КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова праця
на правах рукопису

КОВАЛЕНКО ОЛЕКСАНДР ВАЛЕНТИНОВИЧ

УДК 35-027.21:351.86](477)

ДИСЕРТАЦІЯ

ДЕРЖАВНІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Спеціальність 281 «Публічне управління та адміністрування»
Галузь знань 28 «Публічне управління та адміністрування»

Подається на здобуття ступеня доктора філософії
у галузі публічного управління та адміністрування

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

Науковий керівник – Абрамов Володимир Іванович,
доктор філософських наук, професор

Київ – 2023

АНОТАЦІЯ

Коваленко О.В. Державні механізми забезпечення кібербезпеки України. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії з галузі знань 28 «Публічне управління та адміністрування» за спеціальністю 281 «Публічне управління та адміністрування». – Київський національний університет імені Тараса Шевченка. Київ, 2023.

У дисертаційній роботі вирішено актуальне наукове завдання, яке полягає в обґрунтуванні теоретичних засад та практичних пропозицій щодо вдосконалення механізмів забезпечення кібербезпеки України, що створює підґрунтя для науково обґрунтованого своєчасного та адекватного державного реагування на загрози кібербезпеці.

Установлено ступінь наукової розробленості проблем функціонування механізмів забезпечення кібербезпеки України в галузі знань «Публічне управління та реагування». Зазначено, що на сьогодні ще обмаль наукових праць, у яких би розглядалися питання публічно-управлінської інтерпретації проблем забезпечення кібербезпеки в Україні. У низці наукових праць не повною мірою висвітлено питання щодо теоретико-методологічного обґрунтування механізмів забезпечення кібербезпеки, адміністративно-організаційних напрямів розбудови СКБ України в умовах трансформацій зовнішнього та внутрішнього безпекового середовища, функцій, структури, повноважень та особливостей органів публічної влади усіх рівнів щодо забезпечення кібербезпеки, створення механізмів переведення теоретичних знань кризового та антикризового менеджменту в практичну діяльність органів публічної влади, що опікуються питаннями інформаційної та кібербезпеки.

Осмислення логіки взаємозв’язку проблематики публічного управління кібербезпекою в умовах інформаційних війн різного формату

дало змогу в рамках системно-ситуаційного підходу сконструювати стратифікаційну модель реалізації функцій державного кризового реагування в зазначеній сфері. Остання слугує методологічною основою обґрунтування теоретико-методологічних засад розроблення та функціонування механізмів забезпечення кібербезпеки. Вказана модель представлена автором у вигляді семи страт: страти процесу діяльності, на якому розкривають уявлення про предмет, суб'єкт, мету, засіб, процес і результат публічно-управлінської діяльності у сфері кібербезпеки; страт функцій «комунікація», «планування», «організація», «контроль», «мотивація», «прийняття публічно-управлінських рішень», на яких розкриваються уявлення про обмін релевантною інформацією між учасниками соціально-інформаційних відносин, про систему кібербезпеки, механізми забезпечення кібербезпеки, кібервійни, багаторівневу організацію та здійснення державного проактивного й реактивного реагування.

З'ясовано, що теоретичними основами розроблення механізмів забезпечення кібербезпеки є використання теорії систем, теорії національної безпеки, теорії кібербезпеки, теорії публічного управління та теорії інституціоналізму, а функціонування вказаних механізмів має здійснюватися в рамках теорії ефективності механізму державного реагування на загрози національній безпеці.

Обґрунтовано, що структурними компонентами системи забезпечення кібербезпеки є: державно-політичний, правовий, інституційний механізми, механізм розробки державної політики у сфері кібербезпеки та комплексний механізм її реалізації. СЗКБ структурно включає в себе: організаційно-адміністративний і фінансовий механізми, механізми реактивного й проактивного реагування на загрози кібербезпеці, кадровий, науково-методичний та інформаційно-аналітичний механізми забезпечення кібербезпеки, механізми партнерства і співробітництва з питань забезпечення кібербезпеки, механізм інтеграції національного

кіберпростору у світовий кібернетичний простір, механізм партисипаторної взаємодії у сфері забезпечення кібербезпеки, які використовуються у комплексі з метою забезпечення кібербезпеки.

Показано, що в сучасній практиці міждержавного протиборства досить широко застосовуються технології кібервійн та мережо-центричних війн, що суттєво, а інколи й визначально впливає на трансформацію безпекового кіберсередовища.

З'ясовано, що керівництво держав-членів НАТО досягнуло значних результатів в розбудові національних СКБ, а саме: а) реалізовано перспективну модель СКБ на основі задіяння компонентів забезпечення кібербезпеки визначених в керівних документах НАТО і ЄС; б) сформовано інституційне середовище кібербезпеки, яке структурно містить правовий, організаційний, самоорганізаційний, соціокультурний, когнітивний компоненти.

Обґрунтовано доцільність використання у практиці державного управління кібербезпекою України досвіду держав-членів НАТО щодо: визначення перспективної моделі СКБ; формування інституційного середовища кібербезпеки з урахуванням вимог зовнішнього та внутрішнього безпекового середовища до національної СКБ.

Доведено, що в Україні функціонує СЗКБ з усіма її перевагами і недоліками. Наразі вказана система залишається остаточно не сформованою, й в сучасних умовах гібридної війни в повній мірі не задовольняє потреби щодо своєчасного та адекватного реагування на виклики та загрози кібербезпеці України. Суб'єкти забезпечення кібербезпеки здійснюють лише окремі види забезпечення кібербезпеки, що значно знижує можливу інтегральну ефективність СЗКБ. Такий стан справ у цій специфічній сфері може призвести до небезпечної різноспрямованості заходів державного реагування на загрози кібербезпеці України.

Виявлено актуальні проблеми функціонування державних механізмів

забезпечення кібербезпеки України, як-от: проблема забезпечення кібербезпеки України в умовах російсько-української війни, що зумовлена браком систематизованих знань про сучасні технології кібервійн, а також браком аналітичної інформації необхідної для прийняття рішень щодо ефективного реагування на виклики та загрози кібербезпеці; проблема своєчасної адаптації нормативно-правової бази у сфері забезпечення кібербезпеки з урахуванням появи нових викликів, загроз, небезпек кібернетичного характеру; проблема наявних розривів між базовими соціальними інститутами, які визначають зміни в інституціональному середовищі публічного управління кібербезпекою, а також інституційних розривів між суміжними інститутами зовнішнього та внутрішнього інституціонального середовища публічного управління кібербезпекою, інституційного розриву між загальним станом інституту аналітичної діяльності в СЗКБ та складністю безпекового кіберсередовища; проблема наявних розривів в організації діяльності суб'єктів забезпечення кібербезпеки України; проблема удосконалення структури, уточнення функцій та конкретизація завдань СЗКБ, а також проблема удосконалення державних механізмів забезпечення кібербезпеки; проблема низької загальної ефективності механізму державного реагування на загрози кібербезпеці України та інформаційно-аналітичного механізму забезпечення кібербезпеки України.

Показано, що створення державних механізмів забезпечення кібербезпеки є поетапним, поступовим, тривалим за часом процесом, який включає змістовну складову і вимагає проведення відповідної роботи у нормативно-правовому, організаційно-управлінському, фінансовому, безпековому, кадровому та освітньому аспектах.

З метою вдосконалення механізмів забезпечення кібербезпеки України в умовах євроінтеграції та зовнішньої агресії перспективною моделлю СЗКБ визначено креативну модель та сформульовано пропозиції органам державної влади щодо її упровадження в публічно-управлінську

практику, як-от:

1 група пропозицій щодо визначення пріоритетних напрямів вдосконалення інституціонального середовища публічного управління кібербезпекою України: 1) теоретичний напрям, що передбачає формування базових засад формування інституціонального середовища публічного управління кібербезпекою, зокрема загальні положення, базові категорії і поняття публічно-управлінської проблематики забезпечення кібербезпеки; теоретичні підходи до формування інституціонального середовища публічного управління кібербезпекою; 2) правовий напрям, що спрямований на вдосконалення нормативно-правового забезпечення формування інституціонального середовища публічного управління кібербезпекою; 3) організаційний напрям, що передбачає створення інституціональної матриці й механізмів забезпечення кібербезпеки;

2 група пропозицій щодо вдосконалення державно-політичного механізму забезпечення кібербезпеки, що передбачає розробку та впровадження у вітчизняну публічно-управлінську практику структурно-функціональної моделі публічного управління кібербезпекою;

3 група пропозицій удосконалення соціально-психологічного механізму усвідомлення проблем забезпечення кібербезпеки, що передбачає розроблення та упровадження в публічно-управлінську практику структурно-логічних моделей реалізації функцій «комунікація», «планування», «мотивація», «прийняття публічно-управлінських рішень», «контроль» у публічному управлінні у сфері забезпечення кібербезпеки;

4 група пропозицій щодо удосконалення кадрового механізму забезпечення кібербезпеки, а саме удосконалення системи підготовки фахівців-управлінців у сфері національної безпеки;

5 група пропозицій щодо удосконалення СЗКБ України в сучасних умовах російсько-української війни, що передбачає впровадження в публічно-управлінську практику перспективної моделі згаданої системи, яка містить такі складові, як-от: функціональна, інформаційна,

інституційна моделі.

6 група пропозицій щодо удосконалення інформаційно-аналітичного механізму забезпечення кібербезпеки, що передбачає впровадження в публічно-управлінську практику інформаційно-аналітичної діяльності автоматизованих систем збирання й структуризації інформації, а також розвиток науково-методичного апарату інформаційно-аналітичного забезпечення політики забезпечення кібербезпеки, зокрема: визначення системи показників оцінки рівня загроз кібербезпеки; визначення системи критеріїв оцінки ефективності механізмів державного реагування на загрози кібербезпеці; розробку та впровадження в публічно-управлінську практику забезпечення кібербезпеки паспортів загроз у цій сфері;

7 група пропозицій щодо удосконалення механізму державного реагування на виклики та загрози кібербезпеці, що передбачає: розробку та впровадження у публічно-управлінську практику технологій державного реагування на загрози кібербезпеці; визначення змісту механізмів реактивного та проактивного реагування на загрози кібербезпеці.

8 група пропозицій щодо удосконалення організаційно-адміністративного механізму забезпечення кібербезпеки передбачає розробку та офіційне затвердження національної рамки реагування на загрози кібербезпеці.

9-11 групи пропозицій щодо удосконалення інформаційного механізму, механізму забезпечення комунікації суб’єктів забезпечення кібербезпеки, удосконалення механізму міжнародного й міждержавного співробітництва з питань забезпечення кібербезпеки України передбачають дотримання науково обґрунтованих принципів у відповідних сферах забезпечення кібербезпеки.

Ключові слова: кібербезпека, кібератака, паспорт загроз, державне реагування, механізми державного управління, національна безпека, інформаційна безпека, державна політика, система кібербезки, критична інфраструктура, публічне управління, загрози кібербезпеці.

ANNOTATION

Kovalenko O.V. State mechanisms for ensuring cyber security of Ukraine. – Qualifying scientific work on manuscript rights.

Dissertation for obtaining the degree of Doctor of Philosophy in the field of knowledge 28 "Public management and administration" in the specialty 281 "Public management and administration". – Kyiv National University named after Taras Shevchenko. Kyiv, 2023.

The thesis solves an actual scientific task, which consists in substantiating the theoretical principles and practical proposals for improving the mechanisms for ensuring cyber security of Ukraine, which creates the basis for a scientifically based, timely and adequate state response to cyber security threats.

The degree of scientific elaboration of the problems of the functioning of mechanisms for ensuring cyber security of Ukraine in the science of "Public management and response" has been established. It is noted that today there is still a shortage of scientific works in which the issues of public-management interpretation of the problems of ensuring cyber security in Ukraine would be considered. In a number of scientific works, the issue of the theoretical and methodological substantiation of the mechanisms for ensuring cyber security, administrative and organizational directions for the development of the cyber security system of Ukraine in the conditions of transformations of the external and internal security environment, functions, structure, powers and features of public authorities of all levels regarding the provision of cyber security is not fully covered., creation of mechanisms for transferring theoretical knowledge of crisis and anti-crisis management into practical activities of public authorities dealing with issues of information and cyber security.

Comprehension of the logic of the interrelation of the issues of public management of cyber security in the conditions of information wars of various formats made it possible to construct a stratification model of the

implementation of state crisis response functions in the specified area within the framework of the system-situational approach. The latter serves as the methodological basis for substantiating the theoretical and methodological foundations of the development and functioning of cyber security mechanisms. The specified model is presented by the author in the form of seven layers: the layer of the activity process, which reveals the idea of the subject, subject, goal, means, process and result of public management activity in the field of cyber security; layers of functions "communication", "planning", "organization", "control", "motivation", "making public-management decisions", which reveal ideas about the exchange of relevant information between participants of social and information relations, about the cyber security system, mechanisms ensuring cyber security, cyber warfare, multi-level organization and implementation of state proactive and reactive response.

It was found that the theoretical bases for the development of mechanisms for ensuring cyber security are the use of systems theory, the theory of national security, the theory of cyber security, the theory of public administration and the theory of institutionalism, and the functioning of the specified mechanisms should be carried out within the framework of the theory of the effectiveness of the mechanism of state response to threats to national security.

It is substantiated that the structural components of the system of ensuring cyber security are: state-political, legal, institutional mechanisms, the mechanism of development of state policy in the field of cyber security and the complex mechanism of its implementation. The system of ensuring cyber security structurally includes: organizational-administrative and financial mechanisms, a mechanism of state response to threats to cyber security, a mechanism for preventing threats to cyber security, personnel, scientific-methodical and informational and analytical mechanisms for ensuring cyber security, a mechanism for partnership and cooperation on issues of ensuring cyber security, a mechanism integration of the national cyberspace into the global cyberspace, the mechanism of participatory interaction in the field of

ensuring cyber security, which are used in a complex for the purpose of ensuring cyber security.

It is shown that in the modern practice of interstate confrontation, the technologies of cyber wars and network- centric wars are quite widely used, which significantly, and sometimes decisively, affects the formation of the security environment.

It has been found that the leadership of NATO member states has achieved significant results in the development of national cyber security systems, namely: a) a perspective model of cyber security has been implemented based on the implementation of cyber security components defined in the guiding documents of NATO and the EU; b) the institutional environment of cyber security has been formed, which structurally contains legal, organizational, self -organizing, socio-cultural, cognitive components.

The expediency of using the experience of NATO member states in the practice of the state management of cyber security of Ukraine is substantiated in relation to: defining a perspective model of cyber security; formation of the institutional cyber security environment taking into account the requirements of the external and internal security environment to the national cyber security system.

It has been proven that a cyber security system with all its advantages and disadvantages is functioning in Ukraine. Currently, the specified system remains not finally formed, and in the modern conditions of hybrid warfare does not fully satisfy the need for a timely and adequate response to challenges and threats to Ukraine's cyber security. Subjects of cyber security provide only certain types of cyber security, which significantly reduces the possible integrated effectiveness of the cyber security system. Such a state of affairs in this specific area can lead to a dangerous multidirectionality of state response measures to threats to Ukraine's cyber security.

Actual problems of the functioning of the state mechanisms for ensuring cyber security of Ukraine have been identified, such as: the problem of ensuring

cyber security of Ukraine in the conditions of hybrid warfare, which is caused by a lack of systematized knowledge about modern technologies of cyber wars, as well as a lack of analytical information necessary for decision-making regarding effective response to challenges and threats to cyber security; the problem of timely adaptation of the regulatory and legal framework in the field of cyber security, taking into account the emergence of new challenges, threats, and dangers of a cyber nature; the problem of existing gaps between basic social institutions that determine changes in the institutional environment of the state management of cyber security, as well as institutional gaps between adjacent institutions of the external and internal institutional environment of the state management of cyber security, the institutional gap between the general state of the institute of analytical activity in the system of ensuring cyber security and the complexity of cyberspace and safe environment; the problem of existing gaps in the organization of the activities of entities providing cyber security of Ukraine; the problem of improving the structure, clarifying functions and specifying the tasks of the cyber security system, as well as the problem of improving state mechanisms for cyber security; the problem of low overall efficiency of the mechanism of state response to threats to cyber security of Ukraine and the information and analytical mechanism of ensuring cyber security of Ukraine.

It is shown that the creation of state mechanisms for ensuring cyber security is a step-by-step, gradual, long-term process that includes a meaningful component and requires appropriate work in regulatory, organizational, managerial, financial, security, personnel and educational aspects.

In order to improve the mechanisms for ensuring Ukraine's cyber security in the conditions of European integration and external aggression, a prospective model of the cyber security system has been defined, a creative model has been defined and proposals have been formulated for state authorities regarding its implementation in public management practice, such as:

1 group of proposals regarding the identification of priority directions for

improving the institutional environment of public administration in the sphere of ensuring cyber security of Ukraine: 1) theoretical direction, which provides for the formation of the basic foundations of the formation of the institutional environment of public management in the field of cyber security, in particular, general provisions, basic categories and concepts of public management issues of cyber security; theoretical approaches to the formation of the institutional environment of public administration in the field of ensuring cyber security; 2) the legal direction aimed at improving the regulatory and legal support for the formation of the institutional environment of public administration in the field of cyber security; 3) the organizational direction, which provides for the creation of an institutional matrix and mechanisms of public management in the field of ensuring cyber security;

2nd group of proposals for improving the state-political mechanism for ensuring cyber security, which involves the development and implementation of a conceptual model of public management in the field of cyber security into domestic public management practice;

The 3rd group of proposals for improving the social and psychological mechanism for ensuring cyber security, which involves the development and introduction into public management practice of structural and logical models for the implementation of the functions "communication", "planning", "motivation", "making public management decisions", "control » in public administration in the sphere of ensuring cyber security;

4th group of proposals for improving the staffing mechanism for ensuring cyber security, namely improving the system of training managers in the field of national security;

5 group of proposals for improving the system of ensuring cyber security of Ukraine in the modern conditions of the Russian-Ukrainian war, which involves the introduction of a prospective model of the mentioned system into public management practice, which contains such components as: functional, informational, institutional models.

The 6th group of proposals for improving the information and analytical mechanism for ensuring cyber security, which provides for the introduction of automated systems for collecting and structuring information into the public management practice of information and analytical activity, as well as the development of a scientific and methodological apparatus for information and analytical support for the policy of ensuring cyber security, in particular: defining the system indicators for assessing the level of cyber security threats; definition of a system of criteria for evaluating the effectiveness of state response mechanisms to cyber security threats; development and introduction into public management practice of ensuring cyber security of passports of threats in this area;

7th group of proposals for improving the mechanism of state response to cyber security challenges and threats, which includes: development and implementation of state response technologies to cyber security threats into public management practice; determination of the content of the mechanisms of reactive and proactive response to cyber security threats.

8 група пропозицій щодо удосконалення організаційно-адміністративного механізму забезпечення кібербезпеки передбачає розробку та офіційне затвердження національної рамки реагування на загрози кібербезпеці.

9-11 групи пропозицій щодо удосконалення інформаційного механізму, механізму забезпечення комунікації суб'єктів забезпечення кібербезпеки, удосконалення механізму міжнародного й міждержавного співробітництва з питань забезпечення кібербезпеки України передбачають дотримання науково обґрунтованих принципів у відповідних сферах забезпечення кібербезпеки.

Keywords: cyber security, cyber attack, threat passport, government response, national security, information security, government policy, cyber security system, critical infrastructure, public administration, cyber security threats.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Праці, які відображають основні наукові результати дисертації

1. Коваленко О.В. Концептуальні засади розвитку національної системи кібербезпеки України на сучасному етапі державного будівництва. *Державне управління: удосконалення та розвиток*. 2020. № 6. URL: http://www.dy.nayka.com.ua/?op=1&z=1694 (дата звернення: 15.06.2022). DOI: 10.32702/2307-2156-2020.6.102

2. Коваленко О.В. Розбудова системи кібербезпеки Іспанії: уроки для України. *Інвестиції: практика та досвід*. 2020. № 17–18. С. 149–153.

3. Коваленко О.В. Теоретико-методологічні засади формування механізмів забезпечення кібербезпеки України на сучасному етапі державного будівництва. *Věda a perspektivy.* 2022. №6 (13). С. 21–33.

4. Коваленко О.В. Теоретичні засади проектування системи забезпечення кібербезпеки України. Державне управління: удосконалення та розвиток. 2022. № 10. URL: https://www.nayka.com.ua/index.php/dy/article/view/636 (дата звернення: 28.10.2022). DOI: 0.32702/2307-2156.2022.10.12

Праці, які додатково відображають наукові результати дисертації

1. Коваленко О.В. Заходи з протидії негативним інформаційним впливам на групову, масову та індивідуальну свідомість громадян України, які здійснюються російськими спецслужбами в рамках гібридної війни. *Становлення публічного адміністрування в Україні*: матеріали X конференції студентів та молодих учених за міжнародною участю (м. Дніпро, 10 травня 2019 року) / за загальною редакцією О.Б. Кірєєвої. Д.: ДРІДУ НАДУ, 2019. С. 138-141.

2. Коваленко О.В. Державні механізми забезпечення кібербезпеки України в умовах євроінтеграційних та глобалізаційних викликів. *Інституціоналізація публічного управління в Україні в умовах євроінтеграційних та глобалізаційних викликів*: матеріали щорічної

науково-практичної конференції за міжнародною участю (Київ, 24 травня 2019 року) / за загальною редакцією А.П. Савкова, М.М. Білинської, О.М. Петроє. Київ, НАДУ, 2019, том 3, С. 48-50.

3. Коваленко О.В. Концептуальні засади державно-управлінської діяльності у сфері забезпечення кібербезпеки України. *Україна 2030: публічне управління для сталого розвитку*: матеріали щорічній Всеукр. наук.-практ. конф. за міжнар. участю. К. : НАДУ, 2020. Том №3. С. 40-41.

4. Коваленко О.В. Методологічні засади формування управлінської культури кібербезпекою України. Актуальні питання, проблеми та перспективи розвитку гуманітарного знання у сучасному інформаційному просторі: національний та інтернаціональний аспекти: зб. наук. праць / за заг. ред. д.філос.н. Журби М.А. – Монреаль: CPM «ASF», 2020. С. 90-93.

Праці, опубліковані в інших виданнях

1. Коваленко О.В. Механізми формування та реалізації державної політики у сфері інформаційної безпеки України: особливості розбудови в умовах гібридної війни та сучасний стан. *Інформаційно-психологічна протидія у ЗСУ: історія, сучасний стан та перспективи вдосконалення:* матеріали науково-практичного семінару / за ред.. В.М. Мороза. К.: НДЦГПЗСУ, 2021. С. 30-38.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ЄС – Європейський Союз;

ЗМІ – засоби масової інформації;

МВС – Міністерство внутрішніх справ;

МЗС – Міністерство закордонних справ;

МОУ – Міністерство оборони України;

НАТО – Організація Північноатлантичного договору;

РНБОУ – Рада національної безпеки і оборони України;

рф – російська федерація;

СБУ – Служба безпеки України;

СЗНБ – система забезпечення національної безпеки;

СЗКБ – система забезпечення кібербезпеки;

СНБ – система національної безпеки;

СКБ – система кібербезпеки;

США – Сполучені Штати Америки;

ВСТУП

Актуальність теми. Російсько-українська війна, яка ведеться росією проти нашої держави та наростаючі у глобалізованому світі різного роду небезпеки, серед яких значне, а інколи й визначальне значення мають кібервійни, формують довгострокові виклики для національної безпеки України. Саме тому в офіційному дискурсі національної безпеки України визначено завдання реформи СНБ відповідно до вимог динамічного безпекового середовища. Одним із пріоритетних завдань реформованої СНБ має бути надійне гарантування кібербезпеки, адже сьогодні використання кіберзброї в геополітичному інформаційному протиборстві стало окремою та самостійною формою інформаційної війни. За цих умов, загрози кібербезпеці України перешкоджають розв'язанню нагальних проблем інформаційного розвитку та цифровізації різних сфер життєдіяльності нашої країни, порушують цілісність державно-управлінського простору, що насамкінець може призвести до втрати Україною своєї державності.

Ця обставина й визначає зв'язок загальної проблеми гарантування кібербезпеки України з найбільш важливими науково-практичними завданнями реактивного й проактивного реагування на загрози кібербезпеці в умовах динамічного безпекового кіберсередовища. За таких умов, що склалися існує нагальна необхідність пошуку принципово нових концептуальних підходів до розбудови та функціонування державних механізмів забезпечення кібербезпеки з урахуванням сучасних трендів геополітичного інформаційного протиборства та глобальних трансформацій в управлінні великими соціальними системами, до яких належить національна держава.

У процесі написання дисертаційного роботи було використано монографії та інші наукові розробки українських науковців, що стали науковою основою в осмисленні сучасних проблем державного та публічного управління, а саме праці: В. Абрамова [1-3; 214; 232],

В. Бакуменка [11], О. Валевського [21], В. Голубь [33], В. Гурковського [42], В. Козакова [87], Р. Лопушинського [101], Ю. Нестеряка [120], А. Рачинського [174], О. Руденко [178], Г. Ситника [123; 130; 192-196; 257] та ін.

Публічно-управлінські проблеми забезпечення національної, й зокрема, інформаційної безпеки та кібербезпеки України досліджували: В. Антонюк [8; 9], В. Дзюндзюк [47], О. Житник [59], Т. Запорожець [60; 61; 260], О. Зозуля [67; 68], Н. Клименко [76], Д. Костенко [92], Є. Котух [93], Р. Марутян [107-110], М. Орел [128; 129; 257], А. Семенченко [183-192], Є. Таран [207; 228; 257-259], О. Твердохліб [208; 209], та ін. При всій важливості проведених досліджень окремі аспекти залишаються недостатньо вивченими, зокрема питання деструктивного впливу інформаційно-технологічного чинника на національну безпеку та врахування його при розробці та впровадженні публічно-управлінських рішень у сфері забезпечення кібербезпеки України.

Недосконаліть наукових основ розробки та функціонування механізмів забезпечення кібербезпеки в умовах євроінтеграції та російсько-української війни обумовило актуальність проведення даного дисертаційного дослідження.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження проводилося в рамках науково-дослідної роботи кафедри глобалістики, євроінтеграції та управління національною безпекою НАДУ за темою: «Входження України до Європейського та Євроатлантичного просторів як гарантія забезпечення національної безпеки» (ДР № 119U101583). У рамках цієї НДР автором досліджено організаційно-правові засади реактивного та проактивного реагування на загрози кібербезпеці України, узагальнено і систематизовано досвід країн-членів НАТО і ЄС у цій сфері; обґрунтовано пропозиції щодо паспортизації загроз кібербезпеці та технологізації процесу державного реагування на загрози кібербезпеці.

Мета і завдання дослідження. Метою дослідження є обґрунтування теоретичних засад та практичних пропозицій щодо вдосконалення державних механізмів забезпечення кібербезпеки України.

