фактів та доказів для переконання людей у певній думці чи ідеї;
- маніпулювання емоціями: використання різних емоційних технік для виклику певних емоцій у людей і формування їх поведінки;
- створення образу: використання різноманітних способів для створення образу людей, продуктів, послуг чи інших об'єктів;
- ідентифікація зі спільнотою: створення сприятливих умов для ідентифікації людей з певною групою або спільнотою;
- психологічний тиск: використання різних способів для створення психологічного тиску на людей з метою зміни їхньої поведінки;
- контроль за інформацією: використання різних методів для контролю за інформацією, яку отримують люди, що може впливати на їхні думки та переконання;

– соціальна норма: використання соціальної норми як засобу впливу на поведінку людей, зокрема на прийняття рішень.

Такі механізми можуть використовуватися окремо чи в комбінації для досягнення певної мети в мережевих структурах та мати як деструктивні, так і конструктивні цілі та наслідки.

ІПСО в мережевому управлінні можуть використовувати різні засоби для досягнення своєї мети. Основні з них можуть включати:

– засоби масової інформації: використання ЗМІ, таких як телебачення, радіо, газети, журнали та інтернет, для поширення певної інформації серед цільової аудиторії;

– засоби масової комунікації: використання соціальних мереж, таких як Facebook, Twitter, Instagram, LinkedIn тощо, для залучення уваги та впливу на поведінку користувачів;

– рекламні засоби: використання рекламних матеріалів, які можуть бути розміщені в ЗМІ, на вуличних рекламних щитах, в інтернеті та інших місцях для просування певної ідеї або позиції;

– прямий контакт: особистий контакт з людьми, який може бути використаний для переконання, маніпулювання емоціями та інших механізмів впливу;

– візуальні ефекти: використання різних візуальних ефектів, таких як колір, форма, текстура, світло та тінь, для створення певної атмосфери та впливу на психологію людей;

– аудіо ефекти: використання музики, звукових ефектів та інших аудіо елементів для створення певної атмосфери та впливу на психологію людей.

Ці інструменти можуть використовуватися окремо чи в комбінації для підсилення впливу в досягненні поставленого завдання засобами конкретної ІПСО.

ІПСО складні для виявлення, оскільки часто вони мають на меті посилити довіру, викликати певні емоції та змінити поведінку людей без

їхнього відчуття. Однак можна відокремити деякі маркери, як психологічні, мовні, соціальні та технічні, за якими визначається проведення ІПСО:

- нестандартність поведінки аудиторії: якщо певна група людей починає несподівано поводитися або реагувати на певні інформаційні події, то це може бути ознакою того, що вони стали об'єктом ІПСО;

- використання стереотипів: якщо інформаційна кампанія використовує стереотипи, кліше або інші загальновідомі підходи для впливу на цільову аудиторію, то це може бути ознакою ІПСО;

- використання неперевіреної або недостовірної інформації: якщо інформаційна кампанія використовує неперевірену або недостовірну інформацію, то це може бути ознакою ІПСО;

- використання загострених тем: якщо інформаційна кампанія використовує загострені теми, такі як національна безпека, тероризм, економічна криза, то це може бути ознакою ІПСО;

- використання мовних засобів для виклику емоцій: якщо інформаційна кампанія використовує мовні засоби, які мають на меті викликати емоційну реакцію у аудиторії, то це може бути ознакою ІПСО. Наприклад, використання заголовків новин, які містять зайвий емоційний заряд або експресивну лексику, можуть викликати в аудиторії певні емоції та змусити їх реагувати на інформацію зі збільшеним інтересом;

- використання соціальної інженерії: ІПСО можуть використовувати соціальну інженерію, особливо з використанням онлайн-платформ для поширення недостовірної або вигаданої інформації. Це може включати використання ботів, фейкових профілів або інших методів для створення штучного попиту на певну інформацію або створення віртуальної громадської думки;

- використання спеціальних технічних засобів: ІПСО можуть використовувати спеціальні технічні засоби для підвищення ефективності впливу на аудиторію. Наприклад, використання підзвучування або

підсвічування певних фрагментів відео або аудіо може мати психологічний вплив на людей без їхнього відчуття;

- використання стереотипів та узагальнень: ІПСО можуть використовувати стереотипи та узагальнення для поширення своїх ідей. Наприклад, ствердження про те, що «будь-яка влада корумпована», може бути використане для впливу на громадську думку.

- використання перекозучень: ІПСО можуть змінювати значення слів або фактів, щоб впливати на громадську думку. Наприклад, використовується термін «колаборанти» або «сепаратист» для опису протестувальників, що може викликати більше обурення серед громадськості, а ніж використання терміну «протестувальник»;

- використання інтуїтивних аргументів: ІПСО можуть використовувати аргументи, які базуються на емоціях або інтуїції, замість фактів та логіки.

Загалом, ІПСО можуть бути важко виявити в мережевому управлінні, оскільки вони часто маскуються як звичайне поширення інформації.

Первинним у створенні інформаційно-комунікативних механізмів мережевого управління є системний моніторинг, аде лише після нього проводиться аналіз, оцінювання та прогнозування. Моніторинг – це систематичне спостереження, контроль та оцінка певного процесу, явища, події або діяльності з метою отримання актуальної та об'єктивної інформації про їхні зміни та виявлення можливих проблем або небажаних наслідків. Моніторинг може проводитися в різних сферах, таких як екологія, медицина, соціальна діяльність, бізнес-процеси тощо.

Моніторинг інформаційного простору – це систематичний процес збору, аналізу та оцінки інформації, що міститься в Інтернеті та соціальних мережах з метою виявлення трендів, попиту, ставлення користувачів до певної теми або бренду, виявлення негативних відгуків про компанію або продукт, моніторингу конкурентів тощо.

Основна мета моніторингу інформаційного простору полягає в тому, щоб зібрати якомога більше інформації про певну тему або бренд, проаналізувати цю інформацію та отримати корисні висновки для прийняття ефективних рішень в бізнесі або політиці.

Зазвичай для здійснення моніторингу інформаційного простору використовуються спеціалізовані програми та сервіси, що дозволяють зібрати та проаналізувати великі обсяги даних з різних джерел. Також можуть використовуватися методи, наприклад, вручну збирати та аналізувати дані з соціальних мереж та форумів.

Інформаційно-комунікативні механізми реалізації мережевого управління в умовах збройної агресії проти України є, в першу чергу, налагодженою системною протидією проявам інформаційної війни, захист від інформаційно-психологічних операцій шляхом їх прогнозування, моніторингу, аналізу факторів та здійснення упереджувального інформаційного впливу, направленого на знешкодження таких операцій, або максимальне зниження їх наслідків.

3.3 Перспективи використання технологій штучного інтелекту в мережевому управлінні

Сучасні державно-управлінські тенденції свідчать про радикальну трансформацію публічного сектору, що полягає у переході від бюрократичної парадигми, яка ґрунтується на чітких нормах та інструкціях для чиновників, до мережевих моделей управління. Нова концепція мережевого управління спрямована на забезпеченні надання високоякісних публічних послуг та досягненні ефективних результатів. Такий перехід призводить до посилення еволюції ролі державного службовця – від безпосереднього управління людськими ресурсами до координації та оптимізації використання інформаційно-комунікативних ресурсів, що досягається завдяки ефективним інноваційним методам та сервісно-

орієнтованого управління. У цьому контексті розвитком концепцій New Public Management та Good Governance, у поєднанні із сучасними технологіями штучного інтелекту (Artificial intelligence, ШІ) може стати мережеве управління (Network Government). Однак, використання інструментів штучного інтелекту в державному управлінні повинно супроводжуватися адекватним розумінням можливих ризиків, та необхідністю визначення рамок правового регулювання.

Мережеве управління є процесом координації між організаціями, яка характеризується органічною або неформальною соціальною системою, на відміну від бюрократичних структур та формальних відносин між ними [165]. Завдяки мережевій орієнтації отримання знань працівники можуть створювати та використовувати інформацію для збільшення конкурентної переваги завдяки співпраці мобільних та гнучких самокерованих команд, у яких мережеве посередництво робочих процесів забезпечує взаємодію між сферами роботи з різними формами організації [133]. Характерною властивістю мережі, на відміну від усіх інших форм організаційної структури, є те, що в ній не існує чітко виражених центрів і меж [9]. Водночас з іншого боку, мережеве управління містить в собі обмежений, стійкий і структурований набір автономних організацій, що займаються створенням кінцевих продуктів або послуг на підставі неявних та необмежених контрактів для адаптації до зовнішніх обставин, координації та забезпечення обміну [204].

Зазначимо, що питання управління штучним інтелектом, а особливо в державному управлінні є недостатньо розвиненою сферою. Проте, системи та алгоритми штучного інтелекту відіграють визначальну роль у прийнятті управлінських рішень для суспільства, таких, як системи підтримки прийняття рішень, системи контролю. В цифровому суспільстві операції, рішення та вибір, які раніше залишалися за людьми, дедалі більше делегуються алгоритмам ШІ, які можуть давати рекомендації, а в деяких

випадках і вирішувати те, як слід інтерпретувати дані, або що є наслідком/результатом.

Мережеве управління характеризується автономними взаємозалежними суб'єктами, кожен із яких окремо не може вирішувати весь комплекс управлінських задач. Водночас співпраця між суб'єктами відбувається в межах самоконструйованої структури, в рамках якої відбуватимуться взаємодії, що дають змогу комплексно та системно вирішувати складні управлінські проблеми. Зважаючи на вищезначене, мережеве управління – це система комунікативної взаємодії об'єктів системи державного управління.

Мережеве управління сприяє підвищенню рівня ефективності та зменшенню фінансових та часових витрат. Рівень ефективності мережевого управління підвищується за рахунок розподіленого доступу та оптимальному опрацюванню інформації, а також завдяки децентралізованій побудові вирішення управлінських проблем та формуванню колективних рішень у різних саморегульованих секторах діяльності органів державної влади. Проте, у сучасних умовах високої розпорошеності значних об'ємів інформації, яка необхідна для прийняття державно-управлінських рішень, необхідності постійного моніторингу та контролю їхнього виконання, оцінки якості та необхідності внесення коректив у процесі їх реалізації, постає актуальна проблема належного адміністрування даними в мережевій структурі державного управління. Для виконання вищезначених задач у структурі управлінської мережі органам державної влади варто запроваджувати аналітично-цифрові механізми, у якості яких можуть виступати інтелектуальні агенти, що функціонують на основі алгоритмів та технологій штучного інтелекту.

Штучний інтелект має значний потенціал для застосування в різних сферах публічного управління, що дозволяє автоматизувати процеси, покращувати якість управлінських рішень та забезпечувати більш швидку та ефективну роботу органів державної влади. У системах мережевого

управління алгоритми штучного інтелекту можуть функціонально забезпечувати виконання таких завдань:

1) Аналіз даних та прогнозування (функція аналітики даних): алгоритми штучного інтелекту можуть застосовуватися для аналізу великих даних, виявлення закономірності та тенденції. На основі такого аналізу можна робити прогнози для планування дій органів державної влади. До процесу аналізу даних та прогнозування можна також віднести функцію моніторингу систем за широким набором параметрів та прогнозування зміни розвитку ситуації при коректуванні державно-управлінських рішень.

2) Підтримка прийняття рішень (функція асистента): алгоритми штучного інтелекту можуть надавати рекомендації щодо прийняття рішень на основі вхідних даних, моніторингу поточної ситуації та базуючись на обраній стратегії управління, у тому числі для оптимізації розподілу бюджетних ресурсів та плануванні фінансових видатків.

3) Оптимізація процесів адміністрування (функція оптимізації): для забезпечення високої продуктивності та ефективності діяльності органів державної влади алгоритми штучного інтелекту можуть оптимізувати робочі процеси урядових установ, управління завданнями та розподілом обов'язків, а також виявляти можливості реінжинірингу таких процесів.

4) Обробка запитів та звернень громадян (комунікативно-інформаційна функція): алгоритми штучного інтелекту на основі інтелектуальних агентів (ботів) можуть автоматизувати обробку та аналіз звернень громадян, що дозволить забезпечити швидку та точну відповідь на поточні питання користувачів, надання інформації та вирішення запитів. Також може бути реалізована функція консультативної підтримки та допомоги користувачеві за попередньо визначеним переліком базових питань через обробку та реагування на звернення користувачів, які спрямовані на пошук алгоритмів вирішення проблем або запитів, надання користувачеві персоналізованих рекомендацій на основі визначених вподобань, які базуються на досвіді попередньої взаємодії з інтелектуальним агентом.

Окремо варто відзначити здатність алгоритмів ШІ розпізнавати та аналізувати природну мову користувача, що має покращити розуміння запитів та підвищити точність відповідей, які надаються з використанням інтелектуальних агентів.

5) Цифрова безпека, кіберзахист та боротьба із корупцією (функція ШІ, кібербезпеки та протидії корупції): ШІ може виявляти потенційні загрози та вразливості в цифрових системах органів державної влади та забезпечувати кіберзахист, а також, на основі аналізу даних та управлінських рішень, виявляти ознаки корупції.

6) Моделювання та прогнозування ризиків (функція ризик-менеджменту) з використанням штучного інтелекту в органах державної влади полягає у використанні цифрових інтелектуальних алгоритмів та технологій штучного інтелекту для аналізу великих даних, ідентифікації потенційних ризиків та їх впливу на різні сфери, що дозволяє ефективно прогнозувати можливі загрози, розробляти стратегії та приймати обґрунтовані рішення для зменшення ризиків та покращення управлінської ефективності, сприяючи оптимізації процесів та забезпеченню сталого розвитку.

7) Електронний документообіг та логістика даних (функція дата-менеджменту): алгоритми штучного інтелекту можуть автоматизувати обробку та аналіз великого обсягу документів, що дасть змогу ефективніше керувати документообігом та потоками інформації, виявляти важливі дані, класифікувати документи за категоріями, автоматично розподіляти завдання, оптимізувати їх зберігання, доступність та безпеку, що має забезпечити надійну та ефективну роботу органів державної влади у сфері документообігу та прискорити процеси прийняття управлінських рішень.

Проте, повсюдне використання штучного інтелекту в системах мережевого управління в процесі прийняття рішень органами державної влади, може спричиняти виникнення таких базових ризиків:

1) Недостатність прозорості та відповідальності: часто алгоритми штучного інтелекту є занадто складними в розумінні та відслідковуванні, що знижує рівень прозорості та унеможливорює відповідальність за прийняті рішення в разі негативних наслідків, а особливо у сфері життєдіяльності людини. Наслідком цього є також ризик втрати контролю, коли алгоритм прийняття рішень може контролюватися сторонніми суб'єктами, дотичними до створення такого алгоритму.

2) Ризик спотворення та дискримінації в прийнятті рішень полягає в тому, що моделі штучного інтелекту зазнають системних спотворень в аналізі та прийнятті рішень, які виникають через неправильне або некоректне моделювання алгоритмами штучного інтелекту, у тому числі через упередження або дискримінацію, які існують у вихідних даних.

3) Конфіденційність та безпека даних: Використання штучного інтелекту вимагає великих обсягів даних, що підвищує ризик порушення конфіденційності та безпеки особистих даних.

4) Ризик «байєсівської пастки» в контексті статистики та прийняття рішень на основі «байєсівського» підходу, коли при оцінці подій або ризиків недостатньо враховуються або занадто сильно підкреслюються апріорні ймовірності, які впливають на якість рішення або оцінки, а нова інформація не може вплинути на її зміну.

Для успішного впровадження ШІ у сфері мережевого управління варто враховувати наведені ризики та вживати заходи для їхньої мінімізації, зокрема враховуючи те, що основи рішень штучного інтелекту часто непрозорі й можуть бути неприйнятними або неможливими для сприйняття людиною. У такому випадку для підвищення прозорості алгоритмів та рішень варто застосовувати моделі інтерпретованого (поясненого) штучного інтелекту.

Інтерпретований штучний інтелект (Explainable artificial intelligence, XAI) – це підхід до розробки алгоритмів (моделей) штучного інтелекту, який сприяє зрозумілості та забезпечує можливість пояснення прийнятих ним

рішень. Це набір процесів і методів, які дають змогу користувачам розуміти та довіряти рішенням та результатам, створеним алгоритмами машинного навчання. Метою ХАІ є створення моделей та алгоритмів штучного інтелекту, функцією яких є не лише ефективне вирішення завдань, але й відображення логіки та механізмів, як самого прийняття рішень, так і алгоритму, за якими працює обрана модель. Це важливо для забезпечення прозорості, відповідності етичним нормам та можливості перевірки прийнятих рішень, особливо в галузях, де системи штучного інтелекту взаємодіють із людьми, враховуючи їх потреби та очікування. Алгоритми ХАІ мають дотримуватися трьох основних принципів: транспарентності, інтерпретованості та пояснюваності.

Перепонами на шляху повсюдного застосування алгоритмів штучного інтелекту є брак єдиних прозорих стандартів і регулювань, що може призвести до розходження в підходах до прозорості та відповідальності. Вирішенням цього питання є впровадження чіткого правового регулювання питань використання алгоритмів штучного інтелекту в органах державної влади. Таке регулювання має містити етичні норми і правила використання штучного інтелекту, всебічно враховувати виклики та ризики, ставити на меті досягнення єдиних стандартизованих вимог до його використання у тому числі й у системах мережевого управління.

Так, для сприяння розвитку штучного інтелекту та вирішення потенційних високих ризиків, які він створює для безпеки та основних прав, Європейською Комісією було запропоновано проєкт нормативно-правової бази щодо штучного інтелекту, який спрямований на вирішення ризиків, пов'язаних із використанням ШІ, класифікуючи їх на 4 різні рівні: неприйнятний ризик, високий ризик, обмежений ризик і мінімальний ризик. Згідно з цим проєктом, нормативно правова база має на меті досягнення таких цілей [191]:

- забезпечити безпечність системи ШІ, які використовуються у відповідності чинному законодавству про основні права та цінності Європейського Союзу;
- забезпечити юридичну визначеність для сприяння інвестиціям та інноваціям алгоритмів ШІ;
- покращити управління та ефективне забезпечення виконання чинного законодавства про основні права та вимоги безпеки, що застосовуються до систем ШІ;
- сприяти розвитку єдиного ринку для законних, безпечних і надійних програм ШІ та запобігати фрагментації ринку.

Нині в Україні прийнята «Дорожня карта з регулювання штучного інтелекту» [19], яка є покроковим шляхом до ухвалення національного законодавства про штучний інтелект, який відповідає засадам AI Act ЄС та є елементом інтеграції сучасного законодавства України до норм і правил Європейського Союзу, та, у тому числі, передбачає долучення до методології HUDERIA (Human Rights, Democracy, and the Rule of Law Impact Assessment) та адаптацію її в Україні. Методологія HUDERIA, серед іншого, передбачає створення єдиного підходу для виявлення, аналізу, оцінки ризиків та впливу систем ШІ на права людини, демократію та верховенство права, зокрема [158]: ідентифікації ризику систем ШІ, оцінку впливу, оцінка управління та уникнення негативного впливу та оцінку систем ШІ.

Проте, наведені регулюючі ініціативи, попри глибокий рівень оцінки ризиків впровадження систем штучного інтелекту та системність підходу в глобальній стандартизації ШІ, мають враховувати специфіку у сфері мережевого управління, а також динаміку технологічного розвитку, яка вимагає використання прогностичного підходу до нормотворення, що базується на аналізі можливостей регулювання технологій майбутнього.

На підставі проведеного дослідження можна зробити загальний висновок, що зважаючи на ефективність використання алгоритмів штучного інтелекту в мережевому управлінні, зокрема завдяки розподіленому доступу,

децентралізованому вирішенню управлінських питань та формуванню колективних рішень, враховуючи необхідність постійного моніторингу їх виконання, оцінки якості та потреби внесення коректив у процесі їх реалізації, а також широкому переліку задач та функцій, які може виконувати ШІ в таких системах (функції аналітики даних, асистента, оптимізації, кібербезпеки та протидії корупції, ризик- та дата-менеджменту, а також комунікативно-інформаційна функція) та з огляду на ризики за умови застосовування моделі інтерпретованого штучного інтелекту та прийняття відповідної нормативно-правової бази щодо штучного інтелекту, яка спрямована на вирішення ризиків, пов'язаних із використанням штучного інтелекту, використання інструментів штучного інтелекту, як механізмів мережевого управління в галузі публічного управління та адміністрування, дасть змогу автоматизувати процеси, покращити якість управлінських рішень та забезпечити більш швидку та ефективну роботу органів публічної влади.

Висновки до розділу 3

Показано, що узгодження джерел ресурсування ситуаційних центрів з методами їх використання відповідно до визначених цілей їх функціонування, а також формування необхідної та достатньої матеріально-ресурсної бази, передбачає забезпечення розвитку економічного механізму реалізації мережевого управління у діяльності органів державної влади.

На основі аналізу наукових підходів щодо змісту категорії «економічний механізм» дано авторське формулювання суті *економічного механізму реалізації мережевого управління у діяльності органів державної влади*, як такого, що реалізується через функціонування системи ситуаційних центрів, передбачає узгодження процесів визначення їх потреб, акумулювання та використання необхідних ресурсів (фінансових, матеріальних, людських, технологічних та ін.), а також оцінювання результатів їх роботи, що втілюються у створених ними продуктах (послуги,

роботи) та суспільних ефектах, що вони спричиняють, відповідно до визначених цілей та принципів.

Обґрунтовано складові елементи розвитку економічного механізму реалізації мережевого управління у діяльності органів державної влади, якими є забезпечувальна та функціональна підсистеми ситуаційних центрів, що формуються відповідно до визначених цілей (забезпечення матеріально-технічної бази, збалансоване використання ресурсів, підготовка та мотивація персоналу, взаємодія зі стейкхолдерами) та принципів (мобільність, стратегічність, взаємодія, раціональність, підзвітність, контроль, наукова обґрунтованість, інноваційність), з урахування впливових факторів зовнішнього та внутрішнього середовища та передбачає систематичне оцінювання на основі результатів та наслідків діяльності.

З метою удосконалення механізмів бюджетування в реалізації мережевого управління надано рекомендацію щодо запровадження спеціальних бюджетних програм для органів державної влади – головних розпорядників бюджетних коштів, які відображали б узгодження бюджетних коштів, що виділяються на фінансування діяльності ситуаційних центрів, з цілями державної політики та результатами їх досягнення. Типовою назвою таких бюджетних програм може стати *«Забезпечення функціонування ситуаційного центру ... (назва органу державної влади)»*. При цьому, самі ситуаційні центри можуть стати виконавцями таких бюджетних програм, формувати перелік напрямів спрямування бюджетних коштів за погодженням з їх керівним органом державної влади та звітувати про їх використання відповідно до визначених показників оцінювання бюджетної програми.

Обґрунтовано алгоритм формування *моделі процесу ресурсування ситуаційних центрів*, яка передбачає виявлення ресурсних потреб ситуаційного центру, аналіз доступних джерел їх забезпечення та побудову відповідної системи ресурсного забезпечення, структура якої дозволяла б забезпечити успішне виконання завдань ситуаційного центру у відповідності

до цілей державної політики, що реалізується відповідними органами державної влади.

Встановлено, що основні інформаційно-комунікативні механізми, які використовуються для впливу на суб'єктів мережевого управління, зокрема державних службовців, можуть включати такі методи застосування інформаційно-психологічних операцій: переконання; маніпулювання емоціями; створення образу; ідентифікація причетності до певних спільнот; психологічний тиск; контроль за інформацією; спотворення соціальних норм. Визначено, що інформаційно-психологічні операції в мережевому управлінні можуть реалізовувати різні засоби для досягнення своєї мети, а саме: засоби масової інформації; засоби масової комунікації; рекламні засоби; безпосередній контакт; візуальні ефекти; звукові ефекти.

Визначено, що інформаційно-комунікативні механізми реалізації мережевого управління в умовах збройної агресії проти України можуть стати дієвою системною протидією проявам інформаційної війни шляхом застосування захисту від інформаційно-психологічних операцій, завдяки своєчасному здійсненню моніторингу, аналізу, оцінюванню та прогнозування факторів, які впливають (або можуть впливати) на їх вироблення, а також застосуванню інформаційного впливу, спрямованого на поширення, упередження, знешкодження, або максимальне зниження наслідків таких операцій.

Для виявлення інформаційно-психологічних операцій у мережевому управлінні визначено маркери, які характеризують їх ознаки, а саме це використання: соціально-загострених тем; нестандартної поведінки цільової аудиторії; інтуїтивних аргументів; стереотипів, узагальнень та кліше; дезінформації; спеціальних мовних конструкцій та експресивної лексики для виклику зайвих емоцій; соціальної інженерії (боти, фейкові профілі, штучні рейтинги та опитування в соціальних мережах); спеціальних технічних засобів («озвучення» або «підсвічування» певних фрагментів відео або аудіо).