Для досягнення поставленої мети вимагалося вирішення таких завдань:

з'ясувати ступінь наукової розробленості проблем забезпечення кібербезпеки у вітчизняній науці;

удосконалити понятійно-категоріальний апарат публічно-управлінської проблематики забезпечення кібербезпеки;

визначити теоретичні засади розроблення та функціонування державних механізмів забезпечення кібербезпеки;

визначити роль і місце кібервійни в структурі сучасного геополітичного інформаційного протиборства, закономірності розвитку СКБ та СЗКБ;

вивчити зарубіжний досвід (на прикладі країн-членів НАТО і ЄС) щодо формування та функціонування державних механізмів забезпечення кібербезпеки та оцінити можливості його використання в Україні;

оцінити сучасний стан державних механізмів забезпечення кібербезпеки України;

обґрунтувати пропозиції щодо удосконалення механізмів забезпечення кібербезпеки України з урахуванням специфіки переходу від держаного до публічного управління та вимог динамічного безпекового середовища.

Об'єкт дослідження – публічне управління кібербезпекою.

Предмет дослідження – державні механізми забезпечення кібербезпеки України.

Методи дослідження. Для вирішення завдань дисертаційного дослідження використано загальнонаукові і спеціальні методів, за допомогою яких одержано наукові і практичні результати, зокрема: порівняльний метод використано для уточнення основних понять

проблематики забезпечення кібербезпеки, для вивчення зарубіжного та вітчизняного досвіду формування та реалізації політики у сфері забезпечення кібербезпеки; метод систематизації – в процесі аналізу наукових праць українських і зарубіжних учених; абстрактно-логічний метод – для теоретичного узагальнення й формулювання висновків; статистичний метод – для опрацювання статистичної інформації, яка характеризує сучасний стан та динаміку чинників кібербезпеки; метод моделювання і прогнозування – для розробки перспективної моделі СЗКБ, при визначенні механізмів забезпечення кібербезпеки, розробці рекомендацій щодо їх державного конструювання та удосконалення, а також при розробці концептуальної моделі публічного управління кібербезпекою; метод проектування – для впровадження в публічно-управлінську практику забезпечення кібербезпеки перспективної моделі СЗКБ; графічний метод – для наочного відображення досліджуваних явищ та схематичного представлення отриманих результатів дослідження.

Наукова новизна одержаних результатів полягає в тому, що в дисертації вирішено актуальне науково-практичне завдання в галузі знань «Публічне управління та адміністрування», яке полягає в обґрунтуванні науково-теоретичних засад державних механізмів забезпечення кібербезпеки в сучасних умовах державного будівництва в Україні і розробка на цій основі пропозицій щодо підвищення результативності їх функціонування. Зокрема, у дисертаційній роботі:

уперше:

– розроблено та науково обґрунтовано структурно-функціональну модель публічного управління кібербезпекою, яка структурно включає три ієрархічні рівні: перший рівень – це інституціональне середовище публічного управління кібербезпекою; другий рівень – це рівень процесів функціонування комплексного механізму формування сучасної конфігурації кіберпростору в Україні та комплексного механізму публічного управління кібербезпекою, що забезпечує формування та

реалізацію політики забезпечення кібербезпеки; третій рівень – це організаційний рівень, що включає етапи організації державно-регулюючого впливу на процес забезпечення кібербезпеки;

– розроблено і науково обґрунтовано стратифікаційну модель реалізації функцій публічного управління кібербезпекою. Стратифікаційне та ешелоноване відображення основних функцій публічного управління кібербезпекою дозволило здійснити системний аналіз та комплексний опис процесів реалізації функцій публічного управління у згаданій сфері, а також системно відобразити процес державного реагування на загрози кібербезпеці з урахуванням рухомості інституціонального середовища публічного управління, безпекового кіберсередовища;

– розроблено і науково обґрунтовано перспективну модель СЗКБ, яка структурно містить функціональну, інформаційну та інституційні моделі, а також передбачає реалізацію нових завдань згаданої системи відповідно до вимог динамічного публічно-управлінського простору та безпекового середовища – партисипаторну взаємодію між державою та громадянським суспільством, ІТ-бізнесом, реактивне та проактивне реагування на виклики та загрози кібербезпеці;

удосконалено:

– теоретичні засади організації та здійснення публічного управління кібербезпекою через розроблення авторської концепції, що передбачає поєднання модельного підходу з інституціональним та структурно-функціональним підходами. Це дозволило подати інституалізацію державних механізмів забезпечення кібербезпеки як конкретно-історичний процес, якому притаманна власна внутрішня «логіка» та закономірності становлення та розвитку вказаних механізмів;

– теоретичне обґрунтування місії, функцій та завдань перспективної моделі СЗКБ шляхом уточнення наявних і виявлення нових властивостей цієї системи з урахуванням трансформацій в безпековому кіберсередовищі, процесів формування механізму партисипаторної взаємодії держави, ІТ-

бізнесу та громадянського суспільства з питань регулювання суспільно-інформаційних відносин та положень інституціоналізму, що дає змогу поряд з партисипаторною функцією СЗКБ виокремити такі функції, як нормативно-управлінську, програмно-адаптивну, науково-адаптивну та соціально-адаптивну, що регулюють розвиток СЗКБ на базі моделі зміни «соціокультурного поля», яка репрезентована сукупністю: ідей та теорій; норм і цінностей; різних видів взаємодії та організаційних зв'язків; інтересів і статусів суб'єктів забезпечення кібербезпеки;

– науково-теоретичні засади механізму розробки політики забезпечення кібербезпеки через розроблення функціональної моделі визначення імперативів політики забезпечення кібербезпеки в умовах трансформації безпекового кіберсередовища на основі характеристики сучасних тенденцій кібервійни та розвитку загроз кібербезпеці, оцінки майбутнього стану безпекового кіберсередовища та діагностики стану кібербезпеки;

– науково-теоретичні засади організаційно-адміністративного механізму забезпечення кібербезпеки через розроблення національної рамки реагування на загрози кібербезпеці, що регламентує застосування суб'єктами забезпечення кібербезпеки відповідних видів державного реагування на загрози кібербезпеці в контекстній залежності від рівня загрози (потенційна або реальна загроза), а також розподіл відповідальності суб'єктів забезпечення кібербезпеки на загальнодержавному, відомчому та внутрішньовідомчому рівнях за організацію та результати державного реагування на загрози кібербезпеки;

– науково-теоретичні засади механізму державного реагування на загрози кібербезпеці, в які, на відміну від відомих, було додатково введено національну рамку комплекс процедур, що передбачають поєднання: 1) механізму проактивного реагування на загрози кібербезпеці, що передбачає теоретичне обґрунтування і практичне забезпечення спрямованості етапів запобігання та врегулювання конфліктів у

кіберпросторі; 2) механізми реактивного реагування на загрози кібербезпеці, що передбачають теоретичне обґрунтування і практичне забезпечення спрямованості етапів мінімізації існуючих загроз, локалізацію і ліквідацію наслідків їх реалізації;

– теоретичний підхід до оцінювання можливостей використання зарубіжного досвіду щодо формування державних механізмів забезпечення кібербезпеки у вітчизняній практиці гарантування кібербезпеки, що ґрунтується на принципах концепції «національного прагматизму»;

набули подальшого розвитку:

– понятійно-категорійний апарат у сфері забезпечення кібербезпеки шляхом уточнення поняття «кібербезпека», введення в науковий обіг авторських визначень понять: «соціально-психологічний механізм усвідомлення проблем забезпечення кібербезпеки», «система кібербезпеки», «система забезпечення кібербезпеки», «державна політика забезпечення кібербезпеки», «державно-політичний механізм забезпечення кібербезпеки», «механізм розробки політики забезпечення кібербезпеки», «механізм реалізації політики забезпечення кібербезпеки», «організаційно-адміністративний механізм забезпечення кібербезпеки», «інституційний механізм забезпечення кібербезпеки», «фінансовий механізм забезпечення кібербезпеки», «кадровий механізм забезпечення кібербезпеки», «механізм науково-методичного забезпечення кібербезпеки», «механізм забезпечення комунікації суб’єктів забезпечення кібербезпеки», «механізм інформаційного забезпечення кібербезпеки», «механізм забезпечення управлінської взаємодії суб’єктів забезпечення кібербезпеки», «інформаційно-аналітичний механізм забезпечення кібербезпеки», «механізм міжнародного співробітництва з питань забезпечення кібербезпеки», «механізм міждержавного співробітництва з питань забезпечення кібербезпеки», «механізм партисипаторної (громадської) взаємодії у сфері забезпечення кібербезпеки», «механізм інтеграції національного кіберпростору у світовий кіберпростір», «механізм

інформаційно-технологічного забезпечення реагування на загрози кібербезпеці», «механізм державного реагування на загрози кібербезпеці», «механізм проактивного реагування на загрози кібербезпеки», «механізм реактивного реагування на загрози кібербезпеки», «технологія державне реагування на загрози кібербезпеці»;

– обґрунтування необхідності паспортизації загроз кібербезпеці як напряму вдосконалення інформаційно-аналітичного механізму забезпечення кібербезпеки;

– обґрунтування необхідності технологізації процесу державного реагування на загрози кібербезпеці як напряму вдосконалення механізмів державного реагування на загрози кібербезпеці;

– систематизація положень, що містяться в науковому дискурсі кібервійни та мережо-центричної війни, а також їх впливу на процес трансформації безпекового кіберсередовища.

Теоретичне значення дисертації міститься у наукових положеннях, які можуть бути використані у науково-дослідницькій роботі щодо питань: модернізації СЗКБ України; вдосконалення теоретичних підходів дослідження трансформацій кібервійни та безпекового кіберсередовища як соціально-технічної системи.

Практичне значення отриманих результатів полягає в тому, що теоретичні положення й висновки дисертаційної роботи подані у формі пропозицій, які мають придатну для застосування в практиці публічно-управлінської діяльності форму й можуть бути використані для обґрунтування засад та розробки заходів щодо удосконалення державних механізмів забезпечення кібербезпеки України. Вони можуть також бути корисними в організаційно-управлінській роботі органів державної влади, що опікуються питаннями забезпечення кібербезпеки України при розробці або удосконаленні нормативно-правової бази в галузі національної безпеки і оборони, оптимізації структури й функцій СЗКБ.

Наукові висновки, пропозиції, рекомендації, що містяться в дисертації, ураховані та використані:

– Управлінням розвитку автоматизації Апарату Головнокомандувача Збройних Сил України у процесі підготовки пропозицій з питань підвищення рівня кібербезпеки України та протидії впливу іноземних держав у ІТ- сфері (довідка про упровадження № 364/1-1998 від 09 листопада 2020 р.);

– Департаментом контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України у процесі підготовки пропозицій з питань підвищення рівня кібербезпеки України та протидії впливу іноземних держав у ІТ- сфері (довідка про упровадження № 30/3/3-6537 від 8 липня 2020 р.);

– Апаратом РНБО України у процесі підготовки пропозицій з питань визначення організаційно-технічної структури Національного координаційного центру при РНБО України (акт про упровадження № 1430/16-07/2-21 від 3 березня 2020 р.);

– Воєнно-дипломатичною академією імені Євгенія Березняка в навчальному процесі, а саме при підготовці лекційного курсу з навчальної дисципліни «Національна безпека» (акт про упровадження № 222/ВА/1043ВС від 26.12.2022 р.).

Особистий внесок здобувача. Дисертаційне дослідження є самостійною науковою працею автора. Основні розробки, що характеризують наукову новизну й практичне значення отриманих результатів дослідження, здійснені автором особисто.

Апробація результатів дисертації. Основні теоретичні положення і висновки дисертаційного дослідження були оприлюднені на наукових та науково-практичних конференціях, наукових семінарах: «Україна 2030: публічне управління для сталого розвитку» (Київ, 2020 р.); «Актуальні питання, проблеми та перспективи розвитку гуманітарного знання у сучасному інформаційному просторі: національний та інтернаціональний

аспекти» (Монреаль, 2020 р.), «Становлення публічного адміністрування в Україні» (Дніпро, 2019 р.); «Інституціоналізація публічного управління в Україні в умовах євроінтеграційних та глобалізаційних викликів» (Київ, 2019 р.); «Інформаційно-психологічна протидія у ЗСУ: історія, сучасний стан та перспективи вдосконалення» (Київ, 2021 р.).

Публікації. Основні наукові результати дисертаційного дослідження опубліковано у 9 наукових працях, серед яких: три статті у наукових фахових виданнях України з державного управління, одна стаття у наукових періодичних виданнях інших держав з напряму, з якого підготовлено дисертацію; 4 тез у матеріалах науково-практичних конференцій, семінарів; одна публікація, що додатково висвітлює результати дослідження.

Структура та обсяг дисертації. Дисертаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Повний обсяг роботи становить 237 сторінок, із них 199 сторінок основного тексту. Робота містить 11 рисунків, 3 додатки. Список використаних джерел містить 260 найменувань, із них 28 іноземною мовою.

РОЗДІЛ 1
МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ЯК ОБ'ЄКТ НАУКОВОГО АНАЛІЗУ В ПУБЛІЧНОМУ УПРАВЛІННІ

1.1. Ступінь розробки проблематики публічного управління кібербезпекою

З'ясування ступеня розробки проблематики публічно-управлінських проблем забезпечення кібербезпеки України передбачало критичне опрацювання питань, які відображають різні аспекти проблеми, що розглядається. При цьому за напрямами та методологічними засадами досліджень усі джерела інформації умовно були поділені на тринадцять груп.

Першу групу джерел складає нормативно-правова база з ключових питань національної безпеки і оборони України [89; 113; 122; 136; 138; 139; 142; 144-147; 151; 153; 157-159; 161-164]. Результати аналізу цієї групи джерел дозволяють констатувати, що наразі має місце низка неузгоджень між законами, указами і постановами, а саме:

недосконалість понятійно-категоріального апарату, який використовується у сфері національної безпеки та національної стійкості;

дублювання функцій та завдань суб'єктами забезпечення національної безпеки в мирний час та особливий період;

недосконалість правового механізму забезпечення національної стійкості в умовах гібридної війни.

Другу групу джерел складає нормативно-правова база з питань інформаційного розвитку суспільства та забезпечення кібернетичної безпеки України [137; 143; 148-150; 152; 154-156; 160; 165].

Результати аналізу цієї групи джерел дозволяють констатувати, що правові засади забезпечення кібербезпеки України сформовані.

Третю групу джерел складають наукові праці, енциклопедична,

довідкова та навчальна література в яких розглядаються питання історичного розвитку поняття «кібернетична безпека» [4; 10; 13; 14; 16-20; 23; 27; 28; 34; 35; 39; 54-56; 167-169; 207-209].

Аналіз цієї групи джерел дозволяє констатувати, що черговий етап розвитку кібербезпеки пов'язаний із широким використанням новітніх інформаційно-комунікаційних технологій.

Поняття кібербезпеки в науковому дискурсі трактується:

як стан захищеності інтересів особистості, суспільства і держави у кібернетичній сфері;

як забезпечення стану захищеності особистості, суспільства, держави від деструктивних інформаційно-технологічних впливів.

Четверту групу джерел складають наукові праці в яких надано характеристику інформаційної безпеки та кібербезпеки в системі державного управління [112; 170; 210-212].

Аналіз цієї групи джерел дає підстави констатувати:

сформованість СКБ України, яка проте не функціонує як цілісна система;

відсутність в науковому дискурсі загальновизнаного розуміння місії СЗКБ та завдань механізмів забезпечення кібербезпеки України.

П’яту групу джерел складають наукові праці в яких розглядається питання сучасних механізмів міжсекторної взаємодії у сфері забезпечення кібербезпеки [76; 121; 127; 133; 175; 176; 177; 197; 201-203].

На підставі аналізу цієї групи джерел нами було узагальнено перелік проблем міжвідомчої взаємодії суб’єктів забезпечення кібербезпеки України:

відсутність постійних форматів міжвідомчої взаємодії з питань реагування на загрози кібербезпеці;

недосконалість механізмів організації взаємодії і координації дій суб’єктів забезпечення кібербезпеки України;

інституційна неспроможність механізму партисипаторної взаємодії

держави і громадянського суспільства, ІТ-бізнесу з питань забезпечення кібербезпеки.

Шосту групу джерел складають наукові праці в яких розглядається питання державних механізмів забезпечення інформаційної та кібербезпеки України [46; 88; 130; 132; 178-180; 183-191; 220; 221; 226; 227].

Проаналізувавши вказану групу джерел, констатуємо наявність таких проблем у сфері забезпечення кібербезпеки України, як:

потреба в оновленні організаційно-правових засад забезпечення кібербезпеки з урахуванням вимог динамічного безпекового середовища;

подолання етатичних тенденцій у сфері розроблення політики забезпечення кібербезпеки України шляхом широкого обговорення проектів керівних документів у цій сфері;

відсутність ефективного державного механізму інформаційно-аналітичного забезпечення кібербезпеки України;

відсутність ефективних державних механізмів реактивного і проактивного реагування на загрози кібербезпеці;

недостатній рівень взаємодії з НАТО з питань впровадження стандартів реагування на загрози кібербезпеці.

Сьому групу джерел складають документи, що регулюють питання забезпечення інформаційної безпеки та кібербезпеки іноземних держав, а також наукові праці в яких розглядається актуальні проблеми інформаційної та кібернетичної безпеки вказаних держав [15; 45; 58-61; 118; 126; 166; 216; 218; 219; 233-256].

Ця група джерел дозволила нам узагальнити та систематизувати зарубіжний досвід щодо організаційно-правового забезпечення розбудови та функціонування національних систем забезпечення інформаційної та кібернетичної безпеки на принципах національної стійкості, а також здійснити оцінку можливостей використання досвіду країн-членів НАТО і ЄС у сфері гарантування кібербезпеки в Україні. Проте питання

компаративного аналізу досвіду розбудови системи кібербезпеки у вказаних наукових працях в прямій постановці питання не розглядається.

Восьму групу джерел складають наукові праці, навчальна і довідкова література в яких розглядається широкий спектр потенційних та реальних загроз інформаційній безпеці та кібербезпеці України, а також методи реагування на них [4-10; 12; 24-31; 43; 49; 98; 101; 102; 105; 115; 119; 200; 207; 208; 215; 222; 223; 225].

Аналіз цієї групи джерел дозволяє констатувати, що недостатня визначеність та систематизація проблем моніторингу загроз інформаційній безпеці та кібербезпеці України в умовах гібридної війни, підходів до їх розв'язання обмежує можливості щодо розробки та застосування формалізованих моделей при розробці та реалізації державної політики у сфері кібербезпеки.

Дев'яту групу джерел складають наукові праці та аналітичні дослідження проблем формування систем національної безпеки та національної стійкості України, а також матеріали ЗМІ [16; 66; 67; 86; 134; 135; 170; 173-175]. Зокрема, в [135, с. 79] визначено такі напрями забезпечення національної стійкості, як: зовнішньополітичний; економічний; енергетичний; соціально-політичний; правовий; гуманітарний; демографічний; духовно-культурний; освітній і науковий; мережево-інформаційний; воєнно-політичний.

Аналіз цієї групи джерел дозволяє констатувати, що наразі у вітчизняному науковому середовищі йде активна розробка теоретико-методологічних засад формування системи національної стійкості України. Проте питання розробки та реалізації політики забезпечення кібернетичної стійкості України у вітчизняному науковому дискурсі представлено поодинокими публікаціями. Це є підтвердженням своєчасності та актуальності теми нашого дисертаційного дослідження.

Десяту групу складають дисертаційні роботи в галузі знань «Державне управління», в яких розглянуто державно-управлінські

проблеми забезпечення інформаційної безпеки України, а також визначаються шляхи вдосконалення системи забезпечення інформаційної безпеки [9; 42; 57; 93].

В дисертаційному дослідженні В. Гурковського «Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки» обґрунтовано пропозиції щодо удосконалення системи державного управління інформаційною безпекою, а саме розроблено правовий механізм взаємодії, координації діяльності органів державної влади у цій специфічній сфері [42].

В дисертаційному дослідженні В. Гурковським запропоновано включити до понятійно-категоріальної сітки державного управління інформаційною безпекою категорії «правова підтримка національної інформаційної безпеки». Під останньою автор пропонує розуміти нормативно-правову діяльність суб'єктів суспільно-інформаційних у сфері гарантування інформаційної безпеки.

В дисертації Л. Євдоченко «Удосконалення системи державного забезпечення інформаційної безпеки України в умовах глобалізації» [57] обґрунтовано концептуальні підходи та розроблено практичні рекомендації щодо удосконалення системи забезпечення інформаційної безпеки України в контексті вимог розвитку інформаційного суспільства в Україні та у світі.

В цій дисертаційній роботі проведено історичний аналіз становлення та розвитку системи державного забезпечення інформаційної безпеки України, а також здійснено оцінку стану нормативно-правового та інституційного забезпечення інформаційної безпеки України на основі чого обґрунтовано напрями удосконалення цієї системи.

На увагу заслуговують такі наукові результати дослідження Л. Євдоченко як-от:

1) класифікаційна сітка загроз інформаційного характеру;

2) можливі державно-управлінські заходи протидії загрозам

інформаційній безпеці;

3) модель національної інфраструктури захисту інформації.

Вітчизняний дослідник В. Антонюк в дисертаційному дослідженні «Організаційно-правові засади формування та реалізації державної політики інформаційної безпеки України» [9] обґрунтував пропозиції щодо удосконалення державних механізмів розробки і реалізації державної політики інформаційної безпеки Української держави в умовах гібридної війни.

Заслуговує на увагу такі наукові результати В. Антонюка, як-от:

1) уведення в науковий обіг таких понять: «критична інформаційна структура», «об'єкт критичної інформаційної інфраструктури», «спеціальний режим використання інформаційного простору»;

2) структурно-функціональна модель Штабу проведення спеціальних інформаційних операцій Збройних Сил України, що складається із стратегічної, оперативної та тактичної ланок управління;

3) визначено ієрархію керівних документів у сфері забезпечення інформаційної безпеки: Закон – Доктрина – Концепція – Стратегія – державна цільова програма – план;

4) вивчено зарубіжний досвід функціонування механізмів державного реагування на загрози інформаційній безпеці.

В. Антонюк робить висновок, що вітчизняна система забезпечення інформаційної безпеки неспроможна ефективно діяти в сучасних умовах гібридної війни, яку розв'язала рф проти України.

Вітчизняний дослідник Є. Котух в дисертаційному дослідженні «Теоретико-методологічні засади забезпечення кібербезпеки у публічному секторі» [93] обґрунтував пропозиції щодо удосконалення СКБ.

Заслуговує на увагу такі наукові результати Є. Котухи, як-от:

1) обґрунтування концептуальних засад діяльності органів публічної влади гарантування кібербезпеки, з урахуванням поділу вказаної діяльності на дві групи, як-от: людський, організаційний,

інфраструктурний, технологічний, нормативний виміри кібербезпеки; дії у сфері забезпечення кібербезпеки – побудова онлайн-довіри; співпраця, кооперація та координація у сфері забезпечення кібербезпеки; оцінювання стану кібербезпеки; впровадження систем кібербезпеки в практику публічного управління; адаптація нормативно-правової бази в галузі кібербезпеки в контексті вимог динамічного безпекового кіберсередовища; встановлення стандартів діяльності у цій сфері;

2) модель інституційної кібербезпеки компонентами якої є: правові норми; політика, стратегія, стандарти кібербезпеки; безпечна архітектура; кіберстійкість; постійний аудит та моніторинг; співпраця у сфері забезпечення кібербезпеки; управління ризиками, вразливістю, загрозами, інцидентами, логами та кореляція; ситуаційна обізнаність з питань кібербезпеки та освіта; технічні інструменти; безперервність діяльності;

3) теоретико-методологічна модель національної стратегії кібербезпеки, яка розроблена в рамках таких підходи, як: неореалізму, кібервестфалізму, соціального конструктивізму, інтерсекційності;

4) принципи публічно-приватного партнерства з питань гарантування кібербезпеки, а саме: принцип взаємовигідної співпраці партнерів; принцип визначення ролей членів партнерства на основі підходів управління ризиками; принцип спільної відповідальності членів партнерства за стан кібербезпеки; впровадження системи оцінювання партнерства.

Є. Котух робить висновок, що вітчизняна СЗКБ неспроможна адекватно реагувати на кіберзагрози в сучасних умовах російсько-української війни. При цьому, публічний сектор має самий низький рівень кібербезпеки в порівнянні з державним та приватним секторами.

Аналіз захищених дисертацій, що присвячені дослідженню проблем державного й публічного управління інформаційною безпекою та кібербезпекою України, дозволив зробити висновок про недосконаліть правових та інституційних засад забезпечення інформаційної безпеки та

кібербезпеки в умовах динамічного безпекового середовища.

Одинадцяту групу складають праці науковців, котрі розглядають проблеми теорії та практики розбудови систем управління, систем забезпечення інформаційної та кібернетичної безпеки України [3; 31; 51; 56-58; 61; 69; 133-135; 145; 146; 160; 162; 172; 262; 273; 282; 290; 298; 300; 302; 307; 317; 324].

Результати аналізу вказаних наукових публікацій дозволяють констатувати, що проблеми проектування СЗНБ у різних сферах життєдіяльності суспільства, досліджувались у працях таких вітчизняних науковців, як-от:

С. Кримський, котрий обґрунтував методологічні засади проектної діяльності [94, с. 134-147];

Ю. Сурмін, котрий обґрунтував структуру проектної діяльності [205; 206];

В. Абрамов котрий обґрунтував теоретичні засади проектування системи безпеки [1, с. 146-150],

Г. Ситник [193], В. Горбулін та А. Качинський [36; 37], В. Горлинський [38], А. Рачинський [172], котрі обґрунтували теоретико-методологічні засади проектування та конструювання СЗНБ;

О. Левченко [96], М. Шевченко [46. с. 267-269], котрі обґрунтували теоретичні засади проектування системи інформаційної безпеки;

А. Семенченко [181-190], В. Бухарєв [20], І. Діордіца [48], Є. Котух [93], котрі розглянули питання проектування СКБ та СЗКБ;

Д. Костенко [92], котра обґрунтувала теоретичні засади розбудови мережевого управління у сфері національної безпеки;

О. Лук’яненко [103], котра обґрунтувала теоретичні засади проектування механізмів розробки та реалізації соціально-інформаційної політики України;

В. Соколов [198] та Р. Марутян [108-110] котрі обґрунтували теоретичні засади інституалізації аналітичної діяльності в СЗНБ.

Результати аналізу згаданих вище наукових досліджень дозволяє констатувати обмаль праць, в яких розглядалися б питання теоретичних засад проектування СЗКБ України.

У цих працях дослідники вказують на необхідність використання в ході соціального конструювання вказаної системи таких теорій, як: теорії інформаційного суспільства, теорії мережевого суспільства, теорії інформаційного насильства, теорії інформаційної війни, теорії гібридної війни, теорії державного управління, теорії публічного управління, теорії національної безпеки, теорії інформаційної безпеки, теорії кібербезпеки.

Аналіз результатів наукових досліджень цієї групи наукових праць дозволяє констатувати нагальну необхідність удосконалення теоретичних засад розбудови СКБ та СЗКБ з урахуванням сучасних наукових досягнень в галузі безпекознавства, права, політології, державного та публічного управління.

Дванадцяту групу джерел складають наукові та аналітичні дослідження, основною метою якої є розгляд проблем забезпечення кібербезпеки України в умовах гібридної війни. Доцільно передусім назвати роботи таких вітчизняних дослідників, як Р.Марутян [107], О. Леонова [97], О. Сенченко [191], О. Твердохліба [209] та ін.