Доведено, що рівень ефективності мережевого управління підвищується за рахунок розподіленого доступу та оптимальному опрацюванню інформації, а також завдяки децентралізованій побудові вирішення управлінських проблем та формуванню колективних рішень у різних саморегульованих секторах діяльності органів державної влади. Проте, у сучасних умовах високої розпорошеності значних об'ємів інформації, яка необхідна для прийняття державно-управлінських рішень, необхідності постійного моніторингу та контролю їхнього виконання, оцінки якості та необхідності внесення коректив у процесі їх реалізації, постає актуальна проблема належного адміністрування даними в мережевій структурі державного управління. Для виконання вищезазначених задач у структурі управлінської мережі органам державної влади варто запроваджувати аналітично-цифрові механізми, у якості яких можуть виступати інтелектуальні агенти, що функціонують на основі алгоритмів та технологій штучного інтелекту.

Проаналізовано проблематику розвитку мережевого управління з урахуванням перспектив застосування комплексу алгоритмів штучного інтелекту як системи комунікативної взаємодії суб'єктів управління. Описано шляхи підвищення ефективності мережевого управління в саморегульованих секторах діяльності за рахунок розподіленого доступу й децентралізованого підходу до вирішення управлінських питань та колективних рішень.

Визначено основні задачі та функції алгоритмів штучного інтелекту в системах мережевого управління, а саме: аналіз даних та прогнозування, підтримка прийняття рішень, оптимізація процесів управління, обробка запитів та звернень громадян, цифрова безпека, кіберзахист та боротьба з корупцією, моделювання та прогнозування ризиків, електронний документообіг та логістика даних. Проаналізовано базові ризики, що виникають при масовому використанні штучного інтелекту в системах мережевого управління в процесі прийняття рішень в органах державної влади, зокрема: недостатність прозорості та відповідальності, дискримінація

у прийнятті рішень, конфіденційність та безпека даних, ризик «байєсівської пастки».

Доведено, що вирішення проблеми непрозорості алгоритмів штучного інтелекту в мережевому управлінні лежить у площині використання моделі інтерпретованого штучного інтелекту. Констатовано, що брак єдиних прозорих стандартів і регулювань є перешкодою на шляху повсюдного застосування алгоритмів штучного інтелекту. Запропоновано при розробці законів та підзаконних актів враховувати специфіку мережевого управління та використання прогностичного підходу до нормотворення.

Основні результати розділу 3 опубліковано в наукових працях автора:
[52; 105; 118]

ВИСНОВКИ

У дисертаційній роботі вирішено нове наукове завдання, яке полягає у здійсненні теоретичного обґрунтування механізмів реалізації мережевого управління у діяльності органів державної влади та наданні практичних рекомендацій щодо їх удосконалення шляхом застосування інформаційно-комунікативних технологій. У результаті проведеної роботи досягнута її мета та розв'язані поставлені завдання, що дозволяє зробити такі загальні висновки.

1. Розкрито сутність існуючих наукових розробок щодо застосування технологій мережевої організації у державному управлінні, яка розглядається як один із результативних шляхів сприяння взаємодії між різними органами влади та стейкхолдерами/беніфіцарами задля підвищення рівня прозорості, відповідальності, якості та ефективності їхньої діяльності. Констатовано, що застосування технологій мережевої організації у державному управлінні дозволяє публічним службовцям краще адаптуватися до економічних, політичних та соціокультурних змін. У глобальному контексті мережева організація діяльності може сприяти співпраці між різними країнами та міжнародними організаціями для вирішення глобальних проблем, таких як зміна клімату, боротьба з пандемією, міграція та інші. Систематизовано еволюційні періоди розвитку типів організаційних мереж, вважаючи їх початком лінійні, затим функціональні та лінійно-функціональні мережі, згодом – дивізіональні та матричні. Обґрунтовано, що на сучасному етапі відбувається новий період суспільного розвитку в умовах глобалізації та стрімко формується нова організаційна структура управління – мережева, розвиток якої став можливим завдяки зростанню інформаційно-комунікативних та цифрових зв'язків між органами державної влади, приватними компаніями та громадянами.

2. Визначено генезу правового формування механізмів реалізації мережевого управління у діяльності органів державної влади на основі

аналізу законів та підзаконних актів України, яка ґрунтується на історико-правовому підході та має власну періодизацію. Виокремлено 4 етапи правового формування механізмів мережевого управління у діяльності органів державної влади, зокрема: перший етап (1973 – 1996 рр.); другий етап (1998 – 2003 рр.); третій етап (2004 – 2015 рр.) та четвертий – (2016 р. – до тепер), які врегульовують суспільні відносини в інформаційній сфері та цифровізації, вироблення державної політики щодо взаємодії органів державної влади та інститутів громадянського суспільства, формування національного сегменту інтернет мережі та застосування цифрових технологій, право на інформацію та реалізацію участі громадськості в державних справах, інструменти оприлюднення та поширення інформації про діяльність органів державної влади, розвиток громадянського суспільства, а також встановлення обмежень в інформаційній сфері у зв'язку із введенням воєнного стану в Україні.

3. Узагальнено зарубіжний досвід використання органами державної влади ситуаційних центрів як інституцій мережевого управління, діяльність яких спрямована на забезпечення національних інтересів країни та/чи безпеки міжнародної діяльності шляхом оперативного реагування на кризові виклики, ефективного прийняття рішень в сфері управління динамічними ситуаціями на основі виявлення та всебічного аналізу інформації щодо їх змін, а також прогнозування їх подальшого розвитку. В результаті чого визначено основні засади діяльності ситуаційних центрів міжнародних міжурядових організаціях та об'єднаннях на прикладі ситуаційних центрів SITCEN NATO, SANER, ISAC, NCI, а також мережевих платформ HCSS StratBase Datalab, Exonaut, MASA Synergy, Effector та центрів реагування на інциденти у сфері кібербезпеки CSIRT, CERT, NCSC-FI, ECCSA в США й окремих країнах ЄС (Швеції, Франції, Литви, Польщі, Португалії, Норвегії, Фінляндії, Нідерландів). Ситуаційні центри є інструментом постійного моніторингу, аналізу та оцінки даних, моделювання ситуацій для прийняття управлінських рішень в кризових ситуаціях, а також осередком здійснення

результативної координації зусиль органів державної влади щодо протидії військовим внутрідержавним чи міждержавним конфліктам, політичним кризам, кіберзагрозам, пандемічним ситуаціям у випадку поширення хвороб, стихійним лихам, техногенним катастрофам терористичним злочинам, загрозам стратегічної інфраструктури (зокрема, енергетичної, сільськогосподарської та ін.). У світовій практиці спостерігається стійка динаміка до розвитку високотехнологічних спроможностей, які дозволяють максимально швидко відстежувати ситуацію, збирати інформацію та допомагати управлінням приймати оперативні рішення, а також, здійснювати моделювання будь-якої проблемної ситуації, прогнозувати її наслідки та передбачати можливі варіанти її розвитку з використанням кількісної та якісної оцінки одержаної інформації.

4. Розроблено процесну модель механізмів реалізації мережевого управління у діяльності органів державної влади, яка складається з мети, принципів функціонування (співпраці та партнерства, спільного прийняття рішень, децентралізації та автономії, горизонтальних та вертикальних зв'язків), факторів (політичної волі, вироблення державної політики, ресурсів та фінансування, розвитку інституційної культури, наявності кваліфікованих кадрів, міжнародних та геополітичних чинників, технологічних можливостей, готовності до змін), суб'єктів та об'єктів впливу (передбачає взаємодію між ними) та тристороннього алгоритму практичних заходів впровадження (*фасилітації* – залучення учасників до процесу для розуміння цілей їхньої участі, планування способів досягнення цих цілей і спільної роботи; *координації* – організації та синхронізації процесу спільної роботи всіх учасників для досягнення загальної мети; *адміністрування* – забезпечення виконання завдань, контролю, просування та підтримки функціонування мереж).

Наслідки практичного застосування моделі здатні призвести до підвищення ефективності роботи органів державної влади через покращення координації та співпраці між ними та стейкхолдерами (беніфіцарами), що

спричинить досягнення необхідних результатів у відповідності до поставлених цілей та потреб громадян; стимулюватиме залучення зацікавлених сторін до процесів державного управління і прийняття рішень; забезпечить розуміння потреб і очікувань громадськості; дозволить органам державної влади ефективно адаптуватися до змін в політичному, економічному та соціокультурному середовищі; сприятиме впровадженню інновацій та креативності в роботі державних службовців.

5. Визначено сутність економічного механізму реалізації мережевого управління у діяльності органів державної влади, як такого, що реалізується через функціонування системи ситуаційних центрів, передбачає узгодження процесів визначення їх потреб, акумулювання та використання необхідних ресурсів (фінансових, матеріальних, людських, технологічних та ін.), а також оцінювання результатів їх роботи, що втілюються у створених ними продуктах (послуги, роботи) та суспільних ефектах, що вони спричиняють, відповідно до визначених цілей та принципів. Обґрунтовано складові елементи розвитку економічного механізму реалізації мережевого управління у діяльності органів державної влади, якими є забезпечувальна та функціональна підсистеми ситуаційних центрів, що формуються відповідно до визначених цілей (забезпечення матеріально-технічної бази, збалансоване використання ресурсів, підготовка та мотивація персоналу, взаємодія зі стейкхолдерами) та принципів (мобільність, стратегічність, взаємодія, раціональність, підзвітність, контроль, наукова обґрунтованість, інноваційність), з урахування впливових факторів зовнішнього та внутрішнього середовища та передбачає систематичне оцінювання на основі результатів та наслідків. Запропоновано алгоритм формування *моделі процесу* ресурсування ситуаційних центрів, яка передбачає виявлення ресурсних потреб ситуаційного центру, аналіз доступних джерел їх забезпечення та побудову відповідної системи ресурсного забезпечення, структура якої дозволяла б забезпечити успішне виконання завдань ситуаційного центру у відповідності до цілей державної політики, що

реалізується відповідними органами державної влади.

6. Надано практичні рекомендації щодо застосування інформаційно-комунікативних технологій удосконалення мережевого управління у діяльності органів державної влади в умовах збройної агресії проти України, а саме:

- унормувати на законодавчому рівні механізми використання соціальних мереж органами державної влади як феномену інформаційного обміну, що дозволить аналізувати процес масової цифрової комунікації, здійснювати прогнозування громадської думки, виявляти приховані можливості маніпулювання й управління суспільною свідомістю, забезпечувати легітимність віртуальної комунікації для врахування висловлених пропозицій, зауважень, ініціатив тощо;

- імплементувати у державне управління адаптивні системи опису факторів та передумов виникнення можливих ситуацій за допомогою імітаційного (динамічного) моделювання, завданням якого має бути визначення вихідних даних, що відображають умови і фактори виникнення інформаційної окупації задля розробки заходів щодо запобігання їх появі у майбутньому (застосування динамічного моделювання ситуацій із використанням вихідних даних та подальшим аналізом ситуацій щодо пропаганди є необхідним для визначення можливих наслідків прийнятих рішень щодо контрпропаганди та їх впливу на суспільну думку);

- застосувати організаційні механізми мережевого управління у якості інструментарію реалізації державної кіберполітики у сфері аналізу й оцінювання даних, а також наявних кіберзагроз для забезпечення взаємодії суб'єктів національної системи захисту критичної інфраструктури, професійного навчання та підвищення кваліфікації державних службовців;

- протидіяти інформаційно-психологічним операціям, які, застосовуючи переконання, маніпулювання емоціями, створення образу, ідентифікація причетності до певних спільнот, психологічний тиск, контроль за інформацією; спотворення соціальних норм, використовуються для впливу

на державних службовців як суб'єктів мережевого управління шляхом своєчасного здійснення моніторингу, аналізу, оцінюванню та прогнозування факторів інформаційної загрози, а також застосуванню контрвпливу, спрямованого на поширення, упередження, знешкодження, або максимальне зниження наслідків таких операцій;

— запровадити аналітико-цифрові механізми адміністрування даними в мережевій структурі державного управління, у якості яких можуть виступати алгоритми та технології штучного інтелекту за рахунок розподіленого доступу й децентралізованого підходу до вирішення державно-управлінських завдань: аналіз даних та прогнозування, підтримка прийняття рішень, оптимізація адміністративних процесів, обробка запитів та звернень громадян, цифрова безпека, кіберзахист та боротьба з корупцією, моделювання та прогнозування ризиків, електронний документообіг та логістика даних тощо);

— стандартизувати технології застосування інтелектуальних агентів у державному секторі з метою вирішення проблеми непрозорості алгоритмів мережевого управління, що лежить у площині використання моделі інтерпретованого штучного інтелекту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бебик В.М. Інформаційно-комунікаційний менеджмент у глобальному суспільстві: психологія, технології, техніка паблік рилейшнз: монографія. Київ: МАУП, 2005. 440 с.
2. Брижака О. Інвестиційний клімат в Україні за ред. П.І. Гайдучького. К.: Нора-друк, 2002. С.77-78.
3. Бюджетний кодекс України. Прийнятий 08.07.2010 р. № 2456-VI. Редакція від 13.09.2023. URL: <https://zakon.rada.gov.ua/laws/show/2456-17#Text> (дата звернення: 15.09.2023)
4. Валага Л.Ю., Бондаренко С.М. Організаційно-економічний механізм управління системою стандартизації України в умовах євроінтеграції. Ефективна економіка. 2016. № 12. URL: <http://www.economy.nayka.com.ua/?op=1&z=5351> (дата звернення: 10.10.2023)
5. Васюк Н., Гаєвська Л. Механізми мережевого управління в діяльності органів публічної влади: сутність понять. *Аспекти публічного управління*. 2023. №11(2), 17-23. URL: <https://doi.org/10.15421/152314> (дата звернення: 15.10.2023)
6. Великий тлумачний словник сучасної мови. URL: <https://slovnyk.me/dict/vts/%D0%B3%D0%B5%D0%BD%D0%B5%D0%B7%D0%B0> (дата звернення: 17.06.2023).
7. Вишневський В.В. Мережа ситуаційних центрів органів державної влади України. Організаційні аспекти. URL: https://niss.gov.ua/sites/default/files/2014-05/0515_prez2.pdf (дата звернення: 15.10.2022)
8. Власюк О.С. Теорія і практика економічної безпеки в системі науки про економіку. К. : Нац. ін-т пробл. міжнар. безпеки при Раді нац. безпеки і оборони України, 2008. 48 с.

9. Войтович Р. Мережеве суспільство як нова форма соціальної організації в умовах глобалізації. *Політичний менеджмент*. 2010. № 5. С. 3–18.

10. Гаєвська Л.А., Васюк Н.О. Механізми протидії дезінформації органами державної влади засобами мережевого управління. *Державне управління: удосконалення та розвиток*. 2023. № 8. URL: <https://nayka.com.ua/index.php/dy/article/view/1968/1989> DOI: <http://doi.org/10.32702/2307-2156.2023.8.5>

11. Галіч Т.О. Соціальні Інтернет-мережі та віртуалізація суспільного життя. *Соціологія майбутнього: наук. журн. з проблем соціології молоді та студентства*. 2010. Вип. 1. С. 145–152.

12. Галуцько А.В. Соціальні інтернет мережі як об'єкт адміністративно-правового регулювання. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2013. № 22. С.127-129.

13. Геологічний словник. URL: <https://geodictionary.com.ua/node/2146> (дата звернення: 17.06.2023).

14. Головний ситуаційний центр України функціонує в штатному режимі. URL: <https://www.rnbo.gov.ua/ua/Diialnist/3278.html> (дата звернення: 15.09.2022)

15. Горбік В. Війна за стандартами НАТО. Як працюють сучасні технології, ситуаційні центри та мережево-центричність на війні в Україні. *Dev Україна*. 2022. URL: <https://dev.ua/news/sytuatsiini-tsentry-ta-merezhe-tsentrychnist> (дата звернення: 15.09.2022)

16. Данько Ю.А. Феномен соціальних мереж у контексті становлення і розвитку мережевого суспільства. *Вісник Міжнародного Слов'янського університету. Серія «Соціологічні науки»*. 2012. Том XV. № 1, 2. С. 55–61.

17. Денисюк Ж.З. Постфольклор інтернет-комунікації в аксіологічному вимірі: монографія. Київ: НАКККиМ 2017. 384 с. URL: <http://academy.gov.ua/infpol/pages/dop/2/files/cc18fb23-8c23-4ebb-9af9-4b560e9c728b.pdf> (дата звернення: 15.10.2023)

18. Динник І. Соціальні мережі як засіб суспільного розвитку. Ефективність державного управління: зб. наук. пр. Львівського регіонального інституту державного управління НАДУ при Президентові України. Вип. 1 (50): у 2 ч. / за заг. ред. чл.-кор. НАН України В.С. Загорського, доц. А.В. Ліпенцева. Львів: ЛРІДУ НАДУ, 2017. С. 64–69. URL: http://www.lvivacademy.com/vidavnitstvo_1/edu_50/fail/9.pdf (дата звернення: 10.01.2023)

19. Дорожня карта з регулювання штучного інтелекту в Україні URL: https://cms.thedigital.gov.ua/storage/uploads/files/page/community/docs/Дорожня_карта_з_регулювання_ШІ_в_Україні_compressed.pdf (дата звернення: 15.01.2023)

20. Енциклопедія державного управління: у 8 т. / Нац. акад. держ. упр. при Президентові України; наук.-ред. колегія: Ю.В. Ковбасюк (голова) та ін. Т. 1. К.: НАДУ, 2011. С. 748.

21. Євсюкова О. В. Формування механізмів управління розвитком сервісної держави в умовах суспільних трансформацій: автореф. дис. ... д-ра наук з держ. упр. : 25.00.02; Нац. акад. держ. упр. при Президентові України. Київ, 2020. 36 с.

22. Женевська Декларація принципів «Побудова інформаційного суспільства: глобальна задача в новому тисячолітті». Асоціація підприємств інформаційних технологій України. 2003. <https://old.apitu.org.ua/wsis/dp> (дата звернення: 23.06.2023).

23. Загальна декларація прав людини: резолюція 217 А (III) Генеральної Асамблеї ООН від 10 грудня 1948 року. UR: https://zakon.rada.gov.ua/laws/show/995_015#Text (дата звернення: 23.06.2023).

24. Запорожець Т., Цимбаленко Я. Безпека інформаційних систем як чинник ефективності мережевого управління. *Аспекти публічного управління*, 2023. №11(3), 25-29. DOI: <https://doi.org/10.15421/152331>

25. Запорожець Т.В. (2023) Генеза урядових мереж Великобританії: від Public Service Network (PSN) до Future Network for Government (FN4G).

Інвестиції: практика та досвід. 2023, № 11. С. 104-107. URL: <https://doi.org/10.32702/2306-6814.2023.21.104>

26. Інформаційний Рамштайн – початок єдиного інформаційного фронту країн-союзників. URL: <https://www.pravda.com.ua/columns/2022/09/30/7369845/> (дата звернення: 10.02.2023)

27. Інформаційно-комунікативна діяльність органів публічної влади : монографія / В.С. Куйбіда, О.В. Карпенко, А.В. Дуда [та ін.] ; за заг. ред. В.С. Куйбіди, О.В. Карпенка. Київ: ЦП «Компрінт». 2018. 364 с.

28. Карпенко О. В., Карпенко Ю. В. Штучний інтелект як інструмент публічного управління соціально-економічним розвитком: смарт-інфраструктура, цифрові системи бізнес-аналітики та трансферти. *Державне управління: удосконалення та розвиток.* 2021. № 10. DOI: <https://doi.org/10.32702/2307-2156-2021.10.2>

29. Карпенко О., Животова К. Концептуальні підходи до формування інформаційних механізмів запобігання та розв’язання міжнародних конфліктів. *Аспекти публічного управління.* 2022. Том 10. № 6. С. 14-18. DOI: <https://doi.org/10.15421/152238>

30. Карпенко О., Карпенко Ю., Герман, Д. Штучний інтелект як інструмент зниження корупційних ризиків у сфері публічних закупівель. *Аспекти публічного управління,* 2023. 11(2), 129-135. DOI: <https://doi.org/10.15421/152328>

31. Карпенко О.В. Цифрове врядування: імперативи реалізації в Україні. *Актуальні проблеми державного управління: Збірник наукових праць ОРІДУ.* 2017. Вип. 3(71). С. 57-61.

32. Карпець А.Ю. Правові проблеми регулювання соціальних мереж в Україні. *Актуальні проблеми міжнародних відносин.* 2012. Випуск 107 (частина II). С. 105–109.

33. Квітка С., Корсун, В. Механізми мережевого управління взаємодією публічної влади та громадянського суспільства. *Аспекти*

публічного управління, 2023/1(2), 81-87. DOI: <https://doi.org/10.15421/152322>

34. Квітка С., Мазур О. Особливості державної політики протидії соціальним конфліктам на основі розвитку співробітництва громад з використанням мережевого управління та смарт-спеціалізації територій. 2023. *Аспекти публічного управління*, 11(1), 86-93. <https://doi.org/10.15421/152312>

35. Квітка С., Миргородська М. Державна екологічна політика в умовах цифрового розвитку суспільства: механізми мережевого управління. *Аспекти публічного управління*. 2023. № 11(3), 30-37. DOI: <https://doi.org/10.15421/152332>

36. Коліушко І.Б., Демкова М.С. Електронне урядування – шлях до ефективності та прозорості державного управління. Інформаційне суспільство. Шлях України. К.: Бібліотека інформ. суспільства. 2004. С. 138-143.

37. Комунікативна діяльність в державному управлінні: навч. пос. / Н.М. Драгомирецька, К.С. Кандагура, А.В. Букач. Одеса : ОРІДУ НАДУ, 2017 180 с.

38. Комунікації в публічному управлінні: аспекти організаційної культури та ділового спілкування : навч. посіб. / уклад.: Гошовська В. А. та ін. Київ: К.І.С. 2016. 130 с.

39. Конвенція про захист прав людини і основоположних свобод (з протоколами) (Європейська конвенція з прав людини) від 4 листопада 1950 року. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 23.06.2023).

40. Коновал В.О. Методологічні засади електронного урядування на місцевому рівні: поняття, принципи, моделі та передумови. Теорія та практика державного управління. 2016. № 2 (53). URL: <http://www.kbuapa.kharkov.ua/e-book/tpdu/2016-2/doc/1/111.pdf>. (дата звернення: 15.10.2023)

41. Коноплицький С.М. Соціальні аспекти комунікації в мережі

Інтернет: феноменологічний аналіз: дис. канд. соціол. наук: 22.00.01 / НАН України; Інститут соціології. К., 2006. С. 154 – 156.

42. Конституція України: Закон України від 28 червня 1996 року № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text> (дата звернення: 23.06.2023).

43. Концепція застосування програмно-цільового методу в бюджетному процесі. Схваленою Розпорядженням Кабінету Міністрів України №539-р. 14.09.2002 р. URL: <https://zakon.rada.gov.ua/laws/show/538-2002-%D1%80#Text> (дата звернення: 10.03.2023)

44. Кузьменко Г.Є., Морозов А.О. Шлях від АСУП до ситуаційних центрів. Математичні машини і системи. 2008. № 3. С82-107.

45. Куйбіда В.С. Карпенко О.В., Наместнік В.В. Цифрове врядування в Україні: базові дефініції понятійно-категоріального апарату. *Вісн. НАДУ. Серія «Державне управління»*. 2018. № 1. С. 5-11.

46. Левченко О.В. Соціальні інтернет-мережі як вагомий чинник формування інформаційної безпеки України. *Збірник наукових праць Національної академії Державної прикордонної служби України (серія: військові та технічні науки)*. 2014. № 2 (62). С. 46–58.

47. Мехед Д. Інформаційна безпека в соціальних мережах. Методи поширення інформації в соціальних мережах. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: науково-технічний збірник*. 2015. Вип. 2 (30). С. 14–17. URL: http://ela.kpi.ua/bitstream/123456789/18028/1/30_p14.pdf (дата звернення: 15.10.2023)

48. Міжнародний пакт про громадянські і політичні права від 16 грудня 1966 року. Генеральна Асамблея ООН. Док. ООН А/RES/2200 А (XXI). (ратифіковано Указом Президії Верховної Ради Української РСР N 2148-VIII від 19.10.73) URL: https://zakon.rada.gov.ua/laws/show/995_043#Text (дата звернення: 23.06.2023).

49. Назвали найкращі сайти органів виконавчої влади. *Укрінформ*. 2018. URL: <https://www.ukrinform.ua/rubric-society/2733825-nazvali-najkrasisajti-organiv-vikonavcoi-vladi.html> (дата звернення: 15.10.2023)

50. Оприлюднено щорічний Звіт про виконання Угоди про асоціацію Україна-ЄС. *Урядовий портал*. 2023. URL: <https://www.kmu.gov.ua/news/opryliudneno-shchorichnyi-zvit-pro-vykonannia-uhody-pro-asotsiatsiiu-ukraina-ies> (дата звернення: 23.06.2023).

51. Остапчук Ю. Роль електронної комунікації в інформаційному суспільстві. *Вісник Книжкової палати*. 2016. № 5 с. 38-40.