Аналіз результатів вказаних досліджень дозволяє констатувати, що недостатня визначеність та систематизація проблем формування і реалізації державної політики забезпечення кібербезпеки України в сучасних умовах, підходів до їх розв’язання є перешкодою для формулювання вказаних проблем та їх подальшого розв’язання.

Тринадцяту групу джерел становлять наукові розробки в яких обґрунтовано теоретико-методологічні засади інституціоналізму та системно-діяльнісного підходу.

В нашому дослідженні використано ідеї, які були запропоновані:

Г. Ситником щодо розгляду СНБ як складної політико-правової та організаційно-технічної системи та розгляду СЗНБ як складової СНБ [230,

с. 91];

В. Абрамовим щодо структуризації інституціонального середовища національної безпеки [230, с. 237];

Д. Кучмою щодо натуралістичного та системодіяльнісного підходів до забезпечення національної безпеки [230, с. 58-85].

Використання вказаних ідей дозволило нам здійснити аналіз проблем розбудови та функціонування державних механізмів забезпечення кібербезпеки України, визначити місію та функції СЗКБ, а також дослідити взаємозумовленість, взаємозв'язок і залежність результативності й ефективності СЗКБ від системи знань у цій специфічній сфері, що безпосередньо також впливає на способи організації та побудови практичної діяльності у сфері забезпечення кібербезпеки.

Попередньо підсумуємо: аналіз стану джерел з досліджуваної проблеми свідчить що, вітчизняні науковці досліджують розвиток політики забезпечення кібербезпеки, СКБ, СЗКБ та критерії (характеристики), за допомогою яких визначається ступені розвитку згаданих систем. Проте комплексних досліджень з проблематики розбудови та функціонування державних механізмів забезпечення кібербезпеки на сьогодні обмаль, водночас не в повній мірі приділяється увага дослідників щодо визначення місії, функцій та завдань СЗКБ, прогноз можливих наслідків накопичення проблем забезпечення кібербезпеки для сталого розвитку України.

1.2. Категоріально-понятійний апарат публічно-управлінської проблематики забезпечення кібербезпеки

Категоріально-понятійний апарат публічно-управлінської проблематики у сфері забезпечення кібербезпеки України, перебуває на стадії динамічного розвитку разом із розвитком інформаційної сфери суспільного життя, теорій національної та інформаційної безпеки,

кібербезпеки, публічного управління. Його наукова розробка та наступна імплементація в офіційний дискурс публічного управління національною безпекою є однією з головних проблем вказаного розвитку.

На підставі аналізу результатів актуальних наукових досліджень, енциклопедичної, довідкової літератури [17-21; 40; 48-52; 54-56; 61-65; 69-75; 88; 90-93; 99; 100; 111; 117; 120; 125; 131; 167-171;] можна дійти висновку, що публічно-управлінські проблеми у сфері забезпечення кібербезпеки України, стали об'єктом досліджень філософів, політологів, фахівців з інформаційних технологій та публічного управління. Водночас, не достатньо вивченими залишаються проблеми формування та функціонування механізмів забезпечення кібербезпеки України в сучасних умовах гібридної війни та здійснення Українською державою європейської та євроатлантичної інтеграції.

Проблемами, що стосуються безпосередньо розробки категоріально-понятійного апарату публічно-управлінської проблематики у сфері забезпечення кібербезпеки є:

наявність фактів використання офіційно не визначених термінів в публічно-управлінській практиці забезпечення кібербезпеки;

відсутність системності та координованості дій щодо формулювання та застосування категоріально-понятійного апарату в офіційному дискурсі публічного управління кібербезпекою.

Зазначені проблеми стримують розбудову національної системи кібербезпеки і впровадження сучасних методів, моделей, управлінських технологій в публічно-управлінську практику забезпечення кібербезпеки.

Аналіз керівних документів з питань забезпечення кібербезпеки України [137; 141; 143; 148-150; 152; 153; 154] дозволяє констатувати про сформованість загального розуміння базових категорій кібербезпеки, що є запорукою подальшого розвитку понятійного апарату керівних документів, що регламентують питання забезпечення кібербезпеки України.

Зокрема є розуміння, що кібербезпека – це досить складне соціально-

технічне явище, яке відображає наслідки розвитку та функціонування інформаційної сфери суспільства, накопичений історичний досвід та особливості інформаційної культури конкретного суспільства та держави з питань гарантування безпеки у інформаційно-технологічному вимірі суспільних відносин.

У рамках системно-ситуаційного підходу пропонуємо в системі публічного управління у сфері забезпечення кібербезпеки виокремити кілька страт відповідно до положень стратифікаційної концепції ієрархічного відображення соціальних систем [11, с. 119–125].

Сьома (найвища) страта – це страта процесу діяльності (операційна), що дає змогу забезпечити аналіз та опис процесу публічного управління у сфері забезпечення кібербезпеки.

Шоста страта – страта функції комунікація, яка передбачає аналіз та опис соціально-інформаційних відносин, процесів обміну необхідною та релевантною інформацією між суб’єктами забезпечення кібербезпеки. По суті це партисипаторна функція, що забезпечує взаємодію між органами публічної влади, громадськістю, ІТ-бізнесом з питань забезпечення кібербезпеки.

П’ята страта – страта функції планування, що передбачає аналіз та опис процесу:

визначення цілей СЗКБ загалом, й зокрема механізму запобігання та нейтралізації кризових ситуацій, зумовлених кібернетичним фактором;

механізму державного реагування на загрози кібербезпеці;

вироблення державної політики забезпечення кібербезпеки.

Четверта страта – це страта функції організації забезпечує аналіз та опис багаторівневої організації публічного управління кібербезпекою.

Третя страта – страта функції мотивації, яка передбачає аналіз та опис відповідних мотиваційних механізмів діяльності у сфері забезпечення кібербезпеки на всіх рівнях публічного управління.

Друга страта – це страта функції прийняття публічно-управлінських

рішень, що забезпечує аналіз та опис процесів прийняття вказаних рішень.

Перша страта – страта функції контролю, яка передбачає аналіз та опис запровадження методів і засобів отримання та оцінки інформації щодо стану досягнення цілей публічного управління у сфері забезпечення кібербезпеки, політики забезпечення кібербезпеки й, насамкінець стану кібербезпеки, а також формування вектора коригуючих публічно-управлінських впливів на процеси забезпечення кібербезпеки.

На рівні першої страти процесу публічно-управлінської діяльності розглянемо висхідну низку категорій і понять, що формують концептуальну канву публічного управління кібербезпекою.

Такими категоріями та поняттями є: категорії «діяльність», «держава», «безпека», понять «державне управління», «механізми державного управління», «функції держави», «національна безпека», «кібербезпека».

Аналіз наведених у вітчизняному науковому дискурсі визначень категорій «діяльність» [54, с. 172], «держава» [54, с. 141–142], «безпека» [40, с. 13–17], понять «державне управління» [54, с. 150], «механізми державного управління» [54, с. 421], «функції держави» [54, с. 744–745], «національна безпека» [40, с. 67-70], «механізм забезпечення національної безпеки» [56, с. 372-373], кібербезпека [48; 99; 100; 111] дозволяють нам підсумувати: більш точно кібербезпеку в державно-управлінському вимірі можна розглядати як властивість збереження цілісності національного кібернетичного простору.

Є сенс зауважити, що поняття «кібербезпека» у вітчизняному науковому дискурсі [48; 99; 100; 111] сформульоване в рамках захисної парадигми національної безпеки [38, с. 220]. Ми вважаємо, що для потреб нашого дослідження визначення поняття «кібербезпека» потребує уточнення власне в категоріальній сітці науки «Публічне управління та адміністрування» з урахуванням не лише захисної парадигми національної безпеки, а й парадигми розвитку, а також трансформацій безпекового та

інформаційно-технологічного середовища України на сучасному етапі державотворення [20; 210; 229], субстанційної властивості безпеки [38, с. 73-74], законів безпечного та соціального розвитку держави [36, с. 42-43]. Зокрема, на думку, В. Горлинського субстанційна властивість безпеки – це властивість збереження сталості існування предмету, явища або процесу, яка утворюється реальним функціонуванням істотних зв'язків. При цьому, вказана властивість виражає первинну, інтеграційну функцію безпеки – функцію забезпечення просторово-часової і функціональної усталеності існування предмету, явища або процесу [38, с. 73-74].

З урахуванням вище зазначеного під поняттям «кібербезпека» пропонуємо розуміти:

1) властивість збереження цілісності національного кіберпростору в умовах небажаного деструктивного інформаційно-технологічного впливу вороже налаштованих суб'єктів міжнародних інформаційних відносин до ідеї незалежності конкретної національної держави, її інформаційного та кібернетичного суверенітету;

2) створення умов для реалізації життєво важливих інтересів суспільства у кібернетичній сфері в контексті досягнення офіційно визначених національних цілей суспільного розвитку.

Соціально-психологічний механізм усвідомлення проблем забезпечення кібербезпеки – це форма сприйняття суб'єктами забезпечення кібербезпеки актуальних проблем збереження цілісності національного кіберпростору та гарантування цифрового суверенітету, спосіб розподілу цих проблем на смислові утворення, які визначають поведінку згаданих суб'єктів.

У рамках страти функції «комунікація» проведено аналіз та опис процесів соціально-інформаційних відносин та обміну необхідною та релевантною інформацією між суб'єктами забезпечення кібербезпеки.

На рівні цієї страти вибудуємо висхідний ряд категорій та понять за допомогою яких формується структурно-логічна модель реалізації функції

«комунікація» в публічному управлінні кібербезпекою, а саме: категорія «взаємодія», поняття «комунікація», «забезпечення».

Використовуючи напрацювання В. Козакова у царині аналізу основних дефініцій категорії «взаємодія» [87, с. 227] під управлінською взаємодією у сфері забезпечення кібербезпеки будемо розуміти зусилля суб'єктів забезпечення кібербезпеки в напрямі досягнення офіційно визначених національних цілей у цій специфічній сфері. У рамках нашого дослідження такими цілями є своєчасне виявлення загроз кібербезпеці, реактивна та проактивна протидія виявленим загрозам з метою гарантування цілісності національного кіберпростору.

У рамках стратифікаційної концепції відображення соціальних систем розглянемо зміст поняття «комунікація».

В науці «Державне управління» функція комунікації трактується як обмін необхідною та релевантною інформацією для прийняття виважених державно-управлінських рішень, доведення їх до учасників процесу управління, забезпечення зворотнього інформаційного зв'язку з об'єктом управління [11, с. 124].

Виходячи з концепції поділу діяльності на три складові, а саме: основну, управлінську та забезпечувальну [54, с. 163] розглянемо зміст поняття «забезпечення національної безпеки».

На думку вітчизняного дослідника Д. Кучми, поняття «забезпечення» належить до особливого роду відносин між системами або підсистемами діяльності, коли одна з них передає іншій або породжує в ній певні організованості або підсистеми, які необхідні для її функціонування та розвитку. Тобто, забезпечення є особливою функцією та особливим фокусуванням управлінської діяльності щодо подолання розривів в організації діяльності шляхом усунення вказаних розривів та налагодження необхідних кооперативних або комунікативних зв'язків [230, с. 83].

Кажучи про «забезпечення» Д. Кучма дає відповідь на чотири

питання: хто забезпечує, що забезпечується, чим та за рахунок чого забезпечується:

1) забезпечується оргуправлінець, оскільки «забезпечення» – це його функція й водночас назва його діяльності щодо реалізації цієї функції;

2) забезпечується система діяльності – рецепієнт;

3) забезпечується результатами та продуктами діяльності системи-донора;

4) забезпечується за рахунок діяльності оргуправлінця [230, с. 84].

На думку вітчизняного дослідника Д. Кучми, система забезпечення безпеки здійснює такі комплекси процедур, як-от:

1) інвентаризація безпекознавчих знань, а саме знань про безпекове середовище та систему реагування на загрози різного характеру – потенційні та реальні загрози безпеці;

2) розробка заходів проактивного реагування на загрози на основі аналізу причин та джерел виникнення потенційних загроз, прогнозної моделі загроз;

3) перегляд знань про безпекове середовище та систему реактивного реагування з урахуванням вже існуючих реальних загроз;

4) розробка й здійснення заходів реактивного й проактивного реагування на основі нових знань у сфері безпеки [230, с. 81–85].

Структурно-логічну модель реалізації функції «комунікація» в публічному управлінні кібербезпекою відображено на рис. 1.1.

У рамках страти функції «планування» проведемо аналіз та опис процесу визначення цілей та місій СКБ та СЗКБ, вироблення політики забезпечення кібербезпеки як основи державного реагування у цій сфері в умовах деструктивного впливу інформаційно-технологічного чинника.

Рис. 1.1. Структурно-логічна модель реалізації функції «комунікація» в публічному управлінні кібербезпекою

На рівні цієї страти розглянемо висхідну низку понять, що формують структурно-логічну модель реалізації функції «планування» в публічному управлінні кібербезпекою. Такими поняттями є: «система кібербезпеки», «система забезпечення кібербезпеки», «політика забезпечення кібербезпеки».

Під поняттям «система кібербезпеки» пропонуємо розуміти упорядковану багаторівневу та багатоструктуровану сукупність елементів системи суспільно-інформаційних відносин, функціонування яких створює в суспільстві умови для реалізації життєво важливих національних інтересів у кібернетичній сфері і системної захищеності національного кібернетичного простору як запоруки інформаційного розвитку суспільства.

Ми погоджуємося з думкою А. Семенченка, що ефективна СЗНБ має функціонувати в трьох режимах: загальному режимі повсякденного функціонування (реагування на виклики, небезпеки, загрози), раціональному режимі (режимі розвитку) та антикризовому режимі [181, с. 110].

З урахуванням вище зазначеного під поняттям «система забезпечення кібербезпеки» пропонуємо розуміти сукупність органів публічної влади, формальних і неформальних громадських структур, ІТ-компаній, а також правових, політичних, соціальних та інших зв'язків між ними, механізмів, інструментів, технологій за допомогою яких підтримується цілісність і захищеність національного кіберпростору, а також реалізовуються заходи проактивної та реактивної протидії потенційним та реальним загрозам кібербезпеці. Тобто, СЗКБ охоплює два контури публічного управління кібербезпекою – реактивне й проактивне реагування на загрози кібербезпекия. Реактивна протидія має здійснюватися на стратегічному, оперативно-стратегічному та оперативному рівнях управління, проактивна протидія, як правило на стратегічному рівні.

Під поняттям «державна політика забезпечення кібербезпеки» пропонуємо розуміти:

1) систему принципів, підходів та практичних заходів держави, спрямованих на регулювання суспільно-інформаційних відносин в контексті забезпечення просторово-часової і функціональної усталеності існування національного кіберпростору;

2) політичну діяльність суб'єктів суспільства, а також спеціально уповноважених органів, яка спрямована на реалізацію національних інтерсів у інформаційній сфері суспільства, організацію системного захисту національного кіберпростору.

У моделі функції «Планування» виокремимо дві основні напрями дій:

постановка цілей у відповідній сфері діяльності;

вибір способів досягнення поставлених цілей [11, с. 126].

Структурно-логічну модель реалізації функції «планування» публічного управління кібербезпекою представлено на рис. 1.2.

У рамках страти функції «організація» зробимо аналіз та опис

процесу багаторівневої організації публічного управління кібербезпекою.

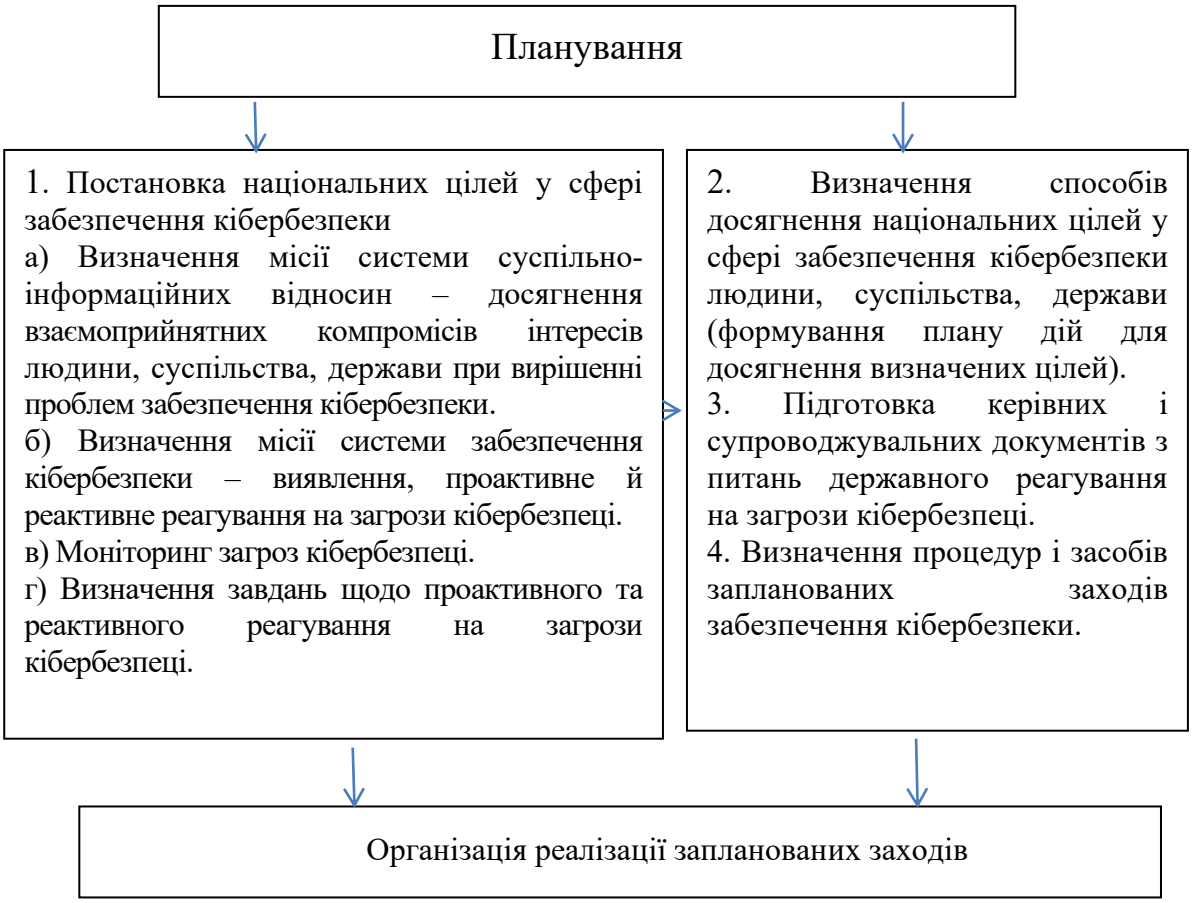

Рис. 1.2. Структурно-логічна модель реалізації функції «планування» в публічного управління кібербезпекою

На рівні цієї страти розглянемо висхідну низку понять, що формують структурно-логічну модель реалізації функції «організації» публічного управління кібербезпекою. Такими поняттями є: «державно-політичний механізм забезпечення кібербезпеки», «правовий механізм забезпечення кібербезпеки», «система розроблення та реалізації політики забезпечення кібербезпеки», «механізм розробки політики забезпечення кібербезпеки», «комплексний механізм реалізації політики забезпечення кібербезпеки», «механізми забезпечення кібербезпеки», «технологія державного реагування на загрози кібербезпеці», «механізм державного

реагування на загрози кібербезпеці».

Державно-політичний механізм забезпечення кібербезпеки – це сукупність процесів, які ініційовані і реалізуються органами державної влади комплексна дія яких стосовно суспільно-інформаційних відносин та задоволення інформаційних потреб людини, суспільства, держави репрезентувала свій кінцевий результат у вигляді теоретичного обґрунтування правових засад розробки та реалізації політики забезпечення кібербезпеки.

Правовий механізм забезпечення кібербезпеки – це нормативно-правова база забезпечення кібербезпеки.

Інституційний механізм забезпечення кібербезпеки – це інституціональні елементи, які представляють суб'єктів забезпечення кібербезпеки, корті мають різний статус та різні повноваження у процесах забезпечення кібербезпеки.

Систему розроблення та реалізації політики забезпечення кібербезпеки пропонуємо представити механізмами розробки та реалізації вказаної політики.

Систему розроблення та реалізації політики забезпечення кібербезпеки можна визначити через поняття «цикл політики», до якого належать такі фази [21, с. 42]:

1) визначення проблеми забезпечення кібербезпеки;

2) формування політики забезпечення кібербезпеки;

3) вибір найприйнятнішого варіанту політики забезпечення кібербезпеки в конкретних умовах;

4) проектування політики забезпечення кібербезпеки;

5) упровадження політики забезпечення кібербезпеки та моніторинг процесу її здійснення;

6) оцінювання політики забезпечення кібербезпеки.

Механізм розробки державної політики забезпечення кібербезпеки пропонуємо представити у вигляді трьохрівневої конструкції:

1) на соціально-політичному рівні вказаний мезанізм представлявляє собою політичну діяльність, яка спрямована на визначення національних цілей у сфері забезпечення кібербезпеки, а також напрямів та принципів діяльності у вказаній сфері;

2) на структурно-організаційному рівні рівні вказаний мезанізм представлявляє собою систему інституцій, які визначають національні цілі у сфері забезпечення кібербезпеки, напрями та принципи діяльності у цій сфері;

3) на технологічному рівні вказаний мезанізм може бути представлений сукупністю методів та технологій, за допомогою яких визначаються цілі, напрями та принципи діяльності у сфері забезпечення кібербезпеки.

Механізм розробки політики забезпечення кібербезпеки включає в себе пакет:

концептуально-настановчих документів з питань захисту прав людини та основних її свобод у інформаційній сфері;

нормативно-правову базу з питань кібербезпеки і суспільно-інформаційних відносин;

систему прийняття рішень у сфері кібербезпеки, систему програмно-цільового планування заходів забезпечення кібербезпеки.

До суб’єктів розробки політики забезпечення кібербезпеки належать органи закододавчої та виконавчої влади, а також різні суб’єкти політичного процесу, громадські організації, ІТ-команії.

Під комплексним механізмом реалізації політики забезпечення кібербезпеки пропонуємо розуміти:

1) на соціально-політичному рівні – сукупність процесів, ініційованих і реалізованих органами публічної влади, громадянським суспільством, ІТ-компаніями через наявні інструменти публічного управління, комплексна дія яких дозволяє досягти взаємоприйнятного компромісу в реалізації корпоративних та загальнонаціональних цілей у

сфері кібербезпеки;

2) на структурно-організаційному рівні – процес спільної діяльності органів державної влади, що опікуються питаннями кібербезпеки, відповідних сил сектору безпеки і оборони, інституцій громадянського суспільства, інституцій ІТ-бізнесу, яка спрямована на досягнення цілей, які визначені у програмі державної політики забезпечення кібербезпеки;

3) на технологічному рівні – це сукупність методів та технологій публічно-управлінської діяльності, які застосовуються з метою реалізації цілей політики забезпечення кібербезпеки.

Зауважимо, комплексний механізм реалізації політики забезпечення кібербезпеки структурно включає в себе:

організаційно-адміністративний, кадровий, науково-методичний, інформаційний, інформаційно-аналітичний, фінансовий механізми забезпечення кібербезпеки;

механізми державного реагування на загрози кібербезпеці та інформаційно-технологічного забезпечення вказаного реагування;

механізми міжнародного і міждержавного співробітництва у сфері забезпечення кібербезпеки;

механізм інтеграції національного кіберпростору у світовий кіберпростір;

механізм забезпечення управлінської взаємодії суб’єктів забезпечення кібербезпеки;

механізм забезпечення комунікації суб’єктів забезпечення кібербезпеки;

механізм партисипаторної взаємодії у сфері забезпечення кібербезпеки.

Організаційно-адміністративний механізм забезпечення кібербезпеки – це сукупність офіційно визначених правил і процедур діяльності суб’єктів забезпечення кібербезпеки згідно вимог чинного законодавства у цій сфері.

Фінансовий механізм забезпечення кібербезпеки – це форми й методи створення і використання фінансових ресурсів суб'єктами забезпечення кібербезпеки відповідно до своїх повноважень.

Кадровий механізм забезпечення кібербезпеки – це системна сукупність освітніх програм та інституцій професійної освіти, що забезпечує підготовку і перепідготовку фахівців у сфері кібербезпеки.

Науково-методичний механізм забезпечення кібербезпеки – це:

1) системна сукупність науково-дослідних установ діяльність яких спрямована на: напрацювання науково-методичної бази впровадження стандартів та протоколів НАТО по забезпеченню кібербезпеки; розробку новітніх технологій забезпечення кібербезпеки України та унормування їх використання на законодавчому рівні;

2) сукупність процесів, які ініційовані та реалізуються науковими установами за участю суб'єктів забезпечення кібербезпеки з метою синтезу знань про кіберзагрози та формування бази релевантних знань задля адекватного та своєчасного реагування на них.

Інформаційно-аналітичний механізм забезпечення кібербезпеки – це:

1) системна сукупність інформаційно-аналітичних підрозділів діяльність яких спрямована на інформаційно-аналітичне забезпечення кібербезпеки;

2) сукупність процесів діагностування й прогнозування суб'єктами забезпечення кібербезпеки тенденцій розвитку кіберзагроз, розробки ними варіантів рішень щодо реагування на виявлені кіберзагрози та оцінки наслідків прийнятих рішень в інтересах гарантування кібербезпеки.

Механізми міжнародного й міждержавного співробітництва з питань забезпечення кібербезпеки мають на меті організацію співробітництва з міжнародними структурами безпеки та державами-партнерами з питань гарантування кібербезпеки з урахуванням впливу чинника інформаційної глобалізації.

Механізм інтеграції національного кіберпростору у світовий

кіберпростір передбачає реалізацію національної моделі входження України у світовий інформаційний простір відповідно вимог міжнародного права та чинного національного законодавства з питань інформаційного розвитку суспільства та гарантування інформаційної безпеки й кібербезпеки.

Механізм партисипаторної взаємодії у сфері забезпечення кібербезпеки передбачає організацію та здійснення громадської взаємодії органів державної влади з громадськими організаціями та ІТ-бізнесом з питань забезпечення кібербезпеки.

Механізм інформаційного забезпечення кібербезпеки – це сукупність процесів, які ініційовані та реалізуються суб'єктами забезпечення кібербезпеки з метою надання посадовим особам СЗКБ відомостей, необхідних для виконання покладених на них завдань у сфері забезпечення кібербезпеки та інформаційного супроводження політики забезпечення кібербезпеки.

Механізм забезпечення управлінської взаємодії суб'єктів забезпечення кібербезпеки – це ініційовані та реалізовані суб'єктами забезпечення кібербезпеки процеси, що спрямовані на створення умов для інтеграції зусиль керівництва органів публічної влади щодо своєчасного та адекватного реагування на кіберзагрози згідно єдиного задуму гарантування кібербезпеки.

Механізм забезпечення комунікації суб'єктів забезпечення кібербезпеки – це сукупність процесів, які ініційовані і реалізуються суб'єктами забезпечення кібербезпеки задля створення умов їхньої інформаційної взаємодії з питань забезпечення кібербезпеки.

Механізм інформаційно-технологічного забезпечення реагування на загрози кібербезпеці – це сукупність процесів, які ініційовані й реалізовані суб'єктами забезпечення кібербезпеки задля створення умов безпечного використання інформаційних та аналітичних технологій в ході реагування на кіберзагрози.