52. Осьмак А., Карпенко Ю., Семененко І. Використання інструментів штучного інтелекту в мережевому управлінні: переваги, ризики та розвиток. *Аспекти публічного управління*. 2023. №11(3). С. 38-42. URL: <https://aspects.org.ua/index.php/journal/article/view/1012>. DOI: <https://doi.org/10.15421/152333>

53. Парубець О. М. Специфіка використання соціальних мереж для формування корпоративного іміджу організації. *International scientific and practical conference «The European development trends in journalism, PR, media and communication» : conference proceedings, February 26–27, 2021. Wloclawek, Republic of Poland : «Baltija Publishing»*. 179 pages. URL: <http://www.baltijapublishing.lv/omp/index.php/bp/catalog/book/108> (дата звернення: 15.06.2023).

54. Питання мережі ситуаційних центрів. Постанова Кабінету Міністрів України від 11.07.2023 р. № 705. URL: <https://zakon.rada.gov.ua/laws/show/705-2023-%D0%BF#Text> (дата звернення: 15.10.2023)

55. Питання сприяння розвитку громадянського суспільства в Україні: Указ Президента України від 25 січня 2012 року № 32/2012. <https://zakon.rada.gov.ua/laws/show/32/2012#Text> (дата звернення: 30.08.2023).

56. Плєскач В. Л., Заярний О. А., Плєскач М. В. Організаційно-правові механізми державного управління забезпеченням кібербезпеки та

кіберзахисту України: сутність, стан та перспективи розвитку. *Проблеми програмування*. 2020. № 2-3. С. 278-286.

57. Політики у сферах громадянського суспільства та медіа. UAReforms. 2023. URL: <https://uareforms.org/pages/new-page-652> (Дата звернення: 30.06.2023).

58. Почепцов Г.Г. Теория коммуникации. Киев: Ваклер, 2001. 656 с.

59. Пристайко В.В. Ситуаційні центри як ключовий інституційний механізм державного антикризового управління: зарубіжний досвід. Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне управління. Том 30 (69). № 3. 2019. С. 138-142.

60. Присяжнюк М.М., Парасунько М.М. Соціальні мережі як ефективний інструмент інформаційно-психологічного впливу іноземними спецслужбами. *Міжнародний науковий журнал «Інтернаука»*. 2017. № 2 (24). 1 т. С. 74–78.

61. Про громадські об'єднання: закон України від 22 березня 2012 року № 4572-VI. URL: <https://zakon.rada.gov.ua/laws/show/4572-17#Text> (дата звернення 30.08.2023).

62. Про деякі заходи щодо поліпшення доступу фізичних та юридичних осіб до електронних послуг: Указ Президента України від 29 липня 2019 року № 558/2019 URL: <https://zakon.rada.gov.ua/laws/show/558/2019#Text> (дата звернення: 30.06.2023).

63. Про доступ до публічної інформації: Закон України від 13 січня 2011 року № 2939-VI URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text> (дата звернення: 23.06.2023).

64. Про друковані засоби масової інформації (пресу) в Україні: закон України від 16 листопада 1992 року № 2782-XII URL: <https://zakon.rada.gov.ua/laws/show/2782-12#Text> (дата звернення: 23.06.2023).

65. Про електронні довірчі послуги: закон України від 5 жовтня 2017 року № 2155-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text>

(Дата звернення: 30.08.2023).

66. Про електронні комунікації: закон України від 16 грудня 2020 року № 1089-IX URL: <https://zakon.rada.gov.ua/laws/show/1089-20#n2246> (дата звернення: 23.06.2023).

67. Про забезпечення умов для більш широкої участі громадськості у формуванні та реалізації державної політики: Указ Президента від 31 липня 2004 року № 854/2004 URL: <https://zakon.rada.gov.ua/laws/show/854/2004#Text> (дата звернення 30.08.2023).

68. Про забезпечення участі громадськості у формуванні та реалізації державної політики: постанова Кабінету Міністрів України від 3 листопада 2010 р. № 996 URL: <https://zakon.rada.gov.ua/laws/show/996-2010-%D0%BF#Text> (дата звернення 30.08.2023).

69. Про забезпечення участі громадськості у формуванні та реалізації державної політики: Указ Президента України від 15 вересня 2005 року № 1276/2005. URL: <https://zakon.rada.gov.ua/laws/show/1276/2005#Text> (дата звернення: 30.08.2023).

70. Про забезпечення функціонування української мови як державної: закон України від 25 квітня 2019 року № 2704-VIII <https://zakon.rada.gov.ua/laws/show/2704-19#n611> (Дата звернення: 30.06.2023).

71. Про засади державної мовної політики: закон України 3 липня 2012 року № 5029-VI URL: <https://zakon.rada.gov.ua/laws/show/5029-17#Text> (дата звернення: 30.06.2023).

72. Про затвердження плану заходів до 2024 року щодо реалізації Національної стратегії сприяння розвитку громадянського суспільства в Україні на 2021-2026 роки: розпорядженням Кабінету Міністрів України від 14 лютого 2023 р. № 160-р. URL: <https://zakon.rada.gov.ua/laws/show/160-2023-%D1%80#Text> (дата звернення: 30.08.2023).

73. Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України: постанова

Кабінету Міністрів України від 3 вересня 2014 р. № 411. URL: <https://zakon.rada.gov.ua/laws/show/411-2014-%D0%BF#Text> (дата звернення: 30.08.2023).

74. Про затвердження Порядку оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади: Постанова Каб. Міністрів України від 04.01.2002 № 3. URL: <https://zakon.rada.gov.ua/laws/show/3-2002-п> (дата звернення: 15.08.2023)

75. Про захист інформації в інформаційно-комунікаційних системах: закон України від 5 липня 1994 року № 80/94-ВР. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text> (дата звернення: 30.08.2023).

76. Про захист персональних даних: закон України від 1 червня 2010 року № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 30.08.2023).

77. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні: Указ Президента України від 31 липня 2000 р. № 928/2000. URL: <https://zakon.rada.gov.ua/laws/show/928/2000#Text> (дата звернення: 30.06.2023).

78. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні: Указ Президента України від 31.07.2000 № 928. URL: <https://zakon.rada.gov.ua/laws/show/928/2000> (дата звернення: 15.10.2023)

79. Про інформацію: Закон України від 2 жовтня 1992 року № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (Дата звернення: 23.06.2023).

80. Про Концепцію Національної програми інформатизації: закон України від 4 лютого 1998 року № 75/98-ВР URL: <https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80#Text> (дата звернення: 30.06.2023).

81. Про медіа: закон України від 13 грудня 2022 року № 2849-IX URL: <https://zakon.rada.gov.ua/laws/show/2849-20#n2349> (дата звернення: 23.06.2023).

82. Про науково-технічну інформацію: закон України від 25 червня 1993 року № 3322-XII URL: <https://zakon.rada.gov.ua/laws/show/3322-12#Text> (дата звернення: 30.06.2023).

83. Про національну інфраструктуру геопросторових даних: Закон України від 13 квітня 2020 року № 554-IX URL: <https://zakon.rada.gov.ua/laws/show/554-20#Text> (дата звернення: 30.06.2023).

84. Про Національну програму інформатизації: закон України від 4 лютого 1998 року № 74/98-ВР URL: <https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80#Text> (дата звернення: 30.06.2023).

85. Про Національну програму інформатизації: закон України від 1 грудня 2022 року № 2807-IX URL: <https://zakon.rada.gov.ua/laws/show/2807-20#n191> (дата звернення: 30.06.2023).

86. Про Національну стратегію сприяння розвитку громадянського суспільства в Україні на 2021-2026 роки: Указ Президента України від 27 вересня 2021 року № 487/2021. URL: <https://zakon.rada.gov.ua/laws/show/487/2021#Text> (дата звернення: 30.06.2023).

87. Про основні засади розвитку інформаційного суспільства в Україні на 2007– 2015 роки: закон України від 9 січня 2007 року № 537-V URL: <https://zakon.rada.gov.ua/laws/show/537-16#Text> (дата звернення: 30.06.2023).

88. Про підготовку пропозицій щодо забезпечення гласності та відкритості діяльності органів державної влади: Указ Президента України від 17 травня 2001 року № 325/2001 URL: <https://zakon.rada.gov.ua/laws/show/325/2001#Text> (дата звернення: 30.06.2023).

89. Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації: закон України від 23 вересня 1997 року № 539/97-ВР URL: <https://zakon.rada.gov.ua/laws/show/539/97-%D0%B2%D1%80#Text> (дата звернення: 30.06.2023).

90. Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади: Постанова Кабінету Міністрів України від 4 січня 2002 р. № 3 URL: <https://zakon.rada.gov.ua/laws/show/3-2002-%D0%BF#Text> (дата звернення: 30.06.2023).

91. Про ратифікацію Конвенції про захист прав людини і основоположних свобод 1950 року, Першого протоколу та протоколів № 2, 4, 7 та 11 до Конвенції: Закон України від 17 липня 1997 року № 475/97-ВР. URL: <https://zakon.rada.gov.ua/laws/show/475/97-%D0%B2%D1%80#Text> (дата звернення: 23.06.2023).

92. Про стан розвитку громадянського суспільства України в 2021 році та його зміни на початку 2022 року : матер. щоріч. доп. / [В. Потапенко, Ю. Тищенко, Ю. Каплан та ін.] ; заг. ред. Ю. Каплан. Київ : НІСД, 2022. 56 с. URL: https://niss.gov.ua/sites/default/files/2022-11/stan_rozvytku_igs_na_site_22_11_22.pdf (дата звернення: 30.08.2023).

93. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації: розпорядження Кабінету Міністрів України від 17 січня 2018 р. № 67-р. URL: <https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text> (дата звернення: 30.08.2023).

94. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018 - 2020 роки та затвердження плану заходів щодо її реалізації: розпорядження Кабінету Міністрів України від 17 січня 2018 року № 67-р. URL: <https://www.kmu.gov.ua/ua/npas/proshvalennyakoncepciyi-rozvitku-cifrovoyi-ekonomiki-ta-uspilstva-ukrayini-na-20182020-rokita->

[zatverdzhennya-planuzahodiv-shodo-yiyi-realizaciyi](#) (дата звернення: 15.10.2023)

95. Про схвалення Концепції сприяння органами виконавчої влади розвитку громадянського суспільства: Розпорядження Кабінету Міністрів України від 21 листопада 2007 р. № 1035-р. URL: <https://zakon.rada.gov.ua/laws/show/1035-2007-%D1%80#Text> (дата звернення: 30.08.2023).

96. Про телебачення і радіомовлення: закон України від 21 грудня 1993 року № 3759-XII URL: <https://zakon.rada.gov.ua/laws/show/3759-12#Text> (дата звернення: 23.06.2023).

97. Про телекомунікації: закон України від 18 листопада 2003 року № 1280-IV. URL: <https://zakon.rada.gov.ua/laws/show/1280-15#Text> (дата звернення: 23.06.2023).

98. Про телекомунікації: Закон України. URL: <https://zakon.rada.gov.ua/laws/show/1280-15/pag> (дата звернення: 23.06.2023)

99. Проблеми інформаційного законодавства України в сфері створення, поширення та використання інформації та шляхи їх вирішення. Аналітична записка. Національний Інститут стратегічних досліджень. 2013. URL: <https://niss.gov.ua/doslidzhennya/informaciyni-strategii/problemi-informaciynogo-zakonodavstva-ukraini-v-sferi> (дата звернення: 30.06.2023).

100. Реалізація Національної стратегії місцевими державними адміністраціями. Урядовий портал. 2021. URL: <https://www.kmu.gov.ua/gromadskosti/gromadyanske-suspilstvo-i-vlada/spriyannya-rozvitku-gromadyanskogo-suspilstva/natsionalna-stratehiia-spriyannia-rozvytku-hromadianskoho-suspilstva-v-ukraini-na-2021-2026-roky/realizatsiia-natsionalnoi-stratehii-mistsevymy-derzhavnymy-administratsiiamy> (дата звернення: 23.06.2023)

101. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32,

частин другої, третьої статті 34 Конституції України від 20 січня 2012 року № 2-рп/2012. URL: <https://zakon.rada.gov.ua/laws/show/v002p710-12#n51> (дата звернення: 23.06.2023).

102. Семененко І.О. Оцінювання кібербезпеки: національний та глобальний виміри. *Кібербезпека державних інституцій та подолання кризових станів*: Матеріали I Міжнародної науково-практичної конференції (м. Київ, м. Вроцлав, 26 травня 2022 року). К.: ІСЗЗІ КПП ім. Ігоря Сікорського, 2022. 321 с. С.313-315.

103. Семененко І.О. Правові механізми використання соціальних мереж у публічному управлінні. *Державне управління: теорія та практика* – електронне наук. фах. видання. Національна академія державного управління при Президентові України. 2019. № 2.. С. 44-50. URL: <https://scholar.archive.org/work/3xi6h4loxrf5nnq2bdb636oqii/access/wayback/http://patp.academy.gov.ua/article/download/190046/189881> (дата звернення: 23.11.2023)

104. Семененко І.О. Світовий досвід функціонування мережі ситуаційних центрів органів державної влади. *Державне управління: удосконалення та розвиток*. 2022. № 9. DOI: <https://doi.org/10.32702/2307-2156.2022.9.15>

105. Семененко І.О. Ситуаційне управління у формуванні інформаційної безпеки: досвід ЄС для України. Політичні технології пропаганди та контрпропаганди у російсько-українській війні. Матеріали Круглого столу за міжнародною участю (м. Київ, КНЕУ, 21 лютого 2023 р.). К.: КНЕУ, 2023. 149 с. С. 145-148.

106. Семененко І.О. Використання соціальних мереж в публічному управлінні. *Теорія та практика публічного управління та адміністрування у XXI сторіччі* : матеріали II Всеукр. наук.-практ. конф. за міжнар. участю здобувачів вищої освіти та молодих вчених, (Київ, 22 листопада 2019 р.): за заг. ред. М.М. Білинської, О.М. Петроє, І.О. Дегтярьової. Київ : НАДУ, 2019. С. 249 – 250.

107. Семененко І.О. Реалізація мережевих технологій в публічному управлінні. *Альманах науки*. Науковий журнал. 2019. № 9 (30). С. 14 – 17.

108. Семененко І.О. Роль цифрових комунікацій в публічному управлінні. *Теорія та практика публічного управління та адміністрування у XXI сторіччі* : матеріали І Всеукр. наук.-практ. конф. за міжнар. участю здобувачів вищої освіти та молодих вчених, (Київ, 30 листопада 2018 р.): за заг. ред. В.С. Куйбіди, О.М. Петроє, І.О. Дегтярьової. Київ : НАДУ, 2018. С. 309 – 311.

109. Семененко І.О. Соціальні мережі як інструмент впливу на масову свідомість в умовах розвитку цифрового суспільства. *Публічне врядування в Україні: стан, виклики та перспективи розвитку* : матеріали щоріч. Всеукр. наук.-практ. конф. за міжнар. участю, присвяч. 100-річчю держ. служби в Україні, (Київ, 25 травня 2018 р.): у 5 т. / за заг. ред. В.С. Куйбіди, М.М. Білинської, О.М. Петроє. Київ: НАДУ, 2018. Т. 3. С. 117 – 119.

110. Семененко І.О. Соціальні мережі як цифровий інструмент маніпулювання свідомістю. *Україна 2030: публічне управління для сталого розвитку*: матеріали щоріч. міжнар. наук.-практ. конф., (Київ, 2020 р.): у 3 т. / за заг. ред. А.П. Савкова, М.М. Білинської, О.М. Петроє. Київ : НАДУ, 2020. Т. 2. – С. 128 – 130.

111. Система публічного управління в умовах децентралізації влади: механізми горизонтальної взаємодії : монографія / Л. Л. Приходченко, С. Є. Саханенко, П. І. Надолішній та ін. Одеса : ОРІДУ НАДУ, 2017. 332 с.

112. Ткач В.О. Економічна безпека України в регіональному вимірі. Бюлетень Міжнародного Нобелівського економічного форуму. 2011. № 1(4). С. 398–403. 12

113. Трансформація організаційно-економічних відносин до соціально-орієнтованих умов господарювання : [монографія] / А.В. Бондарчук, О.Ю. Бронська [та ін.] ; за заг. ред. В.М. Гончарова. Луганськ : Янтар, 2011. 268 с.

114. Три роки без ВКонтакте: яким соцмережам віддають перевагу

українці URL: <http://www.epravda.com.ua/publications/2019/11/14/653664/>
(дата звернення: 23.06.2023).

115. Тютюник В.В., Ященко О.А., Рубан І.В., Тютюник О.О., Особливості функціонування системи ситуаційних центрів на різних стадіях розвитку надзвичайних ситуацій. Сучасні інформаційні технології у сфері безпеки та оборони. 2022. Том 43 № 1. С. 41-52. DOI:10.33099/2311-7249/2022-43-1-41-52.

116. Угода про Асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 21 березня 2014 року, ратифіковано із заявою Законом України від 16 вересня 2014 року № 1678-VII. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text (дата звернення: 23.06.2023).

117. Угода про співробітництво в галузі інформації від 9 жовтня 1992 року. https://zakon.rada.gov.ua/laws/show/997_165#Text (дата звернення: 23.06.2023).

118. Федірко Н. В., Семененко І.О. Економічний механізм забезпечення ситуаційного мережевого управління в діяльності органів державної влади в Україні. *Бізнес-Інформ.* 2023. №10. DOI: DOI: <https://doi.org/10.32983/2222-4459-2023-10-86-94>

119. Цивільний Кодекс України: Закон України від 16 січня 2003 року № 435-IV <https://zakon.rada.gov.ua/laws/show/435-15#Text> (дата звернення: 23.06.2023).

120. Цимбаленко Я. Ю., Ніколенко Д. М. Інституційна корупція в органах публічної влади: філософсько-управлінський підхід. *Публічне управління та митне адміністрування*. 2021. № 1(28). С. 113-118. URL: DOI: <https://doi.org/10.32836/2310-9653-2021-1.18>

121. Цимбаленко Я. Ю., Палажченко, К. С. Узагальнення історичного досвіду становлення та розвитку державно-приватного партнерства. Інвестиції: практика та досвід. 2022. №4. С. 107–111. DOI:

<https://doi.org/10.32702/23066814.2022.4.107>

122. Ципліцька О.О. Регіональна та міжрегіональна мережева взаємодія як чинник модернізації промислового сектору. *Науковий погляд: економіка та управління*. 2020. №2 (68). С. 171-178.

123. Цифрова адженда України – 2020 («Цифровий порядок денний» – 2020): Концептуальні засади (версія 1.0). Першочергові сфери, ініціативи, проекти «цифровізації» України до 2020 року. 2016. 90 с. URL: <https://uccr.org.ua/uploads/files/58e78ee3c3922.pdf> (дата звернення: 23.06.2023).

124. Цифрова трансформація публічного управління : кол. моногр. / О. В. Карпенко, І. Й. Малий, Г. В. Муравицька та ін. Київ : НАДУ, 2020. 256 с.

125. Швець М.Я. Україна на шляху до інформаційного суспільства / М.Я. Швець, Р.А. Калюжний, В.С. Цимбалюк, В.Д. Гавловський та ін. – Правова інформатика. 2011. № 1. С. 90-99.

126. Шинкарук В.І. Комунікація / Філософський енциклопедичний словник / НАН України, Ін-т філософії ім. Г.С. Сковороди; голов. ред. В.І. Шинкарук. Київ: Абрис, 2002. 742 с.

127. Штепа Павло. Словник чужослів. URL: https://slovyk.me/dict/foreign_shtepa/%D0%B3%D0%B5%D0%BD%D0%B5%D0%B7%D0%B0 (дата звернення: 17.06.2023).

128. Шура Н. Принципи публічного адміністрування як регулятори соціально-економічних процесів у національній економіці. *Глобальні та національні проблеми економіки*. 2016. № 14. С.260-263. URL: <http://global-national.in.ua/archive/14-2016/54.pdf> (дата звернення: 23.06.2023)

129. Якимчук О. Онлайнові соціальні мережі: перспективи розвитку. *Релігія та соціум. Міжнародний часопис*. 2011. № 2 (6). С. 199–205.

130. 2020 Guide to Synthetic Media. Paperspace Blog. January 17, 2020. <https://blog.paperspace.com/2020-guide-to-synthetic-media/> (дата звернення: 18.09.2023).

131. A.I. for training military and civilian decision makers. URL:

<https://masasim.com/en/> (дата звернення: 15.09.2022).

132. About NCI ISACs. URL: https://www.nationalisacs.org/_files/ugd/b8fa6c_2abe94d6daa747e09a3ee5c3f64ebfe5.pdf (дата звернення: 26.09.2022)

133. Abrams R., 2009. "Uncovering the Network-Centric Organization." Ph.D. dissertation, University of California, Irvine, 2009. URL: <https://www.proquest.com/docview/304856743?pq-origsite=gscholar&fromopenview=true> (дата звернення: 15.09.2022).

134. Air Force Doctrine Document, 2-5.3 Psychological Operations (27 August 1999). URL: www.globalsecurity.org/military/library/policy/usaf/afdd/2-5-3/afdd2-5-3.pdf (дата звернення: 10.09.2023).

135. Allen, Jonathan; Hunnicutt, M. Sharon; Klatt, Dennis (1987). From Text to Speech: The MITalk system. Cambridge University Press. ISBN 978-0-521-30641-6. URL: https://www.researchgate.net/publication/256279457_From_text_to_speech_The_MITalk_system_Jonathan_Allen_M_Sharon_Hunnicutt_and_Dennis_Klatt_with_Robert_C_Armstrong_and_David_Pisoni_Cambridge_University_Press_Cambridge_1987_xii216_pp_2500 (дата звернення: 10.09.2023).

136. Amanowicz M. A Shared cybersecurity awareness Platform. *Journal of telecommunications and informational technology*. 2021. N3. Pp. 32-41. DOI: <https://doi.org/10.26636/jtit.2021.154421> (дата звернення: 10.09.2023).

137. Assessing the risks of language model «deepfakes» to democracy". 21 May 2021.

138. Barrabi T. Twitter developing 'synthetic media' policy to combat deepfakes, other harmful posts. Fox Business. Fox News. 21 October 2019. <https://www.foxbusiness.com/technology/twitter-synthetic-media-policy-feedback> (дата звернення: 20.09.2023).

139. Bobrovskyi O., Niema O., Domsha O., Zayats D., Vasiuk N. Elements of digitalization of public management and administration: information technologies and artificial intelligence in the field of HR. *AD ALTA: journal of interdisciplinary research*. 2023. Vol. 13/02-XXXV. P. 151-159. DOI:

<https://doi.org/10.33543/j.130235.151159>.

140. Brandon J. Terrifying high-tech porn: Creepy 'deepfake' videos are on the rise. Fox News. 2018-02-16. URL: <https://www.foxnews.com/tech/terrifying-high-tech-porn-creepy-deepfake-videos-are-on-the-rise> (дата звернення: 10.04.2023).

141. Bryson J.M. The Future of Public and Nonprofit Strategic Planning in the United States. Public Management Review. <https://calio.org/wp-content/uploads/2021/01/The-future-of-public-and-nonprofit-strategic-planning-in-the-United-States.pdf> (дата звернення: 15.10.2023).

142. Bryson J.M., Crosby B.C., Middleton Stone M. Designing and Implementing Cross-Sector Collaborations: Needed and Challenging. Public Administration Review. Vol. 75, No. 5, pp. 647-663.

143. Burns M. Information Warfare: What and How? URL: <https://www.cs.cmu.edu/~burnsm/InfoWarfare.html> (дата звернення: 10.09.2023).

144. Caramancion K.M. An Exploration of Disinformation as a Cybersecurity Threat. 2020 3rd International Conference on Information and Computer Technologies (ICICT). 2020. Pp. 440–444. DOI:10.1109/ICICT50521.2020.00076. URL: <https://ieeexplore.ieee.org/document/9092330> (дата звернення: 10.09.2023).

145. Charter on the Preservation of Digital Heritage. UNESCO. 2003. URL: <https://en.unesco.org/about-us/legal-affairs/charter-preservation-digital-heritage> (дата звернення: 23.06.2023).

146. Clemons E.K., Dewan R.M., Kauffman R.J., Weber T.A. Technological Innovations for Communication and Collaboration in Social Spaces. *Journal of Management Information Systems*. Volume 34, 2017. Issue 2. URL: <https://www.tandfonline.com/doi/full/10.1080/07421222.2017.1334464> (дата звернення: 15.10.2023).

147. Commander S., Poupakis S. Political Networks across the Globe. University of Oxford. 2020. URL: <https://www.econstor.eu/bitstream/10419/216415/1/dp13103.pdf> (дата звернення: 15.10.2023).

10.08.2023).

148. Dawes S.S., Gharawi M.A., Burke B.G. Transnational public sector knowledge networks: Knowledge and information sharing in a multi-dimensional context. *Government Information Quarterly*. Volume 29, Supplement 1, January 2012. URL:

<https://www.sciencedirect.com/science/article/abs/pii/S0740624X11000682> (дата звернення: 15.10.2023).