Зауважимо, що в офіційному дискурсі публічного управління кібербезпекою поняття «механізм державного реагування на загрози кібербезпеці», «технологія державного реагування на загрози кібербезпеці» відсутні.

Враховуючи вище зазначене під поняттям «механізм державного реагування на загрози кібербезпеці» пропонуємо розуміти сукупність елементів нормативного й інституційного характеру, які спрямовані на: попередження, запобігання загрозам кібербезпеці; мінімізацію рівня існуючих загроз кібербезпеці; локалізацію і ліквідацію наслідків реалізації загроз кібербезпеці.

Механізмами державного реагування на виклики та загрози кібербезпеці є:

1) механізм проактивного реагування на загрози кібербезпеки – це сукупність процесів, які ініційовані і реалізуються органами державної влади комплексна дія яких стосовно конфліктів у кіберсфері репрезентувала свій кінцевий результат у вигляді теоретичного обґрунтування і практичного забезпечення спрямованості етапів запобігання та врегулювання конфліктів у кіберсфері;

2) механізми реактивного реагування на загрози кібербезпеці – це сукупність процесів, які ініційовані і реалізуються органами державної влади комплексна дія яких стосовно загроз кібербезпеці репрезентувала свій кінцевий результат у вигляді мінімізації існуючих загроз, локалізації і ліквідації наслідків їх реалізації.

Використовуючи результати науковго дослідження [223] сформулюємо визначення поняття «технологія державного реагування на загрози кібербезпеці». Під останнім будемо розуміти цілеспрямовану послідовність робочих операцій суб’єктів забезпечення кібербезпеки, яка за допомогою відповідних методів і засобів впливу на об’єкт кібербезпеки дає змогу попередити і запобігти небезпекам, на стадії їх зародження, а

також мінімізувати існуючі загрози, локалізувати і ліквідувати наслідки їх реалізації. До структури цієї технології входять такі елементи:

теоретична концепція державного реагування на загрози кібербезпеці;

об’єкт державно-управлінського впливу, що спрямований на його захист або регульовання рівня виявлених загроз;

головний суб’єкт забезпечення кібербезпеки; предмет державно-управлінського впливу – конкретна сторона об’єкта кібербезпеки на яку спрямовано вплив;

алгоритм попередження і запобігання небезпекам, на стадії їх зародження, мінімізації існуючих загроз кібербезпеці;

алгоритм призупинення дій загрози на об’єкт кібербезпеки;

алгоритм локалізації та нейтралізації наслідків реалізації загроз кібербезпеці;

технологічні способи і засоби державного реагування на загрози кібербезпеці;

контроль досягнутого результату державного реагування на загрози кібербезпеці.

Структурно-логічну модель реалізації функції «організація» в публічному управлінні кібербезпекою представлено на рис. 1.3.

За результатами аналізу процесу мотиваційних механізмів на всіх рівнях публічно-управлінської діяльності у сфері забезпечення кібербезпеки нами побудовано модель реалізації функції «мотивація». У цій моделі наглядно представлено механізм мотивації суб’єктів забезпечення кібербезпеки – спонукальні чинники діяльності згаданих суб’єктів (див. рис. 1.4).

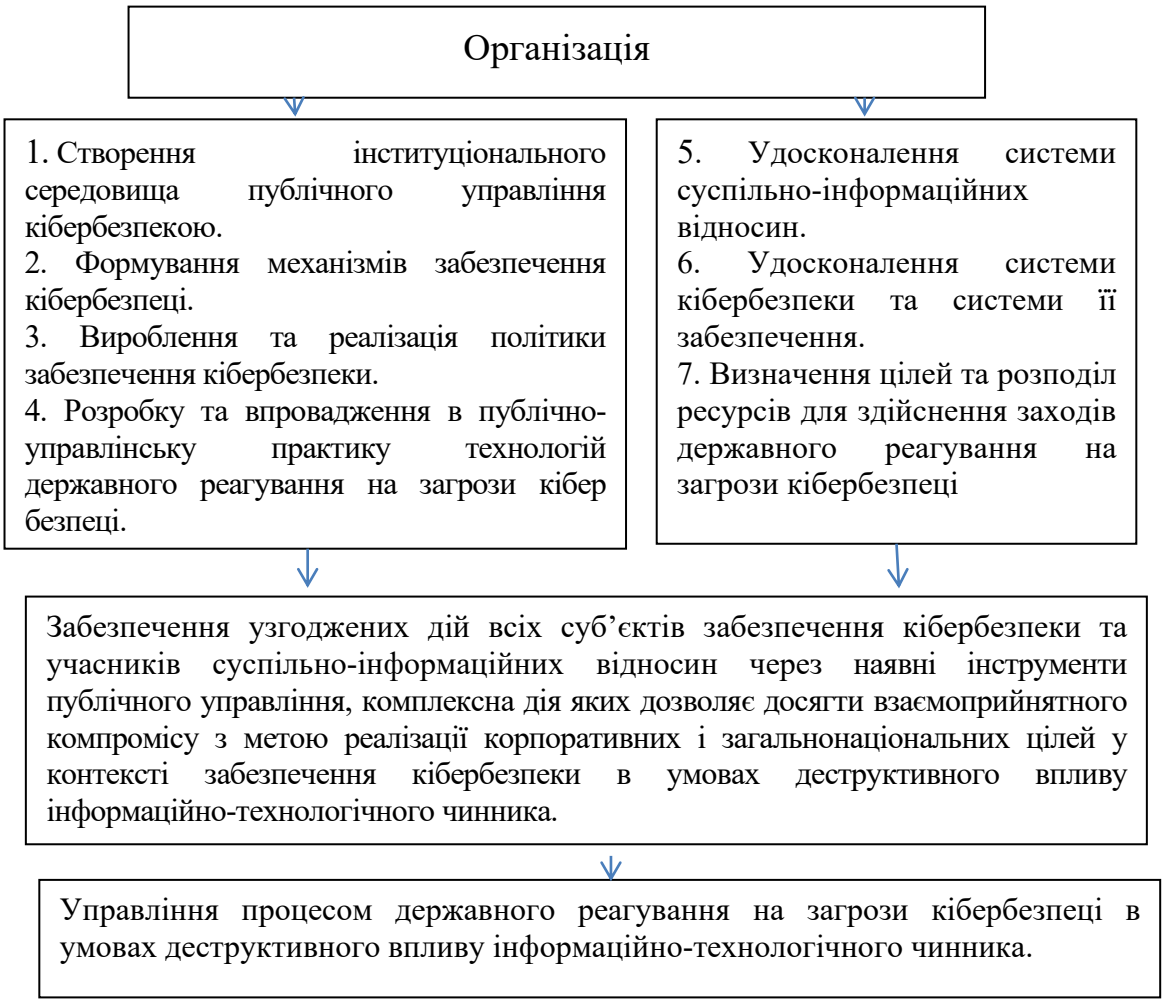

Рис. 1.3. Структурно-логічна модель реалізації функції «організація» в публічному управлінні кібербезпекою

За результатми аналізу процесів розробки й прийняття публічно-управлінських рішень, нами побудовано модель реалізації функції «прийняття публічно-управлінських рішень». У цій моделі відображено алгоритм прийняття рішення щодо досягнення цілей політики забезпечення кібербезпеки (див. рис. 1.5).

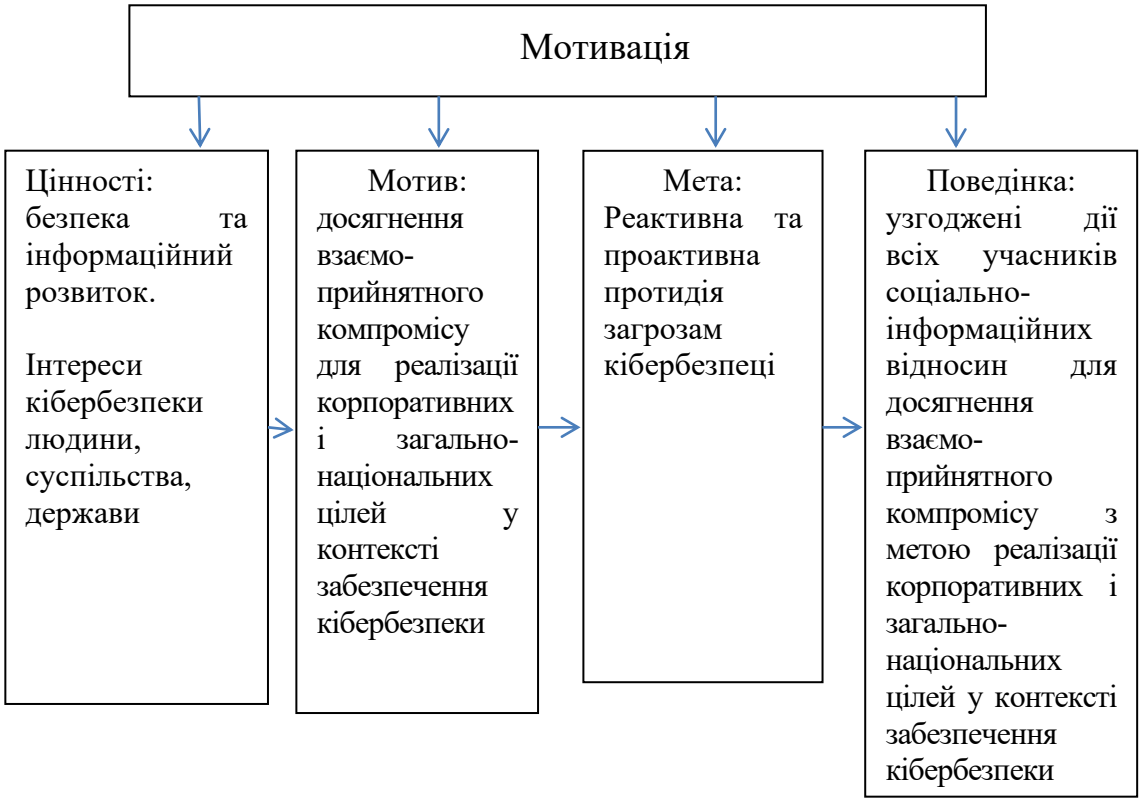

Рис. 1.4. Структурно-логічна модель реалізації функції «мотивація» в публічному управлінні кібербезпекою.

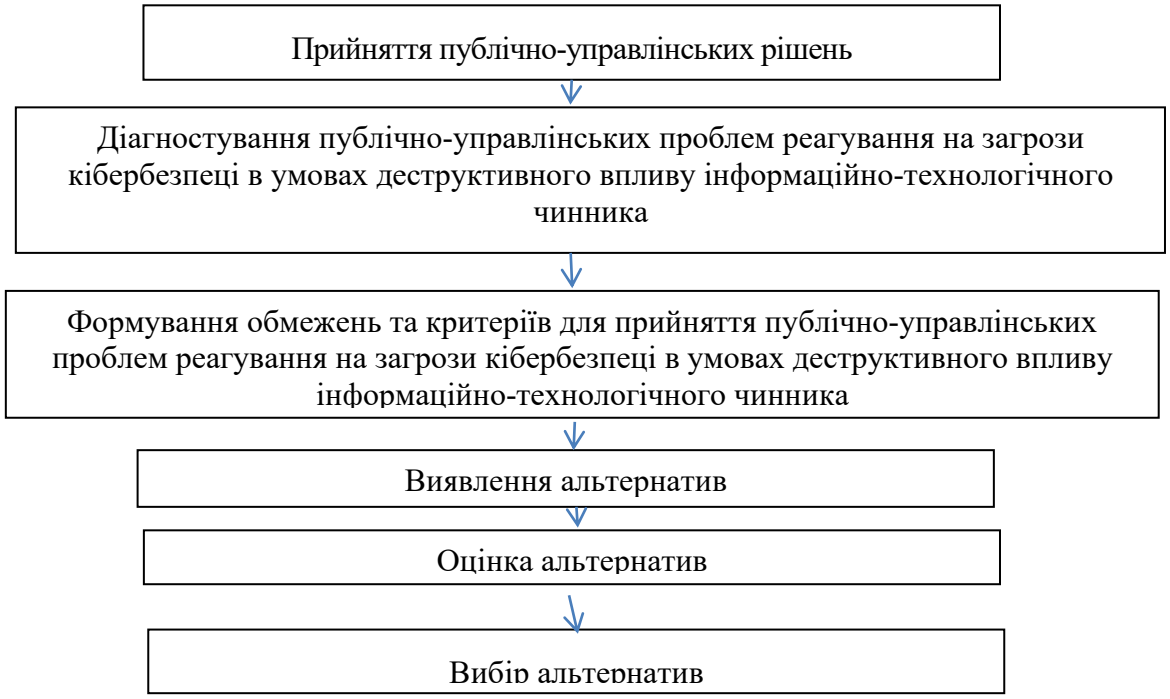

Рис. 1.5. Структурно-логічна модель реалізації функції «прийняття публічно-управлінських рішень» в кризових ситуаціях, зумовлених інформаційно-технологічним чинником

За результатми аналізу процесу контролю в публічному управлінні кібербезпекою нами побудовано модель реалізації функції «контроль». У цій моделі відображено алгоритм контролю результатів досягнення цілей державного реагування на загрози кібербезпеці в умовах деструктивного впливу інформаційно-технологічного чинника (див. рис. 1.6).

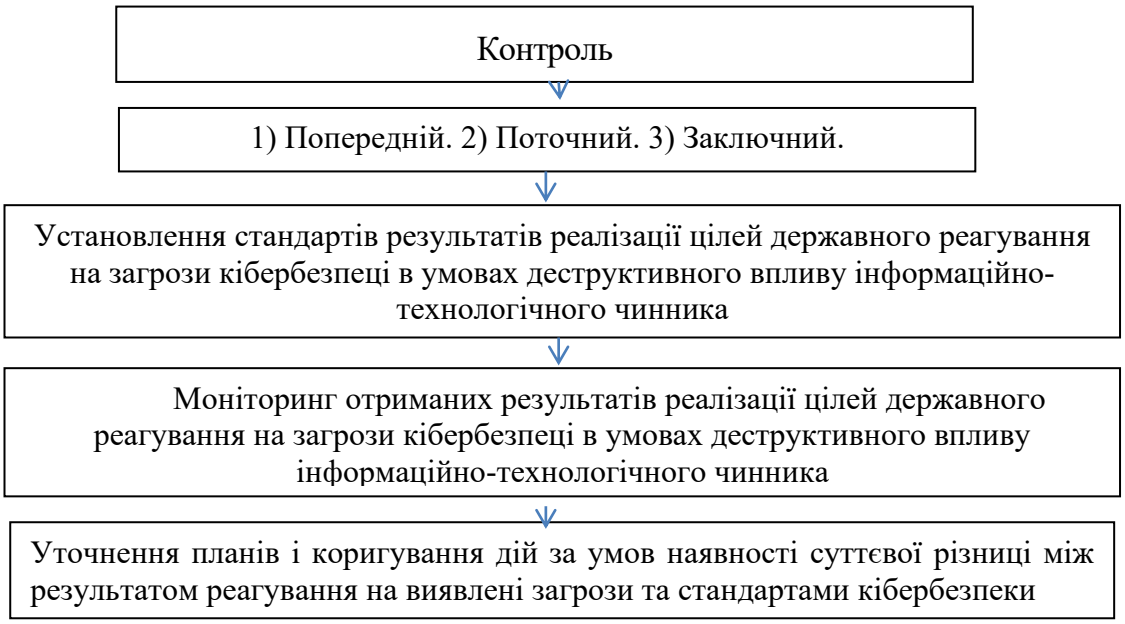

Рис. 1.6. Структурно-логічна модель реалізації функції «контроль» у публічному управлінні кібербезпекою

Отже, визначені категорії та поняття проблематики забезпечення кібербезпеки характеризують публічно-управлінський процес як ціле, що взяте в одному із вимірів управлінської діяльності. Тобто дійсність публічного управління кібербезпекою є динамічною багатогранною цілісністю, адекватне вираження якої можливе лише в самій динаміці й цілісній системі категорій і понять галузі знань «Публічне управління і адміністрування».

1.3. Теоретичні засади розроблення та функціонування державних механізмів забезпечення кібербезпеки

На сучасному етапі державного будівництва в Україні, що характеризується веденням проти Української держави гібридної війни та повномасштабним вторгненням рф, існує нагальна потреба в гарантуванні кібербезпеки України. Це, у свою чергу, зумовлює нагальну необхідність удосконалення СКБ та механізмів забезпечення кібербезпеки з урахуванням динамічності безпекового середовища, що зумовлено перебігом подій російсько-української війни.

Аналіз результатів наукових досліджень [1; 9; 18; 20; 33-39; 48; 51; 59-68; 70-75; 88; 90-93; 95-101; 210-212; 228-231] дозволяє констатувати, що формування СКБ, СЗКБ, механізмів забезпечення кібербезпеки здійснюється в рамках загальної теорії систем, теорії державного управління, теорії публічного управління, теорії національної безпеки, теорії інформаційної безпеки, теорії кібербезпеки, теорії гібридної війни, теорій інформаційної та кібернетичної війн, теорії інституціональних матриць, теорії стратегічного планування у сфері національної безпеки, теорії проектування систем управління.

Згідно теорії інституціоналізму, в структурі інституціонального середовища виокремлюють нормативну підсистему (норми і правила) та організаційно-технічну підсистему (установи та організації) [16]. В науковому дискурсі основними характеристиками згаданого середовища визначено: щільність, ієрархічна структура, організація [16, с. 225]. До основних компонентів інституціонального середовища державного управління національною безпекою відносяться: нормативно-правовий, організаційний, самоорганізаційний, соціально-культурний, когнітивний [230, с. 237].

Зазначимо, що інституціональне середовище публічного управління кібербезпекою є основою формування структури публічного управління у

згаданій сфері. При цьому кожен компонент інституціонального середовища публічного управління повинен розглядатися як системний об’єкт, який динамічно розвивається і має відповідну структуру, власні функції, цілі і завдання в процесах забезпечення кібербезпеки, активно взаємодіє з іншими компонентами інституціонального середовища публічного управління та безпекового середовища.

Факторами, які визначають виникнення та динаміку розвитку СКБ є:

причини геополітичного інформаційного протиборства;

зовнішні та внутрішні рушійні сили, які спричиняють зміни у інституціональному середовищі публічно-управлінської діяльності у сфері забезпечення кібербезпеки, а саме зміни інституціональної матриці діяльності у сфері забезпечення кібербезпеки. Остання містить базові соціальні інститути – економіку, політику, культуру (ідеологію). Ці соціальні інститути утворюють своєрідні внутрішні жорсткі структури інтеграції суспільства. При цьому специфіка змісту базових інститутів визначається культурним контекстом даного суспільства [16, с. 274].

Зауважимо, що в теорії інституціональних матриць виокремлюють такі матриці, як-от:

X-матриця (західна, ринкова);

Y-матриця (східна, командно-адміністративна);

Z-матриця (перехідна, солідарна).

Вітчизняна дослідниця О. Бортнікова інституціональні матриці охарактеризувала наступним чином:

для X-матриці притаманним є державне управління;

для Y-матриці притаманним є публічне управління;

для Z-матриці притаманним є системне управління [16, с. 275-280].

Зауважимо, що під інституціональним середовищем публічного управління кібербезпекою будемо розуміти системну сукупність нормативно-правових, організаційних та самоорганізаційних, соціально-культурних, когнітивних, технологічних правил і норм (інститутів), що

визначають поведінку суб'єктів забезпечення кібербезпеки та взаємовідносини між ними. Вказане середовище є основою формування структури публічного управління кібербезпекою. Кожен компонент інституціонального середовища публічного управління кібербезпекою повинен розглядатися як системний об'єкт, який розвивається відповідно до вимог динамічного безпекового середовища і має відповідну внутрішню структуру, в якій можна виокремити нормативно-правовий, організаційний, самоорганізаційний, соціально-культурний, когнітивний компоненти [230, с. 237]. Основними характеристиками вказаного інституціонального середовища є щільність, ієрархічна структура та організація [16, с. 225].

Факторами, які визначають виникнення та динаміку розвитку механізмів забезпечення кібербезпеки є зміни в безпековому та управлінському середовищі, а саме:

1) інституціональна матриці, що містить такі базові соціальні інститути, як економіку, політику, культуру [16, с. 274], що визначальним чином впливають на формування публічно-управлінського у сфері кібербезпеки як сукупності політичних інститутів та інститутів кібербезпеки, а також кіберпростору національної держави;

2) зовнішнє інституціональне середовище публічного управління кібербезпекою України, яке охоплює собою два середовища:

а) інституціональне середовище публічного управління кібербезпекою суспільно-інформаційних відносин у якому здійснюється взаємодія між суб'єктами забезпечення кібербезпеки;

б) інституціональне середовище регулювання суспільно-інформаційних відносин у якому здійснюється інституціональне, організаційне, правове (державне) регулювання. При цьому, інституціональне середовище суспільно-інформаційних відносин функціонує на макро-, мезо-, мікро- і нано- рівнях, яким притаманні свої характерні особливості регулювання;

3) внутрішнє інституціональне середовище публічного управління кібербезпекою України, яке охоплює собою два середовища:

а) інституціональне середовище кібербезпеки;

б) інституціональне середовище державного реагування на виклики та загрози кібербезпеці.

Під впливом внутрішнього інституціонального середовища формується інституціональна матриця публічного управління кібербезпекою.

В рамках нашого дослідження в другому розділі акцентуємо увагу на впливі базових соціальних інститутів на формування інституціонального середовища публічного управління кібербезпекою.

В рамках теорії стратегічного планування у сфері національної безпеки процес проектування системи забезпечення кібербезпеки (СЗКБ) починається із визначення місії вказаної системи. Після цього визначаються цілі СЗКБ для встановлення меж майбутніх можливостей і точки відліку, відносно якої оцінюється потреба в інформації, необхідної для оцінки цих майбутніх можливостей. Наступний крок – прогнози зовнішнього оточення, погляд у майбутнє, що дає змогу плановикам побудувати модель ймовірного майбутнього стану зовнішнього середовища з відображенням характеру соціальних, економічних, політичних, правових і науково-технічних факторів, з якими силам СЗКБ прийдеться мати справу в майбутньому. На думку А. Семенченка, модель майбутнього може бути використана як основа оцінки і вибору стратегічних цілей [182]. Етап вибору цілей включає уточнення, деталізацію і конкретизацію раніше сформульованих попередніх цілей, що надає напрями подальшого планування (див. рис. 1.7.).

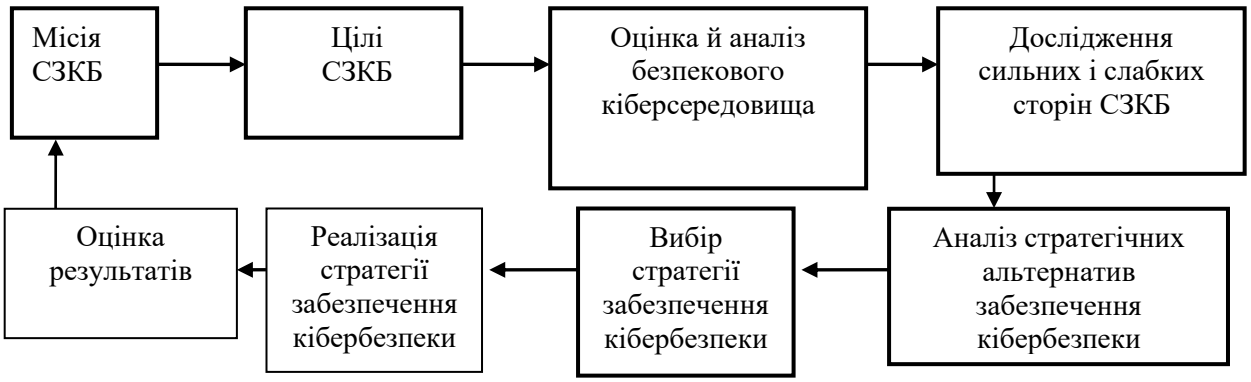

Рис. 1.7. Процес стратегічного планування у сфері кібербезпеки

Наступний етап процесу – визначення й оцінка альтернативних способів використання наявних ресурсів для досягнення поставлених цілей СЗКБ, тобто прийняття рішення про найкращий напрям розвитку сил СЗКБ при заданих обмеженнях і майбутніх умовах. Оцінка альтернатив при використанні методу «витрати-ефективність» повинна здійснюватися на основі раніше обраних цілей і, отже, приводити до вибору альтернатив, співрозмірних цим цілям. Поряд з оцінками ризику і невизначеності, альтернативи утворять ядро стратегічного планування у сфері кібербезпеки. Для того, щоб альтернативи були змістовними, їх варто оцінювати відповідно до того, що повинно бути зроблене і що може бути зроблено, виходячи з заданих цілей і можливих факторів ризику [182].

Після того як обрані цілі й оцінені альтернативи, основну увагу в процесі розробки планів зосереджують на забезпеченні несуперечності цілей і альтернатив, підготовлених різними силам СЗКБ і для різних видів діяльності.

На основі аналізу результатів наукових досліджень проблематики державного управління національною безпекою та публічного управління [168, с. 96-97; 211], державної політики національної безпеки та публічної політики [167, с. 139; 221], забезпечення національної безпеки [167, с. 87; 169, с. 183-185], державної політики забезпечення кібербезпеки [48; 51], глобальних трансформацій у сфері інформаційного протиборства [9; 30;

50], нами визначено структуру СКБ (див. рис. 1.8).

Першим структурним елементом СКБ є соціально-психологічний механізм усвідомлення проблем забезпечення кібербезпеки, який передбачає створення умов для соціальної взаємодії у сфері забезпечення кібербезпеки, яка поляризується позиціями різних соціальних груп стосовно важливості проблем кібербезпеки. Вона включає сукупність дій та заходів за напрямами:

створення умов для рефлексії проблем кібербезпеки в українському суспільстві;

створення умов для готовності українського суспільства щодо підтримки офіційно визначеного курсу державної політики забезпечення кібербезпеки.

Другим елементом СКБ є державно-політичний механізм, який відображає:

процес усвідомлення політичним керівництвом держави проблематики взаємодії політики і кібернетичної сфери, а також необхідності впорядкування національного кібернетичного простору та гарантування кібербезпеки;

процес визначення концептуальних та організаційно-правових засад суспільно-інформаційних відносин, гарантування прав і свобод громадян держави та забезпечення кібербезпеки;

процеси планування та організації діяльності суб’єктів забезпечення кібербезпеки у сфері реагування на загрози кібербезпеці в умовах кібервійни;

процес досягнення суспільної єдності в державі з питань забезпечення кібербезпеки;

процес оптимізації системи суспільно-інформаційних відносин;

процес нормалізації офіційних відносин між Українською державою і міжнародними партнерами з питань міжнародної та національної кібербезпеки.

Третім елементом СКБ є правовий механізм забезпечення кібербезпеки, який формується під впливом різноманітних чинників:

особливості вихідного правового поля з питань національної безпеки й суспільно-інформаційних відносин в українському суспільстві;

особливості стану міжнародних інформаційних відносин та суспільно-інформаційних відносин в Україні;

розширення міжнародної співпраці у сфері забезпечення кібербезпеки України тощо.

Правові засади забезпечення кібербезпеки встановлюють:

норми і правила діяльності суб'єктів забезпечення кібербезпеки, їх статус, функції і компетенцію;

характер й структуру взаємовідносин між суб'єктами забезпечення кібербезпеки;

порядок формулювання мети, цілей та завдань забезпечення кібербезпеки;

принципи побудови та функціонування державно-управлінських інститутів кібербезпеки;

методи, форми, правові засоби державного реагування на загрози кібербезпеці;

сукупність правових інструментів для гарантування реалізації національних інтересів суб'єктами політики забезпечення кібербезпеки.

Четвертим елементом СКБ є інституційний механізм забезпечення кібербезпеки, що охоплює діяльність інституціональних елементів, які представляють суб'єкти забезпечення кібербезпеки. Місце суб'єктів забезпечення кібербезпеки в інституційному механізмі визначається перш за все функціями формування та реалізації згаданої політики. Остання реалізується за допомогою механізму розробки й комплексного механізму реалізації державної політики забезпечення кібербезпеки.

П'ятим елементом СКБ є механізм розробки державної політики забезпечення кібербезпеки.

Шостим елементом СКБ є механізм партисипаторної (громадської) взаємодії, що передбачає організацію та здійснення взаємодії держави та інституцій громадянського суспільства, ІТ-бізнесом з питань гарантування кібербезпеки, а саме розробки політики забезпечення кібербезпеки та громадського контролю її реалізації.

Є сенс зауважити, що складовою частиною СКБ є СЗКБ.

СЗКБ представляє собою комплексний механізм реалізації державної політики забезпечення кібербезпеки. Останній структурно включає в себе нище наведені механізми.

Організаційно-адміністративний механізм забезпечення кібербезпеки покликаний забезпечити функціонування інституцій (суб'єктів) забезпечення кібербезпеки відповідно правил і процедур щодо:

організації виконання відповідними інституціями Стратегії кібербезпеки України та інших нормативно-правових актів, що безпосередньо та опосередковано регулюють питання забезпечення кібербезпеки;

організації ідентифікації (оцінки) загроз кібербезпеці та прогнозування тенденцій їх розвитку;

організації розподілу та використання ресурсів СЗКБ для виконання завдань реактивного та проактивного реагування на загрози кібербезпеці;

організації виконання функціональних завдань та координації дій між суб'єктами забезпечення кібербезпеки на рівні заходів та адміністративно-правових режимів;

організації виконання функціональних завдань підрозділами СБУ, МВС та спецслужбами у сфері забезпечення кібербезпеки;

організації науково-методичного та кадрового забезпечення виконання функціональних завдань СЗКБ;

координації дій між суб'єктами забезпечення кібербезпеки в кризовій ситуації, зумовленій деструктивним впливом інформаційно-технологічного чинника;

організації консультування і громадського обговорення проектів документів щодо забезпечення кібербезпеки;

організації інформаційного супроводження політики забезпечення кібербезпеки;

організації контролю реалізації заходів забезпечення кібербезпеки.

Рис. 1.8. Структурна схема СКБ

Фінансовий механізм забезпечення кібербезпеки має на меті гарантування бюджетного фінансування функціонування СЗКБ.

Механізмами державного реагування загрози кібербезпеці є механізм

проактивного реагування на загрози кібербезпеки, механізм реактивного реагування на загрози кібербезпеці.

Інформаційно-аналітичний механізм забезпечення кібербезпеки має на меті моніторинг та прогнозування загроз національним інтересам у кіберсфері, аналіз внутрішнього і зовнішнього безпекового кіберсередовища країни в контексті досягнення цілей визначених у стратегії забезпечення кібербезпеки.

Кадровий механізм забезпечення кібербезпеки має на меті забезпечити СЗКБ фахівцями з відповідними компетенціями у сфері забезпечення кібербезпеки.

Інформаційний механізм має на меті забезпечити інформаційно-пропагандистське супроводження політики забезпечення кібербезпеки.

Також, до складу комплексного механізму реалізації політики забезпечення кібербезпеки структурно входять: механізм науково-методичного забезпечення кібербезпеки; механізми міжнародного й міждержавного співробітництва з питань забезпечення кібербезпеки; механізм забезпечення управлінської взаємодії суб'єктів забезпечення кібербезпеки; механізм інтеграції кіберпростору України у світовий інформаційний простір; механізм інформаційно-технологічного забезпечення реагування на загрози кібербезпеці; механізм забезпечення комунікації суб'єктів забезпечення кібербезпеки; механізм контролю стану кібербезпеки.

Теоретико-методологічними засадами функціонування механізмів забезпечення кібербезпеки є теорія ефективності механізму державного реагування на загрози національній безпеці [12; 115], теорія ефективності інформаційно-аналітичного забезпечення політики національної безпеки [198; 199].

Зокрема, в [115] визначено основі види оцінки ефективності механізму державного реагування на загрози національним інтересам, а саме загальну та поточну ефективності механізму реагування на загрози

національним інтересам.

Під загальною соціальною ефективністю механізму державного реагування на загрози кібербезпеці будемо розуміти рівень захисту національних інтересів в кіберсфері.

Поточна ефективність механізму державного реагування на загрози кібербезпеці структурно включає в себе:

1. Цільову ефективність механізму державного реагування на загрози кібербезпеці, зміст якої полягає у визначенні ступеню досягнення основних цілей державного реагування на загрози кібербезпеці.

2. Результативну ефективність механізму державного реагування на загрози кібербезпеці, зміст якої полягає у визначенні:

структурної відповідності складових механізму державного реагування на загрози кібербезпеці функціям та завданням СЗКБ, які визначені в офіційному дискурсі національної безпеки України;

інституційної спроможності складових механізму державного реагування на загрози кібербезпеці до виконання завдань за призначенням;

тривалості державного реагування на виявлену загрозу кібербезпеці;

організаційно-технічного рівня механізму державного реагування на загрози кібербезпеці.

3. Витратну ефективність механізму державного реагування на загрози кібербезпеці, зміст якої полягає у визначенні відношення ефекту державного реагування на загрози кібербезпеці до витрат в конкретних умовах.

Зазначимо, що в [12, с. 162] загальну результативність механізму державного реагування на загрози національній безпеці запропоновано оцінювати за шкалою:

0 – результативність відсутня;

1– результативність є частковою;

2 – результативність є обмеженою;

3 – результативність досягнуто в повному обсязі.

Використовуючи результати наукового дослідження [199] пропонуємо розрізняти загальну ефективність інформаційно-аналітичного механізму забезпечення кібербезпеки й оцінювати її по трьох бальній шкалі (0 – відсутній успіх; 1 – керівництву надана певна допомога у вирішенні проблем забезпечення кібербезпеки; 2 – деякий обмежений успіх у гарантуванні кібербезпеки; 3 – повний успіх у гарантуванні кібербезпеки).

Отже, при оцінці ефективності функціонування механізмів державного реагування на загрози кібербезпеці будемо розрізняти загальну соціальну і поточну ефективності.

Висновки до першого розділу

Проведений аналіз теоретико-методологічних засад дослідження публічно-управлінських проблем забезпечення кібербезпеки України дозволяє зробити наступні висновки:

1. Системний аналіз вітчизняної наукової літератури та джерел, присвячених проблемам забезпечення національної безпеки, й зокрема кібербезпеки дозволяє виокремити політичний, соціо-технічний, правовий, державно-управлінський та публічно-управлінський напрями дослідження. Останній є найбільш «молодим», а тому менше розроблений порівняно з рештою. Зокрема, наразі обмаль наукових праць присвячених розгляду питань власне публічно-управлінської інтерпретації проблем формування сучасної конфігурації суспільно-інформаційних відносин в Україні в інтересах забезпечення кібербезпеки. Також не повною мірою висвітлено питання щодо формування та функціонування державних механізмів забезпечення кібербезпеки, щодо взаємозв’язку між інформаційною безпекою й кібербезпекою.

2. Аналіз вітчизняного понятійно-термінологічного апарату основ публічного управління кібербезпекою дає підставу стверджувати про відсутність єдиного розуміння принципів розробки і реалізації політики забезпечення кібербезпеки, а також нескоординований характер підходів

до формування відповідної законодавчої бази. З'ясовано сутність кібербезпеки та специфіки функціонування державних механізмів її гарантування.

Встановлено, що кібербезпека, як органічна складова національної інформаційної безпеки, представляє собою органічну єдність політико-правових та нормативно-правових, соціально-організаційних, інформаційних та інших механізмів, що забезпечують управління процесами взаємодії держави та ІТ-бізнесу з питань реактивного й проактивного реагування на загрози кібербезпеці.

Розвинуто понятійно-категорійний апарат проблематики публічного управління кібербезпекою шляхом введення в науковий обіг авторських визначень понять: «соціально-психологічний механізм усвідомлення проблем забезпечення кібербезпеки», «система кібербезпеки», «система забезпечення кібербезпеки», «державна політика забезпечення кібербезпеки», «державно-політичний механізм забезпечення кібербезпеки», «механізм розробки політики забезпечення кібербезпеки», «механізм реалізації політики забезпечення кібербезпеки», «організаційно-адміністративний механізм забезпечення кібербезпеки», «інституційний механізм забезпечення кібербезпеки», «фінансовий механізм забезпечення кібербезпеки», «кадровий механізм забезпечення кібербезпеки», «механізм науково-методичного забезпечення кібербезпеки», «інформаційно-аналітичний механізм забезпечення кібербезпеки», «механізм міжнародного співробітництва з питань забезпечення кібербезпеки», «механізм міждержавного співробітництва з питань забезпечення кібербезпеки», «механізм інтеграції національного кіберпростору у світовий кіберпростір», «механізм партисипаторної (громадської) взаємодії у сфері забезпечення кібербезпеки», «механізм інформаційного забезпечення кібербезпеки», «механізм забезпечення комунікації суб'єктів забезпечення кібербезпеки», «механізм забезпечення управлінської взаємодії суб'єктів забезпечення кібербезпеки», «механізм державного

реагування на загрози кібербезпеці», «механізм проактивного реагування на загрози кібербезпеки», «механізм реактивного реагування на загрози кібербезпеки», «механізм інформаційно-технологічного забезпечення реагування на загрози кібербезпеці», «технологія державне реагування на загрози кібербезпеці».

В розділі побудовано стратифікаційну модель реалізації функцій публічного управління кібербезпекою, яку подано у вигляді семи страт: а) страти процесу публічного управління кібербезпекою, на якій розкриваються уявлення про зміст та суб'єкти, цілі, засоби й результати публічного управління у цій специфічній сфері; б) страти функцій «комунікація», «планування», «організація», «контроль», «мотивація», «прийняття публічно-управлінських рішень», на яких розкриваються уявлення про діяльність та взаємодію суб'єктів забезпечення кібербезпеки, а також механізми забезпечення кібербезпеки.

3. Обґрунтовано, що структурними компонентами СКБ є механізми: соціально-психологічний механізм усвідомлення проблем забезпечення кібербезпеки, державно-політичний забезпечення кібербезпеки, правовий, інституційний, механізм розробки політики забезпечення кібербезпеки, механізм партисипаторної взаємодії. Структурними компонентами СЗКБ є механізми: комплексний механізм реалізації політики забезпечення кібербезпеки, що структурно містить: організаційно-адміністративний механізм забезпечення кібербезпеки, фінансовий, інформаційний, інформаційно-аналітичний механізми, механізми державного реагування на загрози кібербезпеці, механізм міжнародного й міждержавного співробітництва з питань забезпечення кібербезпеки, механізм інтеграції кіберпростору України у світовий інформаційний простір, механізм інформаційно-технологічного забезпечення реагування на загрози кібербезпеці; механізм забезпечення управлінської взаємодії суб'єктів забезпечення кібербезпеки, механізм забезпечення комунікації суб'єктів забезпечення кібербезпеки, механізм науково-методичного забезпечення

кібербезпеки, механізми контролю стану кібербезпеки.

Доведено, що теоретико-методологічними засадами формування СЗКБ та механізмів забезпечення кібербезпеки здійснюється є загальна теорія систем, теорія державного управління національною безпекою, теорія публічного управління, теорії національної безпеки, інформаційної безпеки і кібербезпеки, теорії гібридної, інформаційної та кібернетичної війн, теорія інституціональних матриць, теорія стратегічного планування у сфері національної безпеки, теорія проектування систем управління.

Основні результати першого розділу дисертаційного дослідження висвітлено у низці публікацій автора [84; 85].

РОЗДІЛ 2
ОСНОВНІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В КРАЇНАХ-ЧЛЕНАХ ЄС ТА НАТО, УКРАЇНІ: СУЧАСНИЙ СТАН ТА ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ

У другому та третьому розділах дослідження буде перевірено гіпотезу дисертаційного дослідження, яка полягає в тому, що систематизовані знання щодо законів, закономірностей, принципів інформаційної глобалістики, геополітичного інформаційного протиборства, інформаційної війни та кібервійни стали основою визначення перспективних моделей СКБ та СЗКБ. Впровадження вказаних моделей в практику управління кібербезпекою НАТО та ЄС, країн-членів вказаних організацій дозволило їм розбудувати результативні СКБ та ефективні СЗКБ. Впровадження позитивного досвіду НАТО та ЄС щодо управління кібербезпекою у вітчизну публічно-управлінські практику у цій сфері значною мірою вдосконалить інституційну структуру СЗКБ України, що стане запорукою надійного захисту національних інтересів у цій специфічній сфері.

2.1. Сучасні трансформації безпекового кіберсередовища як детермінанти розвитку систем кібербезпеки міжнародних організацій та національної держави

Аналіз літератури [8; 50; 51; 66; 67; 125; 140; 171; 229; 232] дозволяє констатувати, що:

1. Наразі сформовано глобальний інформаційний простір, на основі розгортання інформаційної та телекомунікаційної революції. Структурним елементом глобального інформаційного простору є світовий кіберпростір.

2. Домінування інформаційної складової в структурі сучасної цивілізації спричинило переміщення конфліктної логіки з військової сфери

в інформаційну та економічну сфери, що надало якісно нових характеристик сучасному міждержавному протиборству.

3. У глобальному інформаційному просторі розгортається геополітичне інформаційне протиборство, яке визначається геоекономічною конкуренцією і має дві складові інформаційної боротьби: інформаційно-технічну та інформаційно-психологічну, що ведеться на стратегічному, оперативному та тактичному рівнях.

4. Систематизоване виявлення нових інформаційно-технічних явищ у сфері геополітичного інформаційного протиборства призводить до:

а) виокремлення кіберпростору, який структурно містить три складові:

фізична або технологічна інфраструктура систем зв'язку;

семантичні дані;

синтаксичні протоколи передачі даних.

б) виведення нової категорії «кібервійна», що створює платформу для системного вивчення і практичного застосування нових явищ у кіберпросторі.

5. Перехідний період між періодами домінування традиційних форм вирішення конфліктів (класична війна, інформаційна війна, мережоцентрична війна) та перспективних (кібервійна) визначається темпами глобалізації у економічній, інформаційній, політичній та військовій сферах.

6. У світовому кіберпросторі ведуться кібервійни без юридичного факту оголошення останніх.

В [8; 66] проаналізовано динаміку розвитку інструментарію геополітичного інформаційного протиборства на основі чого було обґрунтовано доцільність диференціації форм інформаційної війни на суто інформаційну війну, психологічну та кібернетичну війни. Вітчизняний дослідник В. Антонюк пропонує визначити [8]:

сутність інформаційної війни як управління інформаційними

потоками;

сутність психологічної війни як форматування суспільної свідомості супротивника в інтересах активної сторони геополітичного інформаційного протиборства;

сутність кібервійни як руйнування системи управління інформацією в інтересах активної сторони згаданого протиборства.

Аналіз результатів наукових досліджень [13; 14; 31; 50-52; 71; 72; 175; 232] дозволяють зробити висновок: кібервійна – це система узгоджених за ціллю, місцем та часом інформаційних дій у кіберпросторі із використанням програмних кодів задля захоплення управління (часткове, повне) або руйнування інформаційного зв'язку, що перешкоджає штатному функціонуванню систем управління інформацією у сферах публічного, державного та військового управління, в бізнесі й приватній сфері життєдіяльності людини.

Масштаб кібервійни залежить як від масштабів об'єктів впливу, так і від взаємного розташування систем джерел кіберзагроз, а також від характеристик елементів загальносвітового єдиного кіберпростору, тобто поля бою.

Цілями кібервійни війни є [8; 50-52; 65, с. 99-105; 133]:

знищення або перехоплення даних з метою перекриття доступу до інформаційних джерел конкурентам / супротивнику;

захоплення інформаційних ресурсів супротивника або конкурентів;

переведення «чужої» системи автоматизованого управління в режим, який відповідає інтересам активної сторони інформаційного протиборства;

призупинення функціонування «чужої» автоматизованої системи управління або її знищення задля зміни характеристик зовнішнього кіберсередовища;

руйнування цілісності інформаційної інфраструктури банківської та економічної систем, системи публічного та державного управління задля створення хаосу у різних сферах суспільного життя;

руйнування цілісності інформаційної інфраструктури систем воєнної безпеки держави та військового управління;

руйнування цілісності інформаційної інфраструктури приватного життя людини / громадянина, зокрема викрадення персональних даних та ін.;

зміна характеристик безпекового кіберсередовища.

Варто зазначити, що проведення наступальних кібероперацій спрямовані на дистанційне виведення із ладу системи життєзабезпечення держави-мішені, систем державного й військового управління. Вказані заходи передбачають здійснення:

атак на фізичний шар кіберпростору, тобто задля фізичного руйнування інформаційної інфраструктури та системи передавання даних;

атак на семантичний шар кіберпростору, тобто атак задля порушення цілісності й коректності інформації;

атак на синтаксичний шар кіберпростору, тобто атак задля пошкодження даних за допомогою вірусів і порушення логіки функціонування систем.

Враховуючи те, що атаки на семантичний та синтаксичний шари кіберпростору є більш простими і дешевшими засобами інформаційного протиборства, ніж атаки на фізичний шар кіберпростору зі застосуванням звичайної зброї, опрацювання питань по реалізації згаданих атак приділяється більша увага.

У вітчизняному науковому дискурсі кібербезпеки запропоновано виокремити такі складові кіберпростору, як: інформаційний, комунікаційний, віртуальний комп’ютерно-мережний та соціо-технічний простір [65, с. 93-94]. Проте, на нашу думку, для планування та ведення кібервійни та кібероборони доречно виокремити фізичний, семантичний та синтаксичний шари кіберпростору, які охоплюють собою інформаційний, комунікаційний, віртуальний комп’ютерно-мережний та соціо-технічний простори.

Є сенс зауважити, що в ході інфраструктурних війн, метою яких є руйнування критичної інфраструктури держави-мішені [34; 35], цілями кібератак є системи контролю і комунікацій життєво й стратегічно важливих об’єктів, а саме:

інформаційні і комунікаційні ресурси країни;

хімічна промисловість та АЕС;

автоматизовані системи управління технологічними процесами на стратегічно важливих підприємствах;

фінансова та банківська системи;

енергетична, транспортна, критична інфраструктура країни;

системи публічного, державного та військового управління.

Варто зазначити, що в рамках наявного методологічного апарату не можливо в повній мірі описати явища кібервійни [65, с. 99-105]. Відповідно виникає низка проблем, які потребують свого негайного розв’язання:

розробка методологічного апарату по проектуванню та державному конструюванню СЗКБ, створенню захищеної системи управління телекомунікаційними системами;

розробка методології формування складу й структури СЗКБ;

методології проведення оборонних та наступальних кібероперацій;

розробка системи оцінок (параметрів і критеріїв) потенціалів супротивників щодо ведення кібервійни;

методології формування організаційної структури спеціальних підрозділів для ведення кібервійни та кібероборони.

В рамках сцієнтистської парадигми державного управління [114] розглянемо закони та закономірності інформаційної глобалістики, інформаційної геополітики, інформаційної війни та кібервійни які, в свою чергу є детермінантами трансформацій безпекового кіберсередовища сучасної держави.

Науковими законами інформаційної глобалістики є:

закон посилення чинника інформаційної глобалізації на глобалізаційні процеси у економічній, політичній та військовій сферах, у сфері державного та публічного управління [29; 30; 229];

закон посилення чинника інформаційної глобалізації на трансформацію безпекового простору, на перехід від ієрархічних організацій до мережевих, на зміну парадигми війни, в якій як об'єкти нападу / захисту визначено не лише критичну інфраструктуру, а й інформаційну інфраструктуру держави та систему державного управління [92];

закон посилення чинника інформаційної глобалізації на перехід від суто національного рівня управління інформаційною безпекою та кібербезпекою до інтегрованого управління шляхом синхронізації процесів управління на національному, регіональному та глобальному рівнях [86];

закон посилення чинника інформаційної глобалізації на поширення трансграничних загроз інформаційній безпеці та кібербезпеці, а також віртуалізації згаданих загроз [101; 102; 105]. Як вже було зазначено, в науковому дискурсі виокремлено два види інформаційної боротьби: інформаційно-технічну та інформаційно-психологічну, які ведуться на стратегічному, оперативному та тактичному рівнях [102]. Водночас, варто додати, що на стратегічному рівні геополітичного інформаційного протиборства зазвичай діють вищі органи влади, а на оперативному і тактичному – спецслужби та великий капітал.

При інформаційно-технічній боротьбі головними об'єктами впливу і захисту є інформаційно-технічні системи. Тобто, комп'ютери, засоби зв'язку і програмне забезпечення виступають у ролі зброї масового збою, за допомогою якої можна проникати до комп'ютерних систем і порушувати їх роботу.

Вітчизняні та зарубіжні дослідники констатують, що у світовому кіберпросторі вже давно здійснюються спецоперації і фактично йде неоголошена кібервійна [93; 97].

Провідним науковим законом інформаційної геополітики є утвердження

міжнародних інформаційних відносин, що визначаються інформаційною перевагою у віртуальному просторі й спроможністю переформатування суспільної свідомості населення держави-жертви агресії [55, с. 429].

Другий закон геополітики – це закон домінування комунікаційного та інформаційного контролю над простором державно-територіальних утворень, що все більше набувають транснаціональних форм [98; 101].

Третій закон інформаційної геополітики – це посилення інформаційного та кібернетичного чинників в міждержавному протиборстві [50; 51].

Отже, наукові закони та закономірності інформаційної геополітики надзвичайно зручні для аналізу історії геополітичного інформаційного протиборства та стратегічного планування у сфері національної інформаційної безпеки та кібербезпеки.

Науковими законами інформаційної війни є [8]:

1. Закон залежності стратегії ведення інформаційної війни від політичних цілей цієї війни.

2. Закон залежності стратегії ведення й результату інформаційної війни від співвідношення інформаційних, економічних, соціальних та наукових потенціалів супротивників у цій війні.

На основі аналізу результатів наукових досліджень [8; 50; 51] нами виокремлені такі особливості кібервійни, як-от:

ведення кібервійни відбувається в штучно створеному середовищі, яке також може бути трансформоване відповідно до цілей вказаної війни;

заходи кібервійни можуть здійснюватися без безпосередньої участі збройних сил і навіть при їх відсутності;

ведення кібервійни будь-якого масштабу можливе при відсутності юридичного факту її оголошення;

можливість потаємного розташування засобів ведення кібервійни й велика невизначеність їх можливостей;

результати інформаційно-технічного впливу не пропорційні кількості сил кібервійськ, які можуть бути залучені до здійснення

згаданого впливу;

чим вищий рівень автоматизації об’єктів (процесів), тим більших результатів можна досягнути в кібервійні, адже самими уразливими є найбільш розвинуті інформаційно-комунікаційні системи.

Аналіз наукової літератури [8; 50; 51] дозволяє зробити висновки, що сучасними тенденціями ведення інформаційної боротьби в кіберпросторі є:

поєднання просторового та інформаційного континуумів інформаційної боротьби в кіберпросторі. Це передбачає одночасне розгортання інформаційної боротьби у фізичному, семантичному та синтаксичному шарах кіберпростору;

зміна логіко-часової побудови інформаційної боротьби у кіберпросторі. Це передбачає збільшення тривалості підготовчих дій і зменшення періоду активних дій інформаційної боротьби;

посилення дедуктивних і послаблення індуктивних зв’язків і відносин інформаційної боротьби в кіберпросторі. Це означає зміну співвідношення дій на стратегічному, оперативно-тактичному й тактичному рівнях ведення кібервійни, а саме використання стратегічних та оперативно-тактичних засобів для ураження об’єктів кібербезпеки тактичного рівня, що дозволяє в кінцевому підсумку якнайшвидше досягти перемоги;

організація та ведення інформаційної боротьби в кіберпросторі в реальному масштабі часу. Це означає перехід від управління кібервійськами до управління інформаційною боротьбою згідно положень теорії «керованих війн» (автоматизація розвідки, оцінки обстановки, прийняття рішень, наведення й здійснення інформаційно-технологічного впливу на визначений об’єкт кібербезпеки, контролю);

збільшення розриву у можливостях засобів кібернападу та кіберзахисту. Це означає випереджальний розвиток засобів і способів кібернападу в порівнянні із засобами кіберзахисту.

Що стосується кібервійни, то вона підпорядковуються власним науковим

законам, що вивчає теорія кібервійни, як-от [8; 50; 51]:

1. Закон завдання поразки супротивнику при максимальному збереженні своїх кібервійськ.

2. Закон відповідності цілей кібервійни, наявним силам і засобам кібервійськ.

3. Закон зосередження переважаючих сил кібервійськ у найбільш уразливому місці інформаційної інфраструктури супротивника.

4. Закон кіберстійкості своєї інформаційної інфраструктури.

5. Закон взаємодії кібервійськ за єдиним стратегічним задумом.

У сфері ведення кібервійни можна виокремити такі закономірності:

обумовленість масштабів і спрямованості кібервійни характером безпекової обстановки, політичними цілями згаданої війни;

відповідність змісту і масштабів засобів кібервійни характеру і особливостям інформаційної інфраструктури супротивної сторони, її СКБ та СЗКБ;

залежність масштабів і якості сил і засобів кібервійськ від економічних та інформаційних спроможностей держави.

Основним принципами ведення кібервійни є [8; 50; 51]:

відповідність цілей і завдань кібервійни політичним цілям держави у міждержавному протиборстві;

необхідність зосередження сил кібервійськ у вирішальному місці та вирішальний момент згідно стратегічного задуму;

принцип високої активності й рішучості в ході ведення кібервійни;

принцип раптовості кібердарів;

принцип узгодженого спільного застосування різних сил кібервійськ і засобів ведення кібервійни;

принцип всебічної й завчасної підготовки сил і засобів кібервійськ для ведення кібервійни;

принцип постійної готовності сил кібервійськ до кіберзахисту та кібероборони;

принцип безперервності кібервійни та інтеграції її результатів;

принцип максимальної синхронізації заходів кібервійни з іншими заходами міждержавного протиборства;

принцип максимального ступеню наближення фінальної / запланованої ситуації в кіберпросторі;

принцип пріоритетності вкладу автоматизованої системи управління в створенні й розповсюдженні відповідного інформаційного ресурсу, а також ступеню впливу ефекту його поширення на суміжні системи управління;

принцип врахування характеристик інформаційних телекомунікаційних систем при плануванні та здійсненні кібероперацій;

принцип врахування рівня ІТ-технологій та кваліфікації персоналу при плануванні та здійсненні кібероперацій;

принцип поєднання різних способів і видів інформаційно-технологічного впливу;

принцип «розмитості» стану мирного й воєнного часу.