149. Don F. What Is Disinformation?. *Library Trends*. 2015. №63 (3): 401–426. DOI:10.1353/lib.2015.0014. hdl:2142/89818.

150. Dragos V. Semantic frameworks to enhance situation awareness for defence and security applications. *Information Retrieval*. Université de Paris, 2021. 100 p. URL: <https://hal.archives-ouvertes.fr/tel-03347626/document> (дата звернення: 15.09.2022).

151. Endsley M.R. Toward a theory of situation awareness in dynamic systems. *Situational Awareness*. Routledge, 2017, pp. 9 – 42.

152. Endsley M.R. Toward a theory of situation awareness in dynamic systems. *Situational Awareness*. Routledge, 2017, pp. 9 – 42.

153. European energy information sharing & analysis centre. URL: <https://www.ee-isac.eu/> (дата звернення: 15.09.2022).

154. Gaievska L., Karlova V., Bobrovska O., Kulynych M., Akimova L., Akimov O. Public-private partnership as a tool for implementing state policy/ *Ad Alta: Journal of interdisciplinary research*. 2023. №13(01), XXXIV, 21-30. DOI: <https://doi.org/10.33543/1301342130>.

155. Gulati R., Nickerson Jack A. Interorganizational Trust, Governance Choice, and Exchange Performance. *Organization Science*, INFORMS, vol. 19(5). URL: <https://ideas.repec.org/a/inm/ororsc/v19y2008i5p688-708.html> (дата звернення: 15.10.2023).

156. Haq E.-Ul, Tyson G., Braud T., Hui P. "Weaponising Social Media for Information Divide and Warfare". *Proceedings of the 33rd ACM Conference on Hypertext and Social Media*. HT '22. 2022-06-28 New York, NY, USA:

Association for Computing Machinery: 259–262. doi:10.1145/3511095.3536372. ISBN 978-1-4503-9233-4. S2CID 249872702.

157. Hatani F., McGaughey S.L. Network cohesion in global expansion: An evolutionary view. *Journal of World Business*. 2013. Vol. 48(4), P. 455-465.

158. HUDERIA: етичний компас для штучного інтелекту, September 29, 2023. URL: <https://cedem.org.ua/consultations/huderia/> (дата звернення: 15.10.2023).

159. Information Sharing and Analysis Centres (ISACs) Cooperative models / F.A. Juárez. Heraklion, Greece: European Union Agency for Network and Information Security (ENISA). 2017. 50 p.

160. Iskender D. Why it's time to change the conversation around synthetic media. URL: <https://venturebeat.com/media/why-its-time-to-change-the-conversation-around-synthetic-media/> (дата звернення: 20.10.2023).

161. Janofsky A. AI Could Make Cyberattacks More Dangerous, Harder to Detect". Wall Street Journal. 2018-11-13. URL: https://www.wsj.com/articles/ai-could-make-cyberattacks-more-dangerous-harder-to-detect-1542128667?mod=article_inline (дата звернення: 15.10.2023).

162. Janssen M., Klievink B. Developing Multi-Layer Information Infrastructures: Advancing Social Innovation through Public–Private Governance.

163. Jeffery N. Stakeholder Engagement: A Road Map to Meaningful Engagement. In the Doughty Centre 'How to do Corporate Responsibility' Series. Cranfield School of Management. URL: <https://www.fundacionseres.org/lists/informes/attachments/1118/stakeholder%20engagement.pdf> (дата звернення: 15.10.2023).

164. Jones C., Hesterly W.S., Borgatti, S.P. A General Theory of Network Governance: Exchange Conditions and Social Mechanisms. *Academy of Management Review*. 1997. № 22, p. 911-945.

165. Jones C., Hesterly W.S.; Borgatti S.P. A general theory of network governance: exchange conditions and social mechanisms". *Academy of*

Management Review. 1997. October. №22 (4): 911–945.
doi:10.5465/AMR.1997.9711022109.

166. Kapur R. Understanding the Practices required for Enhancing Organizational Structure. University of Delhi. URL: https://www.researchgate.net/publication/358046327_Understanding_the_Practices_required_for_Enhancing_Organizational_Structure (дата звернення: 15.10.2022).

167. Karpenko O. Manipulative information operations: factors of influence on social unconscious and cultural values. Вісник Національної академії керівних кадрів культури і мистецтв: наук. журнал. Київ: Міленіум, 2018. № 1. С. 26–29. URL: <http://academy.gov.ua/infpol/pages/dop/2/files/b848f23c-7699-4ef6-9d9b-18fa78325758.pdf>. (дата звернення: 15.10.2023).

168. Klijn E.H., Koppenjan J.F.M. Governance network theory: past, present and future. *Policy and Politics*. 2012. Vol 40 (4). Pp. 187-206. DOI: 10.1332/030557312X655431.

169. Knieser L. The case for a situational awareness network for emergency response. 2020. URL: <https://www.healthitanswers.net/the-case-for-a-situational-awareness-network-for-emergency-response/> (дата звернення: 15.09.2022).

170. Koliba C. Networks of Governance. Global Encyclopedia of Public Administration, Public Policy, and Governance. URL: https://link.springer.com/referenceworkentry/10.1007/978-3-319-31816-5_1765-1 (дата звернення: 20.06.2023).

171. Koliba C., Koopenjan J. Managing Networks as Complex Adaptive Systems. Loeffler, E. and Bovaird, T. (editors) *Public Management and Governance* (3rd edition). New York: Routledge Press. 2015. 300 p.

172. Koliba C. Networks of Governance. Global Encyclopedia of Public Administration, Public Policy, and Governance. New York: Springer Press. 2018. 400 p.

173. Lewis B.C. Information Warfare. URL:

<https://irp.fas.org/eprint/snyder/infowarfare.htm> (дата звернення: 10.09.2023).

174. Lunnan R., McGaughey S.L. Orchestrating international production networks when formal authority shifts. *Journal of World Business*. 2019, Volume 54, Issue 5. URL: <https://www.sciencedirect.com/science/article/abs/pii/S1090951618301263> (дата звернення: 15.10.2022).

175. Majava J. Ecosystem stakeholder analysis: an innovation-driven enterprise's perspective. University of Oulu, Finland. URL: <http://www.toknowpress.net/ISBN/978-961-6914-16-1/papers/ML16-078.pdf> (дата звернення: 15.10.2023).

176. Media – (dis) information – security. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf (дата звернення: 15.09.2023).

177. Miles R. E., Snow C.C.. Organizations: New Concepts for New Forms. *California Management Review*. Volume 28, Issue 3. <https://journals.sagepub.com/doi/10.2307/41165202> (дата звернення: 15.10.2023).

178. Minnaar R. Governance and control in the making: a field study of financial shared service centres. URL: https://www.researchgate.net/figure/Positioning-of-the-shared-service-centre-model-Janssen-Joha-2006_fig1_315786654 (дата звернення: 15.06.2023).

179. Mittelstadt B. D., Allo P., Taddeo M., Wachter S., Floridi, L. The ethics of algorithms: Mapping the debate. *Big Data & Society*, 2016. №3(2). DOI: 2053951716679679. URL: https://www.cnil.fr/sites/cnil/files/atoms/files/mittelstaedt_floridi_the_ethics_of_algorithms.pdf (дата звернення: 15.06.2023).

180. Navetta D. The Legal Implications of Social Networking: The Basics (Part One). 2011. URL: <http://www.infolawgroup.com/2011/06/articles/social-networking/the-legal-implications-of-social-networking-thebasics-part-one/> (дата звернення: 20.10.2023).

181. Nemr C., Gangware W. Weapons of Mass Distraction: Foreign State-

Sponsored Disinformation in the Digital Age (PDF). *Park Advisors*. March 28, 2019 Retrieved 26 January 2023. URL: <https://www.state.gov/wp-content/uploads/2019/05/Weapons-of-Mass-Distracton-Foreign-State-Sponsored-Disinformation-in-the-Digital-Age.pdf> (дата звернення: 10.10.2023).

182. Network Management. Cambridge Dictionary. URL: <https://dictionary.cambridge.org/dictionary/english/network> (дата звернення: 12.05.2023).

183. Neuron A., Fraefel M., Riedl R.. Inter-organizational Cooperation in Swiss eGovernment. https://www.researchgate.net/publication/221561050_Inter-organizational_Cooperation_in_Swiss_eGovernment

184. Okinawa Charter on Global Information Societ. Kyushu-Okinawa Summit-2000 (Official Documents). 2000. URL: <https://www.mofa.go.jp/policy/economy/summit/2000/pdfs/charter.pdf> (дата звернення: 23.06.2023).

185. Ostrom E. Understanding knowledge as a commons: from theory to practice. Cambridge, Massachusetts: MIT Press, 2007. 320 p.

186. Ovadya A. Deepfake Myths: Common Misconceptions About Synthetic Media. *Securing Democracy*. 14 June 2019. URL: <https://securingdemocracy.gmfus.org/deepfake-myths-common-misconceptions-about-synthetic-media/> (дата звернення: 15.01.2023).

187. Pangburn, DJ. You've been warned: Full body deepfakes are the next step in AI-based human mimicry. *Fast Company*. 21 September 2019. URL: <https://www.fastcompany.com/90407145/youve-been-warned-full-body-deepfakes-are-the-next-step-in-ai-based-human-mimicry> (дата звернення: 15.10.2023).

188. Pavlov N. Concept development and experimentation for EU conflict prevention and peace-building (CDE4PEACE). D4.1 Catalogue of available and emerging CD&E tools in the European Union. Vienna: SYNYO GmbH. 2021. URL: <https://www.cde4peace.eu/wp-content/uploads/sites/41/2021/07/CDE4Peace-D4.1-Catalogue-of-available-and->

[emerging-CDE-tools-in-the-EU-1.0.pdf](#) (дата звернення: 15.09.2022)

189. Pavlov N. Concept development and experimentation for EU conflict prevention and peace-building (CDE4PEACE). D4.1 Catalogue of available and emerging CD&E tools in the European Union. Vienna: SYNYO GmbH, 2021. URL: <https://www.cde4peace.eu/wp-content/uploads/sites/41/2021/07/CDE4Peace-D4.1-Catalogue-of-available-and-emerging-CDE-tools-in-the-EU-1.0.pdf> (дата звернення: 15.09.2022)

190. Picazo-Vela S., Gutiérrez-Martinez I., Luna-Reyes L. Understanding risks, benefits, and strategic alternatives of social media applications in the public sector. *Government information quarterly*. 2012. Vol. 29(4), pp. 504 – 511.

191. Proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)) URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>

192. Provan K.G., Milward H.B. Do Networks Really Work? A Framework for Evaluating Public-Sector Organizational Networks. URL: <https://www.jstor.org/stable/977503?typeAccessWorkflow=login> (дата звернення: 10.10.2023)

193. Raab J., Kenis P. Heading Toward a Society of Networks: Empirical Developments and Theoretical Challenges. *Journal of Management Inquiry*. Volume 18, Issue 3. URL: <https://journals.sagepub.com/doi/10.1177/1056492609337493> (дата звернення: 15.10.2023)

194. Rivellese N. NYC School Construction Authority Employee Directory. URL: <http://www.nycsca.org/Community/Public-Art-for-Public-Schools/Programs> (дата звернення: 15.10.2023)

195. Rycroft R.W., Kash DE. Self-Organizing Innovation Networks Implications For Globalization. URL: <https://www.scribd.com/document/480066583/RYCROFT-KASH-Self-organizing->

[innovation-networks-implications-for-globalization](#) (дата звернення: 15.10.2022)

196. Samuel G. Heard about deepfakes? Don't panic. Prepare. WE Forum. World Economic Forum. URL: <https://www.weforum.org/agenda/2018/11/deepfakes-video-pragmatic-preparation-witness/> (дата звернення: 15.10.2023)

197. Semenenko I.O. Sieci społecznościowe jako narzędzie do wdrażania decyzji zarządczych. *Cyfrowe instrumenty zarządzania publicznego: Ukraina – Polska: zbiór tez Dialogi zarządzania cyfrowego*. (Kijów, 27 listopada 2019 r.): kol. red.: O. Karpenko, M. Tenenbaum-Kulig, K. Gumenna. – Kijów, Wrocław: Narodowa Akademia Administracji Publicznej przy Prezydencie Ukrainy, Uniwersytet Wrocławski, 2019. S. 80 – 83.