Всі зазначені принципи ведення кібервійни реалізовуються в конкретних способах і формах ведення згаданої війни.

На основі законів, закономірностях, принципах ведення інформаційної війни та кібервійни розробляються принципи (основні положення) гарантування інформаційної безпеки, а також кібербезпеки, яка є складової першої.

Використовуючи модель взаємообумовленості законів, закономірностей і принципів державного управління, які запропоновано в [22], розглянемо механізм опредмечування закономірностей публічного та державного управління кібербезпекою (див. рис. 2.1).

Зауважимо, що закони та закономірності інформаційної глобалістики, інформаційної геополітики, інформаційної війни та кібервійни визначають закономірності розвитку СКБ та СЗКБ.

Наведемо деякі закономірності розвитку СКБ та СЗКБ.

Перша закономірність: за умов втрати державою спроможності щодо захисту державного суверенітету, зокрема інформаційного та цифрового суверенітету – обмежуються спроможності її конструктивного впливу на процеси забезпечення інформаційної безпеки та кібербезпеки, інформаційного розвитку суспільства в цілому [50].

Друга закономірність: сучасні геополітичні центри сили намагаються підірвати інформаційну могутність своїх конкурентів за допомогою економічних та інформаційно-технічних інструментів, що негативно позначить на функціонуванні та удосконаленні СКБ та СЗКБ країн-конкурентів [102].

Третя закономірність: результативність СКБ та ефективність СЗКБ забезпечується врахуванням при проектуванні та конструюванні вказаних систем динаміки трансформацій безпекового кіберсередовища. Зауважимо, що згадана динаміка трансформацій безпекового кіберпростору визначає вимоги до СКБ та СЗКБ щодо своєчасного та адекватного реагування на загрози кібербезпеці [79; 80].

Тобто, наукові закони інформаційної глобалістики, інформаційної геополітики, інформаційної війни та кібервійни визначають закономірності розвитку СКБ та її складової – СЗКБ.

Зауважимо, що останні формулюються в наукових законах державного управління та опредмечуються в нормативно-правових актах, що регламентують діяльність суб’єктів забезпечення кібербезпеки. Закономірності державного управління кібербезпекою також безпосередньо впливають на формування принципів державного управління у цій сфері. Водночас, принципи державного управління кібербезпекою, розпредмечуючись у поведінці суб’єктів забезпечення кібербезпеки, можуть визначати закономірності державного управління. Останні певним чином можуть впливати на формування закономірностей розвитку СКБ та СЗКБ.

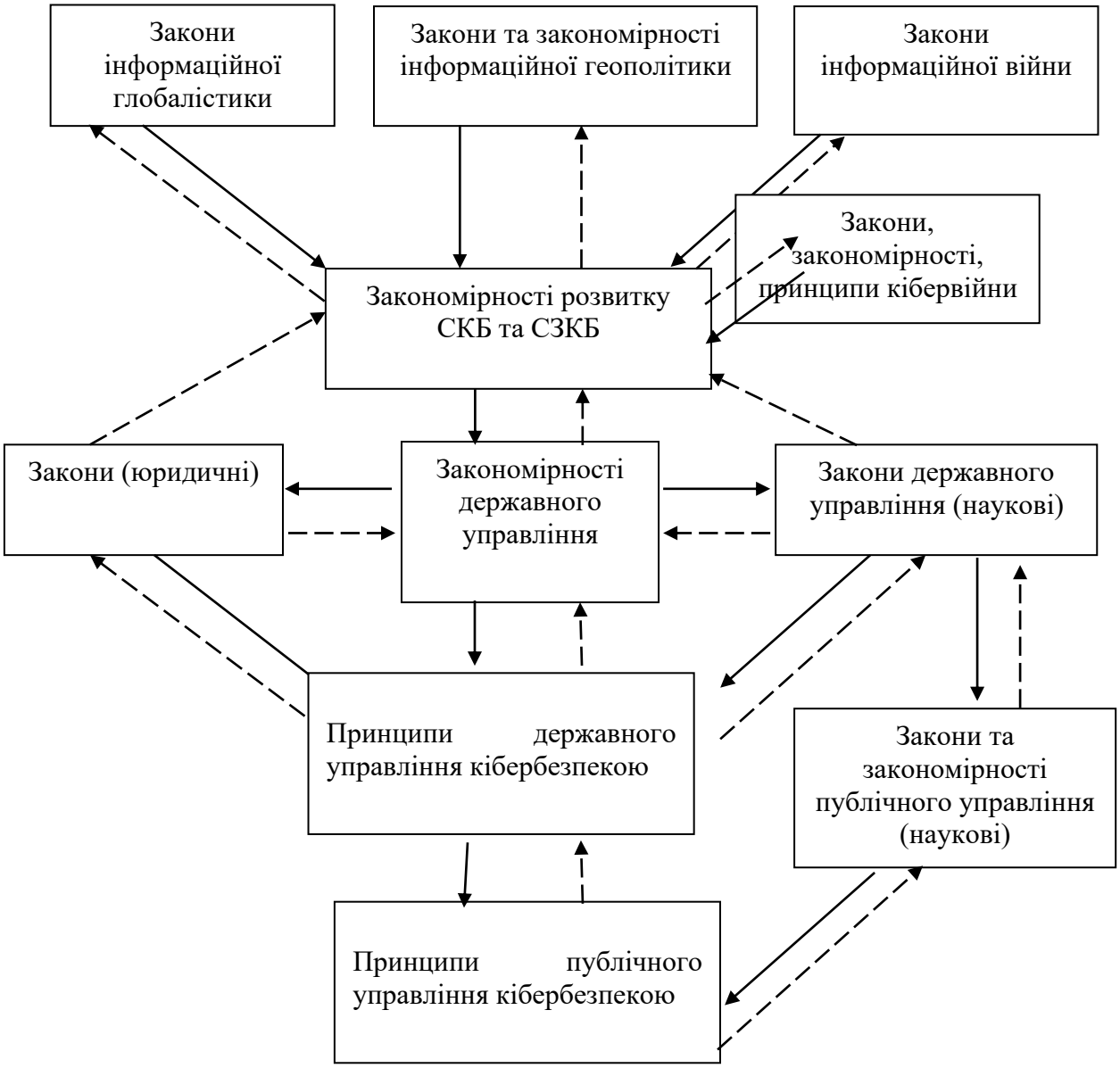

Рис. 2.1. Модель взаємообумовленості законів, закономірностей і принципів державного й публічного управління кібербезпекою

Пропонуємо, виокремити дві групи принципів державного управління кібербезпекою:

принципи, які визначають зміст державного управління у цій сфері;

принципи організації процесу управління кібербезпекою.

Для формулювання згаданих принципів пропонуємо виокремити дві основні групи закономірностей державного управління кібербезпекою.

Перша група закономірностей державного управління кібербезпекою відображає залежність природи забезпечення кібербезпеки, його місця у феноменології та інструментарії державного управління від:

1) особливостей безпекового кіберсередовища, а саме:

а) зміни ролі і місця кібервійни в сучасному геополітичному інформаційному протиборстві [50];

б) трансформацій кібервійни, що характеризується зміною форм кібервійни [51];

в) економічних, інформаційних, наукових і воєнних потенціалів держав [36];

2) офіційного зовнішньополітичного курсу держави, пріоритети зовнішньої політики та політики національної безпеки в рамках яких визначено стратегічні партнери у сфері безпеки;

3) характеру офіційного дискурсу кібербезпеки в якому представлено розуміння загроз кібербезпеці та методи реагування на них.

Друга група закономірностей відображають залежність організаційних форм державного управління кібербезпекою від організаційного середовища держави [92], а саме від:

а) чіткого визначення місії, функції, завдань СЗКБ, а також спроможностей сил, які залучаються до реагування на кіберзагрози;

б) рівня управлінської культури фахівців, котрі здійснюють забезпечення кібербезпеки;

в) загальної та поточної ефективності СЗКБ;

г) рівня науково-методичного та правового забезпечення заходів реактивного та проактивного реагування на загрози кібербезпеці;

д) умови миру та війни в яких здійснюється забезпечення кібербезпеки.

Зазначені вихідні положення дозволяють нам виокремити принципи державного управління кібербезпекою, які є найбільш загальними, засадничими правилами й рекомендаціями, якими слід керуватися при розбудові СЗКБ та організації і здійсненні діяльності у сфері забезпечення кібербезпеки.

Пропонуємо наступну градацію принципів:

методологічні принципи, які визначають зміст державного управління у цій сфері – проектування та конструювання СКБ та СЗКБ, забезпечення функціонування та удосконалення СЗКБ в контексті вимог динамічного безпекового кіберсередовища. Вказані принципи державного управління необхідно використовувати для визначення місії СЗКБ, проектування та конструювання цієї системи. Згадані принципи розробляються на основі першої групи закономірностей державного управління кібербезпекою;

організаційні принципи відповідно яких повинна реалізовуватися місія СЗКБ. Згадані принципи розробляються на основі другої групи закономірностей державного управління кібербезпекою.

До методологічних принципів державного управління кібербезпекою пропонуємо віднести:

1) принцип науковості державного управління кібербезпекою, який передбачає використання результатів наукових розробок у сфері кібербезпеки в процесі проектування та конструювання СЗКБ, планування й здійснення реагування на загрози кібербезпеці, оцінки результатів діяльності суб’єктів забезпечення кібербезпеки;

2) принцип єдності теорії і практики державного управління кібербезпекою, який передбачає одночасне поєднання розвитку теоретичних засад державного управління у згаданій сфері й узагальнення та систематизацію позитивного досвіду забезпечення кібербезпеки;

3) принцип дотримання законності у визначенні та реалізації цілей у сфері забезпечення кібербезпеки, у визначенні засобів забезпечення кібербезпеки;

4) принцип підпорядкованості місії, функцій та завдань СЗКБ положенням офіційного дискурсу національної безпеки конкретної держави, що

забезпечує цілісність СЗКБ в контексті реалізації єдиного задуму відстоювання національних інтересів у різних сферах життєдіяльності загалом, й у сфері кібербезпеки зокрема;

До організаційних принципів державного управління кібербезпекою можна віднести:

1) принцип оптимальної відповідності цілей СЗКБ, її структури та функцій, динаміці і організаційно-управлінським процесам у сфері національної безпеки. Дотримання вказаного принципу передбачає відповідність загальних спроможностей щодо реалізації функцій СЗКБ цілям державної політики забезпечення кібербезпеки, темпам і змістовним змінам у державно-управлінській практиці забезпечення національної безпеки;

2) принципи плановості та послідовності здійснення заходів реактивного та проактивного реагування на кіберзагрози та інших заходів гарантування кібербезпеки;

3) принцип оперативності, що передбачає адекватність й своєчасність заходів реактивного та проактивного реагування на кіберзагрози, що пов'язано із мінливістю безпекового кіберсередовища.

Згадані принципи є взаємопов'язаними й мають реалізуються в єдності.

Використовуючи напрацювання, які представлені в [124, с. 3-10] щодо взаємозв'язку між публічним та державним управлінням проілюструємо модель публічного управління кібербезпекою. Вказана модель містить такі етапи управлінської діяльності, як: актуалізація інтересу або проблеми забезпечення кібербезпеки → усвідомлення проблеми забезпечення кібербезпеки суб'єктом громадянського суспільства → формування публічної політики забезпечення кібербезпеки → легітимізація публічної політики забезпечення кібербезпеки = формування на її основі державної політики забезпечення кібербезпеки (програми / проекту) → реалізація державної політики забезпечення кібербезпеки → моніторинг і контроль за реалізацією державної політики забезпечення кібербезпеки → публічний

аудит публічного управління кібербезпекою суб'єктами публічної сфери та громадянського суспільства.

На наше переконання, публічне управління кібербезпекою слід впроваджувати з урахуванням відповідних законів та закономірностей публічного управління [124, с. 8], а саме:

закону залежності управління суспільством від закономірностей розвитку світової цивілізації;

закону обумовленості засад публічного управління конкретним суспільством базовими цінностями цього суспільства;

законів системності та ціннісно-ситуативного спрямування публічного управління розвитком суспільства та гарантування його безпеки;

закону необхідності посилення регулювання та управління процесами розвитку суспільства та гарантування безпеки;

закону «необхідного різноманіття» управлінських впливів на процеси розвитку суспільства та гарантування безпеки;

закону розширення представництва та участі громадянського суспільства в публічному управлінні на засадах соціального партнерства, що сприяє підвищенню результативності й ефективності згаданого управління;

закону соціально-професійної стратифікації, що забезпечує функціонування механізмів соціальної мобільності й функціонування еліт в системі публічного управління.

На основі аналізу результатів наукових досліджень [170] пропонуємо виокремити дві групи принципів публічного управління кібербезпекою:

а) принципи, які визначають зміст публічного управління у цій сфері, як-от:

принцип упорядкування суспільних справ на загальнодержавному, регіональному та місцевому рівнях у сфері кібербезпеки та забезпечення вирішення проблем у цій специфічній сфері;

принципи децентралізації та демократизації управління на рівні регіону країни та місцевого самоврядування, що передбачає доступ населення до вирішення суспільних проблем забезпечення кібербезпеки;

принцип адаптивності й креативності публічного управління кібербезпекою;

б) принципи організації процесу публічного управління кібербезпекою, як-от:

принцип самодіагностики проблеми забезпечення кібербезпеки;

принцип самоформулювання проблеми забезпечення кібербезпеки;

принцип самопропозиції вирішення проблеми забезпечення кібербезпеки;

принцип самовизначення кращого варіанту публічної політики забезпечення кібербезпеки;

принцип самовизначення кошторису забезпечення кібербезпеки;

принцип самоприйняття плану дій забезпечення кібербезпеки;

принцип самоконтролю та самооцінки результативності й ефективності реалізації публічної політики забезпечення кібербезпеки.

В рамках завдань нашого дослідження розглянемо питання, яким чином враховуються систематизовані знання щодо законів, закономірностей, принципів інформаційної глобалістики, геополітичного інформаційного протиборства, інформаційної війни та кібервійни, принципів державного та публічного управління в розбудові СКБ таї СЗКБ в країнах-членах НАТО і ЄС, Україні.

2.2. Досвід публічного управління кібербезпекою в країнах-членах ЄС та НАТО: уроки для України

Трансформації безпекового кіберсередовища в сучасних умовах глобалізації характеризуються зростанням масштабів деструктивних наслідків реалізації загроз кібербезпеці для СНБ сучасних держав та колективних систем безпеки. За таких умов особливої актуальності набувають питання:

гарантування міжнародної кібербезпеки;

гарантування кібербезпеки критичної інформаційної інфраструктури національної держави та державних електронних інформаційних ресурсів;

кіберстійкості національних СЗКБ.

Країни-члени ЄС та НАТО для вирішення згаданих питань проводять виважену політику забезпечення кібербезпеки, яка спрямована на управління ризиками у цій специфічній сфері та проактивне реагування на загрози кібербезпеці різного характеру.

Ця обставина й визначає зв'язок загальної проблеми гарантування міжнародної та національної кібербезпеки в умовах динамічного безпекового кіберсередовища з науковими та практичними завданнями адаптації досвіду забезпечення кібербезпеки країнами-членами НАТО та ЄС для потреб України.

Аналіз результатів наукових досліджень дозволяє констатувати, що досвід забезпечення кібербезпеки країн-членів НАТО та ЄС є предметом досліджень вітчизняних науковців, зокрема: В. Годлевської та В. Кононенко [32], Д. Дубова [52], М. Камчатного [71] та ін. В наукових працях згаданих авторів акцентується увага на наявності офіційно загально визначених принципів забезпечення кібербезпеки в країнах-членах ЄС та НАТО та особливостях національних СКБ, які необхідно враховувати при впровадженні зарубіжного досвіду у практику публічного управління кібербезпекою України.

З огляду на це, завданням даного підрозділу є узагальнення та систематизація досвіду країн-членів НАТО та ЄС щодо забезпечення кібербезпеки та оцінка можливості його використання у вітчизняній публічно-управлінській практиці.

Узагальнення та систематизацію досвіду країн-членів НАТО та ЄС щодо забезпечення кібербезпеки будемо здійснювати в рамках інституціонального підходу. Це дозволить нам оцінити рівень розвитку інституційного середовища публічного управління кібербезпекою

досліджуваних країн, основними компонентами якого є [230, с. 237-242]:

1) нормативно-правовий компонент публічного управління кібербезпекою, який функціонально призначений для правового регулювання суспільно-інформаційних відносин і взаємодії в СКБ, розробки та реалізації політики забезпечення кібербезпеки, а також для регламентації функціонування СЗКБ;

2) організаційний компонент публічного управління кібербезпекою, який функціонально призначений для організації діяльності суб'єктів забезпечення кібербезпеки в рамках вимог чинного національного законодавства у сфері кібербезпеки;

3) самоорганізаційний компонент публічного управління кібербезпекою, який функціонально призначений для інституалізації соціального партнерства у сфері забезпечення кібербезпеки відповідно до вимог національного законодавства;

4) соціокультурний компонент публічного управління кібербезпекою, який функціонально призначений для формуванні культури кібербезпеки та організаційної культури у сфері забезпечення кібербезпеки;

5) когнітивний компонент публічного управління кібербезпекою, який функціонально призначений для розвитку системи наукових знань у сфері кібербезпеки та публічного управління у цій сфері. Прикладом використання системи наукових знань у сфері розвитку СЗКБ країн-членів ЄС є використання матриці оцінки кібербезпеки, яка була запропонована Міжнародною торгівельною асоціацією BSA (Business SoV ware Allience) [88, с. 16].

В згаданій матриці критеріями оцінки рівня забезпечення кібербезпеки визначено:

наявність та якість нормативно-правової бази в галузі гарантування кібербезпеки держави;

операційні можливості національної СЗКБ;

державно-приватне партнерство у сфері забезпечення кібербезпеки;

наявність окремих планів для окремих секторів забезпечення кібербезпеки;

якість професійної освіти у сфері кібербезпеки.

Результати оцінки рівня забезпечення кібербезпеки слугують основою визначення пріоритетів розвитку національних СКБ країн-членів НАТО і ЄС.

Незважаючи на те, що проблема захисту критично важливих для функціонування держави, суспільства та життєдіяльності населення систем та об'єктів існувала завжди, до числа тих, що потребують системного підходу з точки зору національної та/або державної безпеки, критична інфраструктура та кібербезпека потрапили наприкінці минулого століття [34; 35].

У провідних країнах світу кібербезпека й захист критичної інфраструктури визнано пріоритетними напрямами у сфері національної безпеки. Відповідно, цими країнами активно розбудовуються національні СЗКБ та системи захисту критичної інфраструктури, приймається законодавство для регламентації діяльності суб'єктів забезпечення вказаних видів безпеки, проводиться підготовка кадрів, налагоджуються партнерські стосунки з приватним сектором, здійснюються освітні заходи серед населення тощо.

На теперішній час СЗКБ та системи забезпечення безпеки критичної інфраструктури національного рівня створені практично в усіх розвинених країнах світу.

Розглянемо питання формування нормативно-правової компоненти інституційного середовища публічного управління кібербезпекою США.

Одними із перших політичних та законодавчих напрацювань у сфері забезпечення кібербезпеки та захисту критичної інфраструктури належать США [243; 253]. В офіційному дискурсі 1990-х років з питань кібербезпеки та захисту критичної інфраструктури США було констатовано, що завдяки

досягненням у галузі інформаційних технологій, інформаційна та критична інфраструктури стають більш автоматизованими та взаємопов'язаними. Водночас ці успіхи спричинили нові небезпеки (вразливості) в разі збою обладнання, людської помилки, несприятливих погодних та інших природних факторів, а також фізичних факторів і кібератак.

У січні 2000 р. в офіційному дискурсі США розглядається питання захисту критичної інформаційної інфраструктури, що знайшло своє відображення в Національному плані із захисту інформаційних систем [127]. В подальшому, а саме у 2003 р. в США було прийнято Національну стратегію безпеки у кіберпросторі [251], у 2009 р. була введена посада Національного радника з питань кібербезпеки.

Варто зважити на те, що, починаючи з 2005 р., державна політика США щодо критичної інфраструктури конкретизується планами захисту національної інфраструктури, які регулярно оновлюються, а в структурі Міністерства внутрішньої безпеки США функціонує спеціальний Офіс захисту критичної інфраструктури.

Політика США спрямована на посилення безпеки та стійкості критичної інфраструктури стосовно фізичних і кіберзагроз. З цією метою Федеральний уряд співпрацює із власниками та операторами відповідних об'єктів і систем, державними органами всіх рівнів, місцевими органами влади з тим, щоб вживати активних заходів з управління ризиками, враховуючи при цьому всі види загроз, реалізація яких може призвести до тяжких наслідків для національної безпеки, стабільності економіки, здоров'я та безпеки населення чи будь-якої комбінації з переліченого. При цьому зусилля спрямовуються на зменшення уразливостей, мінімізацію наслідків, ідентифікацію та ліквідацію загроз, прискорення реагування та застосування відновлювальних заходів, пов'язаних з критичною інфраструктурою. Уряд ураховує міжнародний контекст проблем, пов'язаних із безпекою та стійкістю критичної інфраструктури, та взаємодіє з міжнародними партнерами у цій сфері.

Зусилля керівництва США, спрямовані на забезпечення кібербезпеки та стійкості критичної інфраструктури й мають комплексний характер, що обумовлено взаємозалежностями елементів критичної інфраструктури. До того ж у Директиві 21 [127] енергетичні системи та системи зв'язку визначені як такі, що мають унікальний рівень критичності внаслідок того, що вони забезпечують функціонування всіх інших секторів критичної інфраструктури.

Підходи Федерального уряду США на цьому напрямі визначаються трьома стратегічними імперативами:

1) уточнювати та роз'яснювати взаємозв'язки всіх урядових структур задля забезпечення загальнонаціональної єдності при посиленні безпеки та стійкості критичної інфраструктури;

2) забезпечувати ефективний обмін інформацією між усіма суб'єктами захисту критичної інфраструктури;

3) забезпечувати підтримку прийняття рішень щодо захисту критичної інфраструктури.

Відповідно до Плану захисту національної інфраструктури (2009), стратегічну та нормативно-правову основу діяльності у цій сфері становлять три категорії актів та ініціатив, а саме [127]:

1) стратегічні документи і закони США, які визначають політику держави у забезпеченні внутрішньої безпеки;

2) президентські директиви з питань внутрішньої безпеки;

3) національні ініціативи, плани тощо.

Завдяки всьому комплексу елементів, що становлять стратегічну та нормативно-правову основу діяльності всіх учасників процесу захисту критичної інфраструктури, здійснюється координація їхньої діяльності у вказаній сфері.

Правовий механізм забезпечення кібербезпеки США представлено низкою документів і стратегій, а саме [127]:

Національною стратегією внутрішньої безпеки (жовтень 2007 р.);

Національною стратегією фізичного захисту критичної інфраструктури та ключових активів (лютий 2003 р.);

Національною стратегією захисту кіберпростору (лютий 2003 р.);

Законом про внутрішню безпеку (листопад 2002 р.).

Серед найбільш важливих щодо безпеки та стійкості критичної інфраструктури президентських директив необхідно назвати такі [127]:

президентська політична Директива 8 «Національна готовність» (березень 2011 р.);

президентська політична Директива 21 «Безпека та стійкість критичної інфраструктури» (лютий 2013 р.);

указ президента США № 13636 «Удосконалення кібербезпеки критичної інфраструктури» (лютий 2013 р.);

президентська Директива 7 з питань внутрішньої безпеки «Ідентифікація, пріоритетизація та захист критичної інфраструктури» (грудень 2003 р.).

Основні документи, які належать до категорії документів, що утворюють нормативно-правову основу державної політики США щодо критичної інфраструктури, такі:

План захисту національної інфраструктури (2013) «Партнерство заради безпеки та стійкості критичної інфраструктури». Це основний чинний документ з питань критичної інфраструктури, що замінив попередні, а саме: План захисту національної інфраструктури (2009) «Партнерство заради захисту та стійкості критичної інфраструктури» та План захисту національної інфраструктури (2006) [127].

Крім того, відповідно до підходу Міністерства внутрішньої безпеки до цієї ж категорії планів та ініціатив віднесено: Національну систему управління інцидентами (2008), Національну основу реагування (2008) та Національні керівні принципи для забезпечення готовності (2007).

План захисту національної інфраструктури 2013 узгоджений з указом президента № 13636 «Удосконалення кібербезпеки критичної

інфраструктури», а також із Системою забезпечення національної готовності (National Preparedness System), що створена на виконання президентської політичної Директиви 8 «Національна готовність» [127].

У 2014 р. були прийняті такі закони, як: Федеральний закон про модернізацію інформаційної безпеки, Закон про захист національної кібербезпеки, Закон про підвищення рівня кібербезпеки. В подальшому приймалися нові редакції Стратегій кібербезпеки США в контекстній залежності від вимог динамічного безпекового кіберсередовища [126].

З вище викладеного можна зробити висновок, що така правова політика зумовлена метою забезпечення контролю та моніторингу ситуації щодо змін і ризиків у системі критичної інфраструктури з відповідним коригуванням секторальних планів, програмних елементів, концепцій тощо. Тобто кожен наступний документ розробляли відповідно до поточного стану й актуальних проблем захисту критичної інфраструктури, що дало змогу проаналізувати й оцінити ефективність різних заходів, своєчасно реагувати на актуальні запити та потреби секторів і системи загалом, визначати сферу й напрями правового регулювання. Вище зазначене дозволяє констатувати належне функціонування державно-політичного та правового механізмів забезпечення кібербезпеки США, механізму розробки політики забезпечення кібербезпеки США.

Розглянемо інституційний та організаційно-адміністративний механізми забезпечення кібербезпеки США.

Інституційний механізм забезпечення кібербезпеки США охоплює собою три управлінських рівні на яких відбувається функціональна взаємодія держави, національного бізнесу та приватно-державне партнерство.

Стратегічний управлінський рівень включає:

Міністерство оборони, якому підпорядковується Агентство національної безпеки;

Міністерство внутрішньої безпеки, до складу якого входить Національне управління кібербезпеки США;

Міністерство юстиції, до складу якого входить ФБР.

Другий управлінський рівень включає в себе Кіберкомандування США та розвідувальну спільноту, третій – регіональні та відомчі підрозділи кіберзахисту [63, с. 21-22].

Зауважимо, що згідно Директиви 21 міністр внутрішньої безпеки США повинен забезпечувати щоденну взаємодію з визначеними відповідальними за конкретні сектори агентствами (SectorSpecific Agency), постійне залучення спеціалізованих можливостей та досвіду відповідального за конкретний сектор агентства, ефективну взаємодію з операторами та власниками об'єктів і систем критичної інфраструктури, місцевими органами влади всіх рівнів. Партнерство з усіма переліченими суб'єктами є імперативом у діяльності Міністерства внутрішньої безпеки [127].

Крім того, що Міністерство внутрішньої безпеки відіграє провідну роль у забезпеченні взаємодії у рамках зусиль, спрямованих на підвищення безпеки та стійкості критичної інфраструктури на національному рівні, це міністерство виконує функції відповідального федерального органу за 10 секторів критичної інфраструктури (у т. ч. для семи секторів на згадане міністерство покладена виключна відповідальність, і ще для трьох – спільно з іншими федеральними органами).

У зв'язку з провідною роллю Міністерства внутрішньої безпеки у системі безпеки та стійкості критичної інфраструктури важливі функції на національному рівні виконує і спеціалізований підрозділ міністерства – Офіс захисту інфраструктури, призначений керувати національними програмами та координувати їх виконання, а також реалізовувати державну політику щодо безпеки та стійкості критичної інфраструктури. Офіс розвиває ефективне партнерство між урядом та приватним сектором, здійснює оцінку уразливості та наслідків з тим, щоб сприяти власникам і

операторам об’єктів і систем, а також партнерам на всіх рівнях державного управління усвідомити ризики для критичної інфраструктури та вжити необхідних заходів щодо їх зниження. Офіс надає інформацію про появу нових загроз та небезпек, забезпечує можливості для навчання з метою управління ризиками щодо критичної інфраструктури.

До складу Офісу захисту інфраструктури входять такі підрозділи:

Відділ збирання інформації про інфраструктуру (Infrastructure Information Collection Division);

Відділ дотримання вимог щодо безпеки інфраструктури (Security Compliance Division);

Центр координування національної інфраструктури (National Infrastructure Coordinating Center);

Відділ координації з фізичної безпеки (Protectiv e Security Coordination Division).

Згідно із Директивою 21 [127] на кожний федеральний орган, уповноважений виконувати функції відповідального за сектор агентства, покладено відповідальність за розробку та виконання секторальних планів, у яких концептуальні положення Плану захисту національної інфраструктури мають бути конкретизовані відповідно до унікальних характеристик кожного із секторів та безпекових умов, у яких він перебуває. Секторальні плани мають постійно оновлюватися для того, щоб відповідати положенням чинного Плану захисту національної інфраструктури.

У цій же Директиві на керівників міністерств і федеральних агентств покладено відповідальність за ідентифікацію та оцінку загроз національній безпеці. Зокрема на міністра внутрішніх справ покладено обов’язки щодо оцінки проблем захисту критично важливих об’єктів інфраструктури [198, с. 105-106].

В рамках Комплексної національної ініціативи з питань кібербезпеки реалізовується завдання інформаційно-аналітичного забезпечення

кібербезпеки США, а саме забезпечення ситуаційної обізнаності у сфері кібербезпеки в межах державних установ й приватного сектора [126].

Інформаційно-аналітичний механізм забезпечення кібербезпеки США наразі сформований й функціонує відповідно до вимог офіційно прийнятих стандартів аналітичної діяльності у сфері національної безпеки та стандартів у сфері кібербезпеки [126; 198].

Наразі механізми реагування на загрози кібербезпеці США структурно представлено:

Секретною службою США для боротьби з економічними й комп'ютерними злочинами;

Федеральним агентством США, яке забезпечує взаємодію між службами, правоохоронними органами й приватними сектором з питань реагування на кіберзлочини;

військовим підрозділом у сфері кібербезпеки;

національним відділом кібербезпеки від Департаменту внутрішньої безпеки;

відділом комп'ютерної злочинності й інтелектуальної власності;

інтернет-поліцією мережевою поліцією [39].

Розглянемо механізми забезпечення управлінської взаємодії та комунікації суб'єктів забезпечення кібербезпеки США.

Зауважимо, що забезпечення ефективного обміну інформацією віднесено до одного з трьох стратегічних імперативів, які мають визначати підходи федеральних органів до забезпечення безпеки та стійкості критичної інфраструктури. Зокрема, у Плані захисту національної інфраструктури (2013) досягнення обміну придатною до використання та відповідною інформацією у рамках спільноти критичної інфраструктури з метою формування усвідомлення та підтримки процесу прийняття рішень віднесено до п'яти стратегічних цілей, на яких упродовж кількох найближчих років має бути сфокусована діяльність у цій сфері.

План захисту національної інфраструктури реалізується через управління ризиками та розбудови партнерства, одним з основних інструментів для яких є обмін інформацією між усіма учасниками процесу захисту критичної інфраструктури.

Директива 21 (PPD-21) на міністра внутрішньої безпеки покладено відповідальність за належне функціонування центрів з питань національної критичної інфраструктури, які забезпечують [127]:

можливості для отримання інформації про поточну ситуацію на об’єктах і в системах критичної інфраструктури;

узагальнення та підготовку інформації про появу нових трендів, неминучих загроз та розвиток інцидентів і криз на об’єктах та в системах критичної інфраструктури.

Відповідно до уточненої структури у сфері управління Міністерства внутрішньої безпеки мають функціонувати центри з питань фізичної інфраструктури та з питань кіберінфраструктури. Обидва повинні діяти як єдиний комплекс та слугувати координаційними центрами для партнерів міністерства, де вони можуть отримувати інформацію про конкретні умови на тому чи іншому майданчику, а також зведену, готову до використання інформацію для вжиття заходів з фізичної та кібербезпеки на об’єктах і в системах безпеки та стійкості критичної інфраструктури.

У взаємодії з відповідальними за сектори безпеки та стійкості критичної інфраструктури агентствами та іншими федеральними органами міністр має сприяти наданню доступу власникам і операторам до інформації (у т. ч. розвідувальної), необхідної для забезпечення безпеки та стійкості безпеки та стійкості критичної інфраструктури, підтримувати заходи з обміну такою інформацією між усіма суб’єктами процесу.

Положення чинного Плану захисту національної інфраструктури (2013) у частині обміну інформацією узгоджені з Національною стратегією обміну інформацією та її захистом (2012) (National Strategy for Information Sharing and Safeguarding 2012), відповідно до якої мають бути створені

механізми та протоколи обміну інформацією державних органів з приватними партнерами в рамках конкретних секторів з тим, щоб забезпечити належну якість і своєчасність інформації, необхідної для захисту національної інфраструктури.

У США перші кроки в напрямі системної розбудови державно-приватного партнерства (ДПП) у сфері захисту критичної інфраструктури були зроблені після 2005 року. Зокрема, у Плані захисту національної інфраструктури (2006) було визначено Модель секторального партнерства (Sector Partnership Model) як основу для координування діяльності щодо захисту критичної інфраструктури та ключових активів на всіх рівнях управління та в рамках усіх секторів критичної інфраструктури. У подальші роки в оновлених версіях цього державного документа зазначена модель уточнювалась.

Відповідно до Директива 21 [127], окрім секторів критичної інфраструктури та відповідальних за сектори, визначено механізми та інструменти забезпечення секторального та міжсекторального партнерства:

урядові координувальні ради (Government Coordinating Councils), призначені для координування виконання урядових стратегій, програм та забезпечення зв’язків між урядовими органами;

секторальні координувальні ради (Sector Coordinating Councils), що утворюються на добровільній основі та призначені для координації виконання стратегій і здійснення відповідної діяльності власників та операторів об’єктів і систем критичної інфраструктури;

міжсекторальні ради (Cross-Sector Councils) – створено три структури: Партнерство для безпеки критичної інфраструктури (координує діяльність представників приватного сектору); Рада вищих федеральних керівників (Federal Senior Leadership Council), призначення якої – координувати інтереси федеральних органів; Рада координації діяльності

штатів, місцевих органів управління, призначена для координації всіх інших державних органів нефедерального рівня.

Усі ці ради та відповідальні за сектори критичної інфраструктури агентства окремих секторів разом із федеральними органами управління, урядами штатів, регіональними і місцевими органами влади, приватним сектором і неурядовими організаціями повинні співпрацювати при виконанні програм та з метою реалізації підходів до забезпечення безпеки та стійкості критичної інфраструктури, досягнення пов'язаних із цим цілей.

Розглянемо механізм інформаційно-технологічного забезпечення реагування на загрози кібербезпеці США.

США є лідером у запровадженні передових підходів, використанні новітніх технологічних рішень у розв'язанні проблем безпеки та стійкості критичної інфраструктури. Зазначені чинники зумовлюють теперішню ситуацію з підготовкою кадрів і населення за цим безпековим напрямом, яку можна охарактеризувати як бурхливий розвиток. У цій діяльності провідна роль суб'єктів належить Міністерству внутрішньої безпеки, підтвердженням чого можна вважати різноманітність охоплення тем, інструментів і форматів, цільових аудиторій, які спостерігаються в діяльності цього міністерства.

Апробацію дієвості механізму інформаційно-технологічного забезпечення реагування на загрози кібербезпеці США було здійснено в ході навчань Cyber Storm I (2006 р.), Cyber Storm II (2008 р.), Cyber Storm III (2010 р.), навчальної симуляції кібервійни під назвою «Шокова кіберхвиля» (2010 р.), яка дозволила виявити уразливості кібернетичного простору США [18]. Варто додати, що навчальна симуляція кібервійни під назвою «Шокова кіберхвиля» проводилася із залученням фахівців з кібербезпеки таких країн, як: Австрія, Великобританія, Франція, ФРН, Нідерланди, Швеція, Японія.

Зазначене є ознакою функціонування механізму міжнародного й

міждержавного співробітництва з питань забезпечення кібербезпеки та механізму інтеграції кіберпростору США у світовий інформаційний простір.

Як загальний висновок можна зробити те, що система захисту критичної інфраструктури та СКБ в США формувалися шляхом поступових і послідовних політичних, правових, державно-управлінських рішень та дій щодо визначення загального (національного) плану безпеки критичної інфраструктури та кібербезпеки (визначення об'єктів критичної інфраструктури та кібербезпеки, аналіз уразливості, програми щодо запобігання, нейтралізації, ліквідації негативних наслідків реалізації кіберзагроз); створення засад державно-приватного партнерства та взаємодії з визначенням відповідальності у сфері гарантування безпеки критичної інфраструктури та кібербезпеки; створення виконавчих органів, відповідальних за забезпечення безпеки елементів (об'єктів) критичної інфраструктури в різних галузях та кібербезпеки; координації діяльності різних суб'єктів (державний і приватний сектори), що стосуються захисту критичної інфраструктури та кібербезпеки на національному рівні; формування системи інформування та сповіщення щодо загроз критичній інфраструктурі та кібербезпеці.

Розглянемо питання формування нормативно-правової компоненти інституційного середовища кібербезпеки країн-членів НАТО і ЄС.

У 2001 р. Радою Європи було прийнято Міжнародну конвенція про кіберзлочинність. В подальшому європейські країни приймають нормативно-правові акти, що регулюють питання забезпечення національної кібербезпеки, а саме: ФРН приймає Державний план захисту інформаційної інфраструктури (2005 р.) [249], а в 2011 р. Стратегію кібербезпеки [237]. Стратегії кібербезпеки були прийняті Швецією (2006 р.), Естонією, Фінляндією [244], Великобританією (2011 р.) [239], Чехією (2011 р.), Францією (2011 р.) [254], Литвою (2011 р.), [252], Люксембургом [255], Нідерландами [256]. У 2010 р. – Канада [233] та Японія [245]

приймають стратегії кібербезпеки.

Результати порівняльного аналізу стратегій кібербезпеки згаданих держав представлено в [93, с.176-199]. Вітчизняний дослідник Є. Котух констатує, що забезпечення кібербезпеки у публічному секторі визначається двома парадигмами – державницькою та економічною. Перша відображає традиційну роль етатизму, тобто визначальну роль держави в гарантуванні національного цифрового суверенітету, в рамках якого кібербезпека вважається одним із визначальних чинників забезпечення воєнної та економічної безпеки держави. Друга відображає зростаючу роль інтернету в економічному зростання держави та децентралізованого підходу до формування та реалізацій стратегій кібербезпеки в контекстній залежності від рівня інформаційного розвитку конкретного суспільства.

Варто зазначити, що спільною рисою згаданих стратегічних документів у сфері кібербезпеки є визначення спільної відповідальності усіх суб'єктів забезпечення кібербезпеки, а саме держави, бізнесу та громадян. Водночас у цих документах наголошено увагу на доцільності регулювання питання кібербезпеки на регіональному та міжнародному рівнях. Це, на нашу думку, обумовлено перш за все транскордонним характером кіберпростору, комплексним характером кіберзагроз та їхньою гібридизацією в умовах сучасного геополітичного інформаційного протиборства.

Особливістю вказаних стратегій кібербезпеки є реалізація принципів партисипаторного управління та демократичного управління сектором безпеки і оборони, управління ризиками та проактивного реагування на кіберзагрози, національної стійкості. Зокрема, узагальнення та систематизація зарубіжного досвіду, зокрема країн-членів ЄС та НАТО, щодо формування і реалізації політики забезпечення національної стійкості дозволила вітчизняним дослідникам О. Рєзніковій зробити висновки щодо напрямів згаданої політики [173]:

налагодження ефективної взаємодії між державними та недержавними суб'єктами забезпечення національної стійкості;

удосконалення інформаційно-аналітичного механізму забезпечення національної стійкості, зокрема посилення спроможностей органів державної влади, що опікуються питаннями виявлення та ідентифікації загроз національній безпеці;

підвищення рівня обізнаності державних та недержавних суб'єктів забезпечення національної стійкості щодо широкого спектру реальних та потенційних загроз національній безпеці;

перерозподіл відповідальності суб'єктів політики у сфері національної безпеки, а саме спостерігається подолання етатичних тенденцій, що представлено делегуванням більшого обсягу повноважень та обов'язків у безпековій сфері недержавним суб'єктам, місцевим громадам, громадянам. При цьому на державу покладаються завдання щодо створення сприятливих умов для діяльності недержавних суб'єктів, а також координаційні і контрольні функції;

забезпечення безперервності процесу державного управління системою національної стійкості і забезпечення безпеки населення в умовах кризових ситуацій;

забезпечення високого рівня готовності всіх суб'єктів забезпечення національної безпеки до реагування на загрози різного характеру та масштабу;

налагодження стійких двосторонніх каналів комунікації державних органів державної влади і місцевих органів з населенням з питань національної безпеки;

посилення спроможностей всіх суб'єктів забезпечення національної безпеки щодо протидії широкому спектру загроз.

Апробацію дієвості механізму інформаційно-технологічного забезпечення реагування на загрози кібербезпеці країн-членів ЄС було здійснено в ході кібернавчань під назвою Cyber Europe–2010, 2012 [18].

Значним внеском у розвиток згаданого механізму є прийняття першого стандарту по кібербезпеці [248].

У 2010 р. були прийняті Стратегічна концепція НАТО [45] та Європейська стратегія безпеки [15] в яких значна увага приділялася питанням виявлення й адекватному реагуванню на кібератаки.

На початку 2013 р ЄС ухвалив Стратегію кібербезпеки, яка мала на меті гарантування відкритого, надійного і безпечного кіберпростору. В цьому документі було визначено наступні напрямки діяльності суб'єктів забезпечення кібербезпеки країн-членів ЄС [88, с. 10]: кіберстійкість та кібероборона, боротьба із кіберзлочинністю, розвиток технологічного потенціалу в інтересах забезпечення кібербезпеки ЄС, міжнародна кібербезпека. У цьому ж році Європарламент прийняв директиву з питань посилення покарань за кіберзлочини та було відкрито Європейський центр по боротьбі з кіберзлочинністю (ЕС3), основною функцією якого визначено координацію боротьби із кіберзлочинністю у ЄС.

Реалізація Стратегії кібербезпеки ЄС здійснювалася в контексті вимог Стратегії Єдиного Цифрового Ринку та Європейського Порядку Денного з питань безпеки. При цьому на Агентство ЄС з питань мережевої та інформаційної безпеки (ENISA) покладено завдання організації взаємодії країн-членів ЄС у сфері забезпечення безпеки [126].

27 червня 2019 р. набув чинності Регламент про кібербезпеку ЄС, про ENISA та сертифікацію кібербезпеки в галузі інформаційних та комунікаційних технологій. Цей документ має на меті зміцнити спроможність ENISA у сфері надання допомоги країнам-членам ЄС щодо реагування на кіберзагрози [126].

В практиці управління кібербезпекою країн-членів ЄС та НАТО використовуються «Глобальний індекс кібербезпеки» (GCI) та «Національний індекс кібербезпеки» (NCSI) для моніторингу та порівняльної оцінки спроможностей країн до реагування на кіберзагрози. Згадані індекси оцінюють ризики у сфері кібербезпеки для корпоративної, промислової та урядової

інформаційних інфраструктур.

Наразі ЄС як організація має високий показник кібербезпеки за формотворчими критеріями, які складають Глобальний індекс кібербезпеки [216]:

правовий, технічних, організаційний критерії;

критерій спроможності суб'єктів забезпечення кібербезпеки;

критерій міждержавного та міжнародного співробітництва у сфері забезпечення кібербезпеки.

Формування Індексу NCSI ґрунтується на врахуванні таких кіберзагроз, як-от: втручання в систему електронних послуг; порушення цілісності та конфіденційності даних. Реалізація вказаних кіберзагроз порушують нормальний режим функціонування національних комп'ютерних інформаційних систем електронних послуг, що в кінцевому підсумку може спричинити колапс в державному управлінні та економіці [75].

У 2017 р. Естонія, Франція та Норвегія були лідерами ЄС за показником Глобального індексу кібербезпеки, Іспанія посідала 19 позицію [216]. У 2018 р. рейтинг Глобального індексу кібербезпеки очолила Велика Британія, другу місце обійняли США, третє місце посіла Франція [75]. У 2021 р. згідно рейтингу підготовленого Міжнародним союзом телекомунікацій Організації Об'єднаних Націй, Іспанія посіла 7-ме місце у світі [32].

Розглянемо більш докладно досвід Іспанії щодо публічного управління кібербезпекою.

У 2013 р. в Іспанії було схвалено Стратегію національної кібербезпеки [241]. Цей документ слугував правовою основою для діяльності Уряду Іспанії в контексті виконання положень Стратегії національної безпеки (2013 р.) [241] щодо захисту кіберпростору держави, й зокрема щодо реалізації реактивного та проактивного реагування на кіберзагрози.

У розділі І Стратегії національної кібербезпеки [241] надано загальну характеристику кіберпростору, зокрема визначено можливості та загрози, які надає кіберпростір (хакерство, тероризм, шпигунство, саботаж та ін.). В цьому розділі також охарактеризовано сучасні тенденції розвитку інформаційного суспільства в Іспанії, й зокрема акцентовано увагу на тенденції зростання кількості ризиків та загроз кібербезпеці в умовах інформатизації суспільства. При цьому джерелами загроз кібербезпеці Іспанії визначено: іноземні держави, терористичні організації та хакери, організована злочинність. При цьому розкрито причини появи загроз кібербезпеці, а саме причини технічного, соціального та природного характеру.

У розділі ІІ Стратегії національної кібербезпеки [241] визначено місію СКБ Іспанії, а також принципи її функціонування. Зокрема, місією визначено запровадження загальних правил безпечного використання кіберпростору за допомогою комплексного бачення, яке передбачає координацію дій органів державної влади, приватного сектору та громадян, а також міжнародні ініціативи з дотриманням національного і міжнародного права, інших національних та міжнародних стратегічних документів.

Принципами функціонування національної СКБ Іспанії визначено:

національне лідерство і координація зусиль суб’єктів забезпечення кібербезпеки;

спільна відповідальність суб’єктів забезпечення кібербезпеки;

раціональність і ефективність заходів забезпечення кібербезпеки;

міжнародне співробітництво у сфері кібербезпеки.

На основі вказаних принципів здійснюється планування розвитку національної СКБ з особливим акцентом на захисті національних цінностей, які визначено у Конституції Іспанії (1978 р.) [235].

У розділі ІІІ Стратегії національної кібербезпеки [241] детально визначено цілі та завдання національної СКБ.

В офіційнму дискурсі кібербезпеки Іспанії визначено такі національні цілі:

гарантування безпеки інформаційних і телекомунікаційних систем;

спроможність держави щодо ідентифікації, аналізу, оцінки рівня загроз кібербезпеці, прогнозування майбутнього безпекового кіберсередовища;

реактивне й проактивне реагування на загрози кібербезпеці;

стійкість інформаційних і телекомунікаційних систем.

Завданнями СКБ Іспанії є:

1) для органів державної влади – гарантування кібербезпеки та стійкості інформаційних та телекомунікаційних систем, які використовуються в державному управлінні;

2) для об’єктів критичної інфраструктури та підприємств – гарантування кібербезпеки та стійкості інформаційних та телекомунікаційних систем, які використовуються операторами критичної інфраструктури та бізнес-структурами;

3) у судовій та правоохоронній сфері – розширення можливостей з проактивного реагування на кіберзагрози та координації діяльності згаданих суб’єктів забезпечення кібербезпеки у сфері реагування на загрози терористичного та кримінального характеру;

4) у сфері сенсибілізації – підвищення рівня культури кібербезпеки громадян, фахівців бізнес-структур та органів державної влади із кіберзагрозами та ризиками у сфері кібербезпеці;

5) у сфері освіти – формування компетентностей і технологічних можливостей, які є необхідними для досягнення національних цілей у сфері забезпечення кібербезпеки Іспанії;

6) у рамках міжнародного співробітництва – підвищення рівня кібербезпеки Іспанії шляхом координації заходів реалізації політики кібербезпеки на національному, регіональному (на рівні ЄС) та міжнародному рівнях (на рівні ООН), а також шляхом міждержавної

співпраці в галузі освіти.

У розділі IV визначено 8 основних напрямів досягнення національних цілей у сфері забезпечення кібербезпеки*:*

реактивне та проактивне реагування на кіберзагрози;

гарантування кібербезпеки інформаційних і телекомунікаційних систем органів державної влади;

гарантування кібербезпеки інформаційних і телекомунікаційних систем на об'єктах критичної інфраструктури;

боротьба із кіберзлочинністю та кібертероризмом;

гарантування безпеки і стійкості ІКТ приватного сектора;

здобуття фахівцями у сфері кібербезпеки відповідних професійних компетенцій, впровадження інноваційних технологій забезпечення кібербезпеки;

формування культури кібербезпеки;

виконання міжнародних зобов'язань у сфері забезпечення кібербезпеки.

У розділі V визначено місце СКБ в системі національної безпеки Іспанії, а також визначається її інституційна структура.

Прийняття Стратегії національної безпеки Іспанії (2013 р.) є свідченням належного функціонування державно-політичного механізму забезпечення кібербезпеки Іспанії, й водночас розвитку правового механізму забезпечення кібербезпеки Іспанії. Прийняття згаданої стратегії заклало основу для належного функціонування механізму розробки політики забезпечення кібербезпеки та комплексного механізму реалізації політики забезпечення кібербезпеки Іспанії.

Є сенс зауважити, що в Стратегії національної безпеки Іспанії (2017 р.) на відміну від редакції 2013 р. акцентовано увагу на боротьбі з дезінформацією [216]. Це, в свою чергу висувало додаткові вимоги до національної СКБ Іспанії щодо реагування на загрози кібербезпеці, що знайшло своє відображення у новій редакції Національної стратегії

кібербезпеки (2017 р.) [32].

У 2019 р. була затверджена нова редакція Національної стратегії кібербезпеки, в якій визначено п’ять цілей й сім напрямків діяльності щодо досягнення згаданих цілей [32].

Позитивним є те, що починаючи з 2013 р. керівництво Іспанії періодично оновлює керівні документи у сфері забезпечення кібербезпеки відповідно до вимог динамічного безпекового кіберсередовища щодо своєчасного й адекватного реагування на загрози кібербезпеці. Це є свідченням належного функціонування соціально-психологічного механізму усвідомлення проблем забезпечення кібербезпеки, який дозволяє здійснювати рефлексивне управління з метою адаптації СЗКБ Іспанії до вимог динамічного безпекового кіберсередовища.

Організаційний компонент інституційного середовища публічного управління кібербезпекою Іспанії формує інституційний та організаційно-адміністративний механізми забезпечення кібербезпеки, механізми державного реагування на загрози кібербезпеці, механізм забезпечення управлінської взаємодії суб’єктів забезпечення кібербезпеки; фінансовий механізм забезпечення кібербезпеки, механізми міжнародного й міждержавного і співробітництва, інтеграції національного кіберпростору у світовий кіберпростір, механізм забезпечення комунікації суб’єктів забезпечення кібербезпеки, механізми контролю стану кібербезпеки.

Інституційний механізм забезпечення кібербезпеки Іспанії представлено трьома органами, що безпосередньо опікуються питаннями кібербезпеки, а саме:

Радою національної безпеки Іспанії;

Спеціалізованим комітетом з кібербезпеки. Останній надає допомогу Раді національної безпеки Іспанії з питань реалізації політики забезпечення кібербезпеки, а також координує державно-приватне партнерство;

Ситуативним спеціалізованим комітетом. Останній за допомогою

Ситуативного центру, який є структурним підрозділом Департаменту національної безпеки Секретаріату Глави Уряду Іспанії управляє кризовими ситуаціями в кіберпросторі [241];

Національним Центром із захисту критичної інфраструктури (CNPIC), який є відповідальним за кібербезпеку критичної інфраструктури та координацію й співпрацю між державними та приватними інституціями з питань безпеки критичної інфраструктури. Одним із завдань CNPIC є створення робочих Груп, які розробляють секторальні плани забезпечення кібербезпеки [88, с. 17].

Інституційний механізм забезпечення кібербезпеки Іспанії представлено також Національним центром розвідки Іспанії, основним завданням якого визначено надання уряду необхідної інформації про загрози національній безпеці у різних сферах задля організації своєчасного й адекватного реагування на виявлені загрози.

Механізми реагування на загрози кібербезпеки Іспанії структурно включає в себе відповідні сили сектору безпеки і оборони Іспанії, функціональним призначенням яких є забезпечення кібербезпеки:

CCN-CERT – команда реагування на інциденти у сфері кібербезпеки, яка підпорядковується Національному криптологічному центру та підзвітна Іспанському національному центру розвідки;

Національний центр захисту інфраструктури та кібербезпеки;

Центр реагування на інциденти у сфері кібербезпеки для громадян та приватних компаній Іспанії, який підпорядкований Іспанському національному інституту кібербезпеки [58, с. 65-76; 126].

Стратегією кібербезпеки Іспанії (2013 р.) [241] було передбачено функціонування:

самоорганізаційного компоненту інституційного середовища публічного управління кібербезпекою, що забезпечує здійснення державно-приватного партнерства у сфері забезпечення кібербезпеки, партисипаторного управління у цій сфері. В рамках вказаного компоненту

формуються та функціонують механізм партисипаторної взаємодії, механізм забезпечення комунікації суб'єктів забезпечення кібербезпеки;

соціокультурного компоненту інституційного середовища публічного управління кібербезпекою, який забезпечує поширення цінностей культури кібербезпеки. В рамках вказаного компоненту формується та функціонує інформаційний механізм забезпечення кібербезпеки Іспанії.

Приладом функціонування вказаних механізмів забезпечення кібербезпеки Іспанії є:

організована органами державної влади «гаряча лінія». Функціональне призначення останьої полягає у кіберзахисті дітей від шкідливого контенту, у підвищенні обізнаності щодо кібезагроз, у налагодженні співпраці між державою, бізнесом, громадянським суспільством з питань забезпечення кібербезпеки [88, с. 17];

створення у 2020 р. Національного форуму із кібербезпеки. Функціональне призначення згаданої організації є поширення цінностей культури кібербезпеки, надання підтримки державно-приватному співробітництву під егідою Ради національної безпеки Іспанії [32];

державно-приватне партнерство у сфері забезпечення кібербезпеки реалізується за допомогою асоціації «Іспанський кластер інновацій у кібербезпеці», Іспанської технологічної платформи з промислової безпеки [126].