198. Serban I.V., Sankar C., Germain M. Zhang S., Lin Z., Subramanian S., Kim T., Pieper M., Chandar S., Ke N.R., Rajeshwar S., De Brebisson A., Sotelo J.M.R., Suhubdy D., Michalski V., Nguyen A., Pineau J., Bengio Y. A Deep Reinforcement Learning Chatbot. 2017.

199. Situation centers. RCI-Consulting Solutions. URL: <https://rci-c.com/en/technology/sytuatsijni-tsentry/> (дата звернення: 31.03.2022)

200. Situation Centre (SITCEN). URL: https://www.nato.int/cps/en/natohq/topics_57954.htm (дата звернення: 31.03.2022)

201. Skoog R.A., Jasinski N., Shayman M.A., Ghahremanpour R., Kalantari M.. *Network management and control mechanisms to prevent maliciously induced network instability*. Conference: Network Operations and Management Symposium. Florence, Italy, 2002.

202. Smith, Bruce L. (17 February 2016). Propaganda. Encyclopædia Britannica, Inc. Retrieved 23 April 2016 <https://www.britannica.com/topic/propaganda> (дата звернення: 15.10.2023)

203. Söderholm P., Hellsmark H., Frishammar J., Hansson J., Mossberg J. et al. Technological development for sustainability: The role of network management in the innovation policy mix. *Technological forecasting & social*

change. 2019. URL: <https://www.diva-portal.org/smash/get/diva2:1263488/FULLTEXT01.pdf> (дата звернення: 15.10.2023)

204. Sorensen E., Torfing J. The democratic anchorage of governance networks". *Scandinavian Political Studies*. 2005. №28 (3): 195–218. DOI:10.1111/j.1467-9477.2005.00129.x.

205. Stein G.J. Information warfare. Air University (U.S.). Press. Retrieved March 26, 2022. URL: <https://www.hsdl.org/?view&did=439935> (дата звернення: 15.10.2023)

206. Van Baelen S., Peeters G., Bruyninckx H., Piloizzi P. Slaets P. Dynamic semantic world models and increased situational awareness for highly automated inland waterway transport. *Frontiers in Robotics and AI*. 2022. Vol. 8. Pp. 1-26. DOI: 10.3389/frobt.2021.739062

207. Waddell K. Welcome to our new synthetic realities. 2019. URL: <https://www.axios.com/2019/09/14/synthetic-realities-fiction-stories-fact-misinformation> (дата звернення: 15.10.2023)

208. Wallis T., Leszczyna R. EE-ISAC—Practical cybersecurity solution for the energy sector. *Energies*. 2022. 15. 2170. DOI: <https://doi.org/10.3390/en15062170>

209. What is explainable AI? URL: <https://www.ibm.com/topics/explainable-ai> (дата звернення: 15.10.2022)

210. Zaghloul E., Li T., Ren J. Security and Privacy of Electronic Health Records: Decentralized and Hierarchical Data Sharing using Smart Contracts. URL: <https://ieeexplore.ieee.org/document/8685552> (дата звернення: 15.09.2022)

211. Zolkiewski J. The Complexity of Power Relationships Within a Network. <https://www.escholar.manchester.ac.uk/uk-ac-man-scw:2b2665> (дата звернення: 15.11.2023)

ДОДАТКИ

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Статті у наукових фахових виданнях України

1. **Семененко І.О.** Правові механізми використання соціальних мереж у публічному управлінні. *Державне управління: теорія та практика* – електронне наук. фах. видання. Національна академія державного управління при Президентові України. 2019. № 2.. С. 44-50. URL: <https://scholar.archive.org/work/3xi6h4loxrf5nnq2bdb636oqii/access/wayback/http://patp.academy.gov.ua/article/download/190046/189881> (0,63 д.а.)
2. **Семененко І.О.** Світовий досвід функціонування мережі ситуаційних центрів органів державної влади. *Державне управління: удосконалення та розвиток*. 2022. № 9. DOI: <https://doi.org/10.32702/2307-2156.2022.9.15> (1,1 д.а.)
3. Федірко Н. В., **Семененко І.О.** Економічний механізм забезпечення ситуаційного мережевого управління в діяльності органів державної влади в Україні. *Бізнес-Інформ*. 2023. №10. DOI: <https://doi.org/10.32983/2222-4459-2023-10-86-94> (0,96 д.а., особисто автору 0,65 д.а., обґрунтовано зміст та структуру економічного механізму забезпечення функціонування ситуаційних центрів органів державної влади)
4. Осьмак А., Карпенко Ю., **Семененко І.** Використання інструментів штучного інтелекту в мережевому управлінні: переваги, ризики та розвиток. *Аспекти публічного управління*. 2023. №11(3). С. 38-42. URL: <https://aspects.org.ua/index.php/journal/article/view/1012>. DOI: <https://doi.org/10.15421/152333> (0,6 д. а., особисто автору – 0,45 д.а., визначено основні переваги, перспектив розвитку та ризиків застосування інструментів штучного інтелекту, як механізмів мережевого управління, а також надання практичних рекомендацій щодо підходів до розробки

алгоритмів застосованих моделей та їхнього законодавчого регулювання).

В інших виданнях

5. **Семененко І.О.** Соціальні мережі як інструмент впливу на масову свідомість в умовах розвитку цифрового суспільства. *Публічне врядування в Україні: стан, виклики та перспективи розвитку* : матеріали щоріч. Всеукр. наук.-практ. конф. за міжнар. участю, присвяч. 100-річчю держ. служби в Україні, (Київ, 25 травня 2018 р.): у 5 т. / за заг. ред. В.С. Куйбіди, М.М. Білинської, О.М. Петроє. Київ: НАДУ, 2018. Т. 3. С. 117 – 119. (0,2 д.а.)

6. **Семененко І.О.** Роль цифрових комунікацій в публічному управлінні. *Теорія та практика публічного управління та адміністрування у XXI сторіччі* : матеріали I Всеукр. наук.-практ. конф. за міжнар. участю здобувачів вищої освіти та молодих вчених, (Київ, 30 листопада 2018 р.): за заг. ред. В.С. Куйбіди, О.М. Петроє, І.О. Дегтярьової. Київ : НАДУ, 2018. С. 309 – 311. (0,2 д.а.)

7. **Семененко І.О.** Реалізація мережевих технологій в публічному управлінні. *Альманах науки*. Науковий журнал. 2019. № 9 (30). С. 14 – 17. (0,15 д.а.)

8. **Семененко І.О.** Використання соціальних мереж в публічному управлінні. *Теорія та практика публічного управління та адміністрування у XXI сторіччі* : матеріали II Всеукр. наук.-практ. конф. за міжнар. участю здобувачів вищої освіти та молодих вчених, (Київ, 22 листопада 2019 р.): за заг. ред. М.М. Білинської, О.М. Петроє, І.О. Дегтярьової. Київ : НАДУ, 2019. С. 249 – 250. (0,16 д.а.)

9. **Semenenko I.O.** Sieci społecznościowe jako narzędzie do wdrażania decyzji zarządczych. *Cyfrowe instrumenty zarządzania publicznego: Ukraina – Polska: zbiór tez Dialogi zarządzania cyfrowego*. (Kijów, 27 listopada 2019 r.): kol. red.: O. Karpenko, M. Tenenbaum-Kulig, K. Gumenna. – Kijów, Wrocław: Narodowa Akademia Administracji Publicznej przy Prezydencie Ukrainy, Uniwersytet Wrocławski, 2019. S. 80 – 83. (0,1 д.а.)

10. **Семененко І.О.** Соціальні мережі як цифровий інструмент маніпулювання свідомістю. *Україна 2030: публічне управління для сталого розвитку*: матеріали щоріч. міжнар. наук.-практ. конф., (Київ, 2020 р.): у 3 т. / за заг. ред. А.П. Савкова, М.М. Білінської, О.М. Петроє. Київ : НАДУ, 2020. Т. 2. – С. 128 – 130. (0,1 д.а.)

11. **Семененко І.О.** Оцінювання кібербезпеки: національний та глобальний виміри. *Кібербезпека державних інституцій та подолання кризових станів*: Матеріали I Міжнародної науково-практичної конференції (м. Київ, м. Вроцлав, 26 травня 2022 року). К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2022. С.313-315. (0,15 д.а.)

12. **Семененко І.О.** Ситуаційне управління у формуванні інформаційної безпеки: досвід ЄС для України. Політичні технології пропаганди та контрпропаганди у російсько-українській війні. Матеріали Круглого столу за міжнародною участю (м. Київ, КНЕУ, 21 лютого 2023 р.). К.: КНЕУ, 2023. С. 145-148. (0,18 д.а.)



**АДМІНІСТРАЦІЯ
ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ
(АДМІНІСТРАЦІЯ ДЕРЖСПЕЦЗВ'ЯЗКУ)**

вул. Солом'янська, 13, м. Київ, 03110, тел. (044) 281-93-08, факс: (044) 281-94-83,
e-mail: info@cip.gov.ua, сайт: www.cip.gov.ua, код згідно з ЄДРПОУ 34620942

14.11.2023 № 04/01/02-4548/BC На № _____ від _____

ДОВІДКА

про впровадження результатів дисертаційного дослідження
Семененко Ірини Олександрівни
за темою “Механізми реалізації мережевого управління у діяльності органів
державної влади”

Результати дисертаційного дослідження аспірантки кафедри національної економіки та публічного управління Київського національного економічного університету імені Вадима Гетьмана Семененко Ірини Олександрівни за темою “Механізми реалізації мережевого управління у діяльності органів державної влади” на здобуття ступеня доктора філософії за спеціальністю 281 “Публічне управління та адміністрування” використано у діяльності Департаменту захисту критичної інфраструктури Адміністрації Держспецзв'язку.

При розробці проекту постанови Кабінету Міністрів України “Про затвердження Плану взаємодії суб'єктів національної системи захисту критичної інфраструктури” враховано науково-обґрунтовані пропозиції дисертантки щодо застосування організаційних механізмів мережевого управління для забезпечення взаємодії суб'єктів національної системи захисту критичної інфраструктури в межах функцій та повноважень, визначених Законом України “Про критичну інфраструктуру” від 16 листопада 2021 року № 1882-IX.

Заступник Голови Держспецзв'язку



Олександр ПОТІЙ



Україна

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
імені Вадима Гетьмана

03057, м. Київ, пр-т Берестейський (пр-т Перемоги), 54/1. e-mail: office@kneu.edu.ua
Тел.: (044) 456-50-55, (044) 371-61-19. ЄДРПОУ: 02070884

06.12.22 № 01/13-619

На № _____

ДОВІДКА

про впровадження результатів дисертаційного дослідження
Семененко Ірини Олександрівни за темою «Механізми реалізації
мережевого управління у діяльності органів державної влади» в
навчальний процес Київського національного економічного університету
імені Вадима Гетьмана

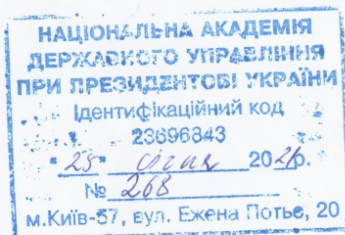
Довідка видана у підтвердження того, що результати дисертаційного дослідження сформульовані в роботі Семененко Ірини Олександрівни за темою «Механізми реалізації мережевого управління у діяльності органів державної влади» використано в навчальному процесі кафедри національної економіки та публічного управління Київського національного економічного університету імені Вадима Гетьмана при підготовці та викладанні навчальних дисциплін «Цифрові технології в публічному управлінні» та «Сервісна діяльність органів публічної влади». Запропоновано науково-обґрунтовані підходи щодо досягнення максимального рівня ефективності діяльності ситуаційних центрів у сфері забезпечення захисту критичної інфраструктури та реалізації кібербезпеки інформаційного середовища України.

Проректор
з науково-педагогічної роботи,
доктор економічних наук, професор



Анатолій КОЛОТ

001753



ДОВІДКА

про участь у науково-дослідних роботах

Видана СЕМЕНЕНКО Ірині Олександрівні з підтвердженням про те, що вона дійсно брала участь у виконанні науково-дослідних робіт за комплексним науковим проектом "Державне управління та місцеве самоврядування" (державний реєстраційний номер 0199U002827) Національної академії державного управління при Президентові України, а саме:

- у 2019 році - виконавець на громадських засадах (наказ від 14 березня 2019 року № 143-ос "Про призначення виконавців науково-дослідних робіт") науково-дослідної роботи "Сервісна діяльність органів публічної влади в умовах розвитку цифрового суспільства", державний реєстраційний номер 0119U101449.

Керівник науково-дослідної роботи,
д.держ.упр., доцент

Олександр КАРПЕНКО

Директор Інституту
експертно-аналітичних
та наукових досліджень
д.держ.упр., доцент

Ольга ПЕТРОШ