Когнітивний компонент інституційного середовища публічного управління кібербезпекою Іспанії представлено механізмом науково-методичного забезпечення кібербезпеки Іспанії до складу якого входять: Вищий центр досліджень національної оборони [234], Іспанський інститут стратегічних досліджень [246], Іспанський національний інститут кібербезпеки [201], Іспанський кластер інновацій в кібербезпеці, Іспанська технологічна платформа з промислової безпеки [126].

Попередньо підсумуємо: наразі механізми формування і реалізації

політики забезпечення кібербезпеки країн-членів НАТО і ЄС є досить ефективними й адаптивними в умовах сучасного геополітичного інформаційного протиборства. Позитивним моментом є те, що наразі державно-управлінська еліта країн-членів НАТО і ЄС у своїй діяльності щодо забезпечення кібербезпеки приділяє рівнозначну увагу як питанням довгострокової, так і поточної політики у цій сфері. Зокрема, довгострокова державна політика забезпечення кібербезпеки спрямована на вирішення важливих стратегічних питань – прогнозування змін безпекового кіберсередовища та майбутніх тенденцій розвитку загроз кібернетичного характеру, побудова принципово нової СЗКБ, яка б враховувала майбутні трансформації безпекового кіберсередовища (нові загрози та виклики кібербезпеці). Поточна державна політика забезпечення кібербезпеки спрямована на вирішення тактичних та оперативних питань державної політики у цій сфері – реактивне та проактивне реагування на загрози кібербезпеці.

В рамках системно-ситуаційного підходу щодо оцінки можливостей запровадження зарубіжного досвіду забезпечення національної безпеки, що запропонований в [219] дозволив нам здійснити оцінку можливостей впровадження позитивного досвіду країн-членів ЄС та НАТО щодо забезпечення кібербезпеки у публічно-управлінську практику України у цій сфері. Зокрема, оцінка можливостей впровадження досвіду Іспанії щодо забезпечення кібербезпеки в Україні нами представлено в [83].

На нашу думку, досвід країн-членів ЄС та НАТО у сфері забезпечення кібербезпеки може бути використаний в Україні щодо:

а) проектування СКБ шляхом визначення перспективної моделі СКБ на основі задіяння таких компонентів забезпечення кібербезпеки, як-от:

досконала нормативно-правова база в галузі гарантування національної кібербезпеки країн-членів ЄС та НАТО, кібербезпеки згаданих регіональний інтеграційних інституцій;

національна стійкість СЗКБ;

високі технологічні спроможності сил СЗКБ держави;

ефективні системи державно-приватного партнерства у сфері забезпечення кібербезпеки;

ефективна система планування політики забезпечення кібербезпеки у різних секторах;

високий рівень професійної освіти фахівців у сфері кібербезпеки.

б) формування інституційного середовища публічного управління кібербезпекою з урахуванням вимог динамічного безпекового кіберсередовища до національної СКБ;

в) державне конструювання СКБ та її складової СЗКБ.

2.3. Оцінка стану та можливостей державних механізмів забезпечення кібербезпеки України в умовах російсько-української війни

Є сенс зауважити, що перебіг соціальних змін в Україні після 1991 р. суттєво вплинув на розвиток інституціонального середовища українського суспільства, що в свою чергу, визначило напрямок розвитку інституціонального середовища державного управління у сфері інформаційної безпеки, й в подальшому публічного управління у сфері кібербезпеки.

Розвиток інституціонального середовища публічного управління кібербезпекою визначається такими базовими соціальними інститутами, як-от:

інститутом міжнародного права, що регулює міжнародні інформаційні відносини та регламентує діяльність міжнародних організацій щодо гарантування міжнародної інформаційної безпеки та взаємодії з національними державами з питань забезпечення кібербезпеки [7; 20; 39; 71];

соціально-правовим інститутом, що регулює в рамках міжнародного права суспільно-інформаційні відносини та інформаційний розвиток

сучасних національних держав [29];

інститутом глобального громадянського суспільства, що регулює відносини між організаціями і громадами, коаліціями і громадськими рухами, громадськими і бізнес-ініціативами у міждержавному відкритому соціальному просторі, який сповнений конфліктів і компромісів, що стають відчутними на національному рівні та у планетарному масштабі [116];

інститутом соціального партнерства, що регулює взаємодію конкретного громадянського суспільства та держави з актуальних питань життєдіяльності суспільства та суспільного розвитку [177];

інститутом державно-приватного партнерства, що унормовує партнерські відносини держави та приватного сектору у різних сферах життєдіяльності суспільства [88; 93];

інститутом взаємодії держави та ІТ-ринку, що регулює відносини держави з ІТ-компаніями, які виникають між економічними агентами в процесі матеріально-технічного і фінансового забезпечення діяльності ІТ-компаній, обміну товарами, послугами, ресурсами [101];

інститутом публічного управління, що регулює управлінську діяльність на основі високого рівня розвитку соціального партнерства щодо суспільного розвитку, політики розвитку держави та національної безпеки [177].

Базовими соціальними інститутами, які формують зовнішнє інституціональне середовище публічного управління у сфері кібербезпеки, що задає зовнішній контур обмежень для вибору альтернатив у сфері забезпечення кібербезпеки України в сучасних реаліях є [92]:

інститут національної безпеки;

інститут права в галузі національної безпеки;

інститут політики національної безпеки;

інститут державного управління;

інститут публічної політики;

інститут політичної комунікації;

інститут інформаційного розвитку суспільства.

Внутрішнє інституціональне середовище публічного управління у сфері кібербезпеки України в сучасних реаліях формується під безпосереднім впливом таких базових соціальних інститутів, як-от [92]:

інститут забезпечення національної безпеки;

інститут права, що регулює взаємодію суб'єктів забезпечення національної безпеки;

інститут партисипаторної взаємодії суб'єктів забезпечення національної безпеки і громадськості;

інститут удосконалення архітектури публічного управління національною безпекою, що передбачає використання моделі зміни «соціокультурного поля» управлінської діяльності у вказаній сфері;

інститут мережевого управління, що регулює перехід системи публічного управління від ієрархічного управління до управління за допомогою мережевих структур;

інститут електронного урядування, що регулює адаптацію державного управління до нових вимог суспільного розвитку на основі впровадження новітніх інформаційних і комунікаційних технологій.

Внутрішнє інституціональне середовище публічного управління кібербезпекою України структурно містить такі компоненти:

1. Нормативно-правовий компонент інституціонального середовища публічного управління кібербезпекою представлено двома рівнями, а саме:

а) національно-правовий рівень, що визначає загальні напрями і пріоритети політики забезпечення кібербезпеки, порядок взаємодії суб'єктів забезпечення кібербезпеки, принципи і норми їх діяльності. На цьому рівні інституціонального середовища функціонують:

інститут публічного управління кібербезпекою, що регулює питання мережевої взаємодії уряду, IT-бізнесу, громадянського суспільства у сфері забезпечення кібербезпеки.

Похідними від інституту публічного управління кібербезпекою є:

інститут права, що регулює питання розробки та легітимізації публічної політики забезпечення кібербезпеки;

інститут права, що регулює питання розробки та реалізації державної політики забезпечення кібербезпеки України;

інститут забезпечення кібербезпеки, що регулює діяльність суб'єктів забезпечення кібербезпеки;

інститут права, що регулює питання моніторингу і контролю за реалізацією державної політики забезпечення кібербезпеки;

інститут права, що регулює питання публічного аудиту публічного управління кібербезпекою суб'єктами публічної сфери та громадянського суспільства;

б) об'єктно-правовий рівень, що конкретизує інституціонально-правові норми щодо державного реагування на загрози кібербезпеці. На цьому рівні інституціонального середовища функціонує інститут права, що регулює питання державно-управлінського впливу на кібернетичну сферу та державного реагування на загрози кібербезпеці.

2. Організаційний компонент інституціонального середовища публічного управління кібербезпекою представлено інститутом організації державного реагування на виклики та загрози кібербезпеці, який є похідним від інституту забезпечення кібербезпеки.

Наразі інститут організації державного реагування на загрози кібербезпеці України функціонує на трьох рівнях державного управління національною безпекою:

а) на стратегічному рівні державного управління кібербезпекою, що представлений такими інституціями, як: Комітет Верховної Ради України з питань національної безпеки і оборони, РНБО України, Конституційний суд і Верховний суд України, та інші органи, які визначають державну політику національної безпеки і виконують роль головних регуляторів відносин у сфері забезпечення національної безпеки.

На цьому рівні державного управління кібербезпекою здійснюється проактивне реагування на загрози кібербезпеці, яке спрямоване на запобігання загрозам кібербезпеці;

б) на оперативно-тактичному рівні державного управління кібербезпекою, що представлений такими інституціями, як: Міністерство оборони України, Міністерство юстиції України, Міністерство внутрішніх справ України, Міністерство цифрової трансформації, Служба безпеки України;

в) на оперативному рівні державного управління кібербезпекою, що представлений такими організаційними елементами, як:

Держспецзв'язок;

силами сектору безпеки – Служба безпеки України, Національна поліція України, Національна гвардія України [146; 147; 163];

обласними та районними державними адміністраціями, місцевими органами самоврядування.

На оперативно-тактичному та оперативному рівнях державного управління кібербезпекою здійснюється реактивне реагування на виклики та загрози кібербезпеці, що спрямоване на мінімізацію існуючих загроз, локалізацію і ліквідацію наслідків їх реалізації.

Наразі ціннісно-нормативна, технологічна та організаційна складові інституту організації державного реагування на виклики та загрози кібербезпеці сформовані.

3. Компонент самоорганізації інституціонального середовища публічного управління кібербезпекою представлено інститутом партисипаторної взаємодії «держави – ІТ-бізнесу – суспільства» з питань забезпечення кібербезпеки, що репрезентує формальні та неформальні правила взаємодії складових тріади «держава – ІТ-бізнес – суспільство» з питань формування та легітимізації публічної політики забезпечення кібербезпеки.

Інститут партисипаторної взаємодії «держави – ІТ-бізнес –

суспільства» з питань забезпечення кібербезпеки структурно представлено такими інституціями, як: Президент України, РНБО України, Міністерство цифрових трансформацій повноваження яких з питань партисипаторної взаємодії з інститутами громадянського суспільства в інтересах національної безпеки визначено в чинному законодавстві [136; 137; 149; 154].

4. Соціокультурний компонент інституціонального середовища публічного управління кібербезпекою представлено інститутом культури безпеки [81; 104], складовими якої є інформаційна культура, культура кібербезпеки, управлінська культура у сфері забезпечення кібербезпеки. Зокрема, управлінська культура у сфері забезпечення кібербезпеки специфічним чином впливає на інститут державного реагування на загрози кібербезпеці, а також є основою цілепокладання вказаної системи діяльності [81].

Наразі ціннісно-нормативна та організаційна складові інститутів інформаційної культури, культури кібербезпеки, управлінської культури у сфері забезпечення кібербезпеки частково сформовані [81; 104].

5. Когнітивний компонент інституціонального середовища публічного управління кібербезпекою представлено реалізацією таких функцій, як:

дослідження закономірностей забезпечення кібербезпеки;

формування самостійного пізнавального напряму наукових шкіл у сфері кібербезпеки, а також науково-дискусійного середовища, засобів і методів накопичення і передачі знання у цій специфічній сфері.

Напрямами наукового пошуку у сфері забезпечення кібербезпеки України є:

розробка і вдосконалення загальної теорії і методології кібербезпеки [18; 20; 48; 51; 93];

розвиток спеціальних наукових теорій в наочному полі кібербезпеки, таких як міжнародна кібербезпеки, національна кібербезпеки [111], а

також об'єктно-орієнтованих спеціальних теорій, до яких можна віднести кібербезпеку особи, суспільства, держави [106; 112; 113; 117];

створення науково-консультативних структур за участю провідних учених країни, наприклад Національний інститут стратегічних досліджень, Національна Академія Наук України та ін. [138];

формування наукових підрозділів у структурі вищих навчальних закладів України і шкіл, що розробляють проблематику кібербезпеки в різних її теоретичних та прикладних аспектах [88-92];

реалізація науково-дослідних авторських проектів у сфері кібербезпеки, що забезпечує органи вищої державної влади необхідними науковими підходами при прийнятті державно-управлінських рішень [121];

науковий дискурс кібербезпеки [53; 61-65; 131-133].

Внутрішнє інституціональне середовище публічного управління кібербезпекою України формує інституційну матрицю кібербезпеки України. Остання структурно містить сукупність соціальних інститутів, які склалися історично та регулюють діяльність суб’єктів забезпечення кібербезпеки України.

Вказана матриця являє собою своєрідний адаптер, що забезпечує:

органічну трансформацію (перехід) від чинників базового рівня, що представлено базовими соціальними інститутами, які визначають зміни в інституціональному середовищі публічного управління кібербезпекою до чинників конкретної сфери застосування, а саме зовнішнього та внутрішнього інституціонального середовища публічного управління кібербезпекою України;

конвергенцію між контуром формування СКБ та її складової – СЗКБ і контуром функціонування згаданих систем**;**

трансформацію сучасних механізмів забезпечення кібербезпеки в механізми майбутнього на основі моделювання, проектування та конструювання СЗКБ України.

Інституціональна матриця кібербезпеки структурно містить інститут кібербезпеки та інститут забезпечення кібербезпеки, а також інститути, які є похідними від них.

Варто зауважити, що інститут кібербезпеки є похідним від:

інституту міжнародного права, що регламентує забезпечення міжнародної кібербезпеки;

інституту державного управління;

інституту права, що регулює соціально-інформаційні відносини в українському суспільстві;

інституту національної безпеки.

Інститут кібербезпеки уособлює собою організаційно-правові засади забезпечення кібербезпеки України та систему державного управління кібербезпекою до складу якої входять – Президент України, Верховна Рада України, міністерства, суди, РНБО України.

Похідним від інституту кібербезпеки України є:

1) інститут права, що регулює питання забезпечення кібербезпеки. Цей інститут є наразі сформованим. Його ціннісно-нормативна складова представлена сукупністю норм і процедур забезпечення кібербезпеки. Організаційна та технологічна складові вказаного інституту представлено правовим механізмом забезпечення кібербезпеки [149; 154];

2) інститут організації державного управління кібербезпекою передбачає визначення суб'єктів забезпечення кібербезпеки України на стратегічному, оперативно-тактичному та оперативному рівнях державного управління національною безпекою. Наразі інституційний механізм забезпечення кібербезпеки України охоплює діяльність інституцій, які представляють суб'єктів забезпечення кібербезпеки, а саме:

Президент України, Офіс Президента України, Кабінет Міністрів України, РНБО України та ін. [122, с. 227-232];

Міністерство цифрової трансформації [137];

Міністерство оборони України [149; 158];

Міністерство внутрішніх справ України [154];

3) інститут державної політики забезпечення кібербезпеки, що регулює питання розробки та реалізації вказаної державної політики. Цей інститут наразі є сформованим й представлено державно-політичним механізмом забезпечення кібербезпеки та механізмом розробки політики забезпечення кібербезпеки. Вказані механізми представлено інституціями є: Президент України, РНБО України, Міністерство цифрових трансформацій, Держспецзв'язок повноваження яких з питань формування та реалізації державної політики забезпечення кібербезпеки визначено в чинному законодавстві [149; 154], а також положення про відповідні державні служби та відомства [136-139; 141; 142; 144; 146; 147; 151; 160; 162-164].

Державна політика забезпечення кібербезпеки України є складовою частиною політики національної безпеки, яка передбачає системну діяльність органів публічної влади із надання гарантій кібербезпеки особі, соціальним групам та суспільству загалом, а саме [149; 154]:

створення умов для своєчасного виявлення джерел загроз кібербезпеці та визначення можливих наслідків їх реалізації;

визначення комплексу превентивних заходів з метою нейтралізації або зменшення негативних наслідків реалізації загроз кібербезпеці;

створення умов для забезпечення своєчасної, релевантної повної і точної інформації для ухвалення державно-управлінських рішень у сфері забезпечення кібербезпеки;

здійснення ефективного (рівноправного, взаємовигідного) міждержавного співробітництва у сфері забезпечення кібербезпеки.

Наразі недоліками державно-політичного механізму забезпечення кібербезпеки України та механізму розробки політики забезпечення кібербезпеки є значна інертність у врахуванні змін в безпековому кіберсередовищі в ході розробки згаданої політики. Прикладом зазначеного може слугувати досить запізніле, в умовах посилення

геополітичного тиску рф на ЄС та ведення гібридної війни росією проти України, затвердження Стратегії інформаційної безпеки України (затверджена 2021 р.) [152] та Стратегії кібербезпеки України (затверджена 2016 р.) [154], Закону України «Про основні засади забезпечення кібербезпеки України» (прийнято 2017 р.) [149].

4) інститут партисипаторної взаємодії в СЗКБ України визначає норми, правила та процедури взаємодії держави, ІТ-бізнесу та суспільства за питань забезпечення кібербезпеки. Структурно цей інститут представлено механізмом партисипаторної взаємодії в СЗКБ, що включає в себе: Верховну Раду України, Президента України та РНБО України [145], громадські ради при центральних та місцевих органах виконавчої влади [202].

Механізм партисипаторної взаємодії в СЗКБ України покликаний організувати взаємодію «держава – громадянське суспільство» з питань розробки та реалізації політики у сфері кібербезпеки. Зауважимо, що особливістю сучасного етапу державного будівництва в Україні є зростання ролі громадянського суспільства у вирішенні соціально-значущих питань, й зокрема у сфері кібербезпеки. Так, наразі чільне місце у загальній структурі суб'єктів кібербезпеки України посідає громадянське суспільство, яке інтенсивно розвивається й справляє значний, а інколи й визначальний вплив на процеси забезпечення кібербезпеки України. Зокрема, при міністерствах постійно діють громадські ради, які покликані приймати активну участь в розробці державної політики у різних сферах національної безпеки та контролювати виконання згаданої політики [93].

Аналіз стану механізму партисипаторної взаємодії в СЗКБ України дозволив виявити низку зовнішніх й внутрішніх факторів, що гальмують процес інституалізації соціального партнерства у згаданій системі [48; 93]:

а) фактори зовнішнього середовища:

недосконалість нормативно-правової бази соціального партнерства у сфері національної безпеки загалом, й у сфері кібербезпеки зокрема;

незавершеність процесу інституціоналізації соціального партнерства у сфері національної безпеки загалом, й у сфері кібербезпеки зокрема;

відсутність релевантної інформації про взаємодію суб'єктів соціального партнерства у сфері забезпечення кібербезпеки.

Похідним від інституту кібербезпеки України також є інститут забезпечення кібербезпеки України, що регулює процеси функціонування СЗКБ, яка реалізовує комплекс завдань державного реагування на загрози кібербезпеці. Становлення та розвиток інституту забезпечення кібербезпеки України відбувався в контексті розвитку інституційної структури системи забезпечення інформаційної безпеки України. Наразі ціннісно-нормативна, технологічна та організаційна складові інституту забезпечення кібербезпеки України частково сформовані. Водночас, цей інститут структурно представлено такими механізмами забезпечення кібербезпеки, що є структурними елементами комплексного механізму реалізації політики забезпечення кібербезпеки, як-от:

1) організаційно-адміністративний механізм забезпечення кібербезпеки України, що містить в собі комплекс офіційно визначених правил і процедур діяльності суб’єктів забезпечення кібербезпеки згідно вимог чинного законодавства у цій сфері. Ці норми і правила викладені в Стратегії кібербезпеки України [154], Положенні про Державну службу спеціального зв’язку [141].

Наразі актуальними проблемами функціонування вказаного механізму є:

неопрацьованість підходів щодо впровадження стандартів НАТО щодо кризового реагування;

відсутність норм та правил організації і координації дій суб’єктів забезпечення кібербезпеки у сфері кризового менеджменту;

відсутність норм та правил управління ризиками у сфері кібербезпеки та проактивного підходу до нейтралізації кіберзагроз;

2) інформаційний механізм забезпечення кібербезпеки України, що

містить в собі комплекс взаємопов'язаних інституцій, які є необхідними для досягнення цілей інформаційного супроводження політики забезпечення кібербезпеки України, а саме:

Національний координаційний центр кібербезпеки [160];

центр Стратегічних комунікацій та інформаційної безпеки при Міністерстві культури та інформаційної політики [165; 217];

Центр протидії дезінформації при РНБО України [139].

3) інститут інформаційно-аналітичної діяльності в СЗКБ України. Цей інститут сформовано, при цьому його ціннісно-нормативна складова представлена сукупністю норм і процедур державно-управлінської аналітики, які досить розлого представлено в [198]. Водночас, організаційна та технологічна складові вказаного інституту представлено державним механізмом інформаційно-аналітичного забезпечення кібербезпеки, який структурно включає в себе інформаційно-аналітичні служби міністерств і відомств, що опікуються питаннями забезпечення кібербезпеки, розвідувальну спільноту, Головний ситуаційний центр України, Національний координаційний центр кібербезпеки, ситуаційні центри сил безпеки і оборони України [139; 160; 197], неурядові аналітичні центри.

Порівняльний аналіз переліків загроз, які наведені у офіційному та науковому дискурсах кібербезпеки України дозволяє констатувати:

1) в офіційному дискурсі кібербезпеки України актуальними загрозами визначено загрози критичній інформаційній інфраструктурі та державним електронним інформаційним ресурсам, низький рівень ефективності СЗКБ [154];

2) в науковому дискурсі визначено такі загрози кібербезпеці, як-от [48; 51; 68; 69; 74; 95-100]:

кіберзлочинність та інформаційний тероризм;

несанкціонований доступ до інформаційних ресурсів органів державної та місцевої влади, бізнесових структур, інститутів

громадянського суспільства та окремих громадян;

перехоплення інформації в телекомунікаційних мережах;

низький рівень розвитку вітчизняних наукоємних виробництв у сфері телекомунікаційних засобів і технологій;

недостатній рівень інформатизації сфери державного управління;

низький рівень розвитку національної інформаційної інфраструктури тощо;

загрози системам підтримки управлінської діяльності: організаційно-правові загрози, апаратно-технологічні загрози, програмно-математичні загрози, фізичні загрози інформаційній інфраструктурі, інформаційно-технічну загрозу;

3) в Концепції забезпечення національної системи стійкості подано трактування терміну «загрози гібридного типу» [159]. Проте, в офіційному дискурсі кібербезпеки України перелік вказаних загроз не визначено.

Є сенс зауважити, що в науковому дискурсі визначено такі загрози інформаційній стійкості Українській державі, як-от [48; 51; 68; 69; 74; 95-100]:

руйнування цілісності національних інформаційно-телекомунікаційних систем, що є передумовою порушення функціональної єдності систем державного і публічного управління, а також системи військового управління;

загрози інформаційній безпеці управлінських структур;

деструктивні інформаційні впливи, що спрямовані на осіб, котрі приймають державно-управлінські рішення;

поширення суб'єктами інформаційної діяльності у світовому інформаційному просторі викривленої та недостовірної інформації, що формує негативний імідж Української держави та завдає шкоди національним інтересам України;

розголошення державної таємниці.

У 2017 р. в ході гібридної війни росією було здійснено низку

кібероперацій проти України: «BugDrop», «WannaCry», «NotPetya» [62, с. 40-41].

Попередньо підсумуємо:

1) ключовим елементом російсько-української війни є кібернетичний чинник, який формує довгострокові виклики для України як національної держави;

2) в офіційному дискурсі наведений перелік загроз кібернетичній безпеці України є неповним і потребує значного доповнення із врахуванням загроз представлених у вітчизняному науковому дискурсі в аспекті власне загроз кібернетичного характеру, що деструктивно впливають на організаційну безпеку держави [107; 166], кібербезпеку держслужбовців, кібербезпеку особи [212] та ін.;

3) в офіційному дискурсі відсутні паспорти загроз кібербезпеці, що перешкоджає впровадженню в державно-управлінську практику стандартів НАТО у сфері забезпечення кібербезпеки та стандартів систем менеджменту інформаційної безпеки.

За даних умов перед Українською державою постало питання удосконалення державного механізму інформаційно-аналітичного забезпечення кібербезпеки з урахуванням нових викликів та загроз кібербезпеці, що з'явилися в ході російсько-української війни. Вказаний механізм має бути удосконалений на основі дотримання принципу інформаційної стійкості;

4) інститут державного реагування на виклики та загрози кібербезпеці, який визначає норми, правила та процедури попередження, запобігання, послаблення, нейтралізацію та усунення кризових ситуацій, зумовлених кібернетичним фактором, а також мінімізацію існуючих загроз та локалізацію і ліквідацію наслідків їх реалізації [149; 154].

Механізм проактивного реагування на загрози кібербезпеки структурно представлено Верховною Радою України, Президентом України, РНБО України та КМУ [149; 154], Міністерством цифрових

трансформацій [137], Головним ситуаційним центром України [164], Національним координаційним центром кібербезпеки [160].

Механізми реактивного реагування на загрози кібербезпеці структурно представлено Державною службою спецзв'язку, силами сектору безпеки – СБУ, Національна поліція України, Національна гвардія України [141; 146; 147; 157; 162; 163], Головним ситуаційним центром України [164], Національним координаційним центром кібербезпеки [160].

За шкалою оцінювання загальної результативності механізму державного реагування на загрози національній безпеці запропонованої в [12, с. 162] на основі фактичних даних ми оцінюємо загальну ефективність механізмів реактивного та проактивного кризового реагування на загрози кібербезпеці як частково результативними (1 бал).

За умов, що скалилися перед Українською державою постало питання удосконалення механізмів реактивного та проактивного реагування на загрози кібербезпеці на основі технологізації процесів вказаного реагування;

5) інститут фінансового забезпечення заходів державного реагування на виклики і загрози кібербезпеці, який визначає норми та процедури вказаного виду забезпечення державно-управлінської діяльності. Структурно цей інститут представлено фінансовим механізмом забезпечення кібербезпеки, що включає в себе Кабінет Міністрів України, Міністерство фінансів України [144]. Основним недоліком функціонування цього механізму є недостатній рівень фінансування потреб забезпечення кібербезпеки України, що обумовлено обмеженістю ресурсів в умовах російсько-української війни;

6) інститут партисипаторної взаємодії в СЗКБ України, який визначає норми, правила та процедури контролю виконання політики забезпечення кібербезпеки з боку громадянського суспільства. Структурно цей інститут представлено механізмом контролю стану кібербезпеки, що включає в себе: громадські ради при центральних та місцевих органах

виконавчої влади [202].

Основним недоліком цього механізму є невизначеність статусу рішень громадських рад при центральних і місцевих органах виконавчої влади з питань національної безпеки і оборони України;

7) кадровий механізм забезпечення кібербезпеки України, який забезпечує підготовку фахівців відповідної кваліфікації у сфері кібербезпеки наразі сформований й структурно включає в себе: Міністерство освіти і науки України, а також профільні ВНЗ [131; 189].

Основним недоліком функціонування цього механізму є низький рівень адаптації системи професійної підготовки фахівців у сфері кібербезпеки до вимог динамічного безпекового кіберсередовища;

8) науково-методичний механізм забезпечення кібербезпеки України сформований й забезпечує взаємодію органів державної влади, що опікуються питаннями кібербезпеки та науково-дослідними інститутами щодо:

напрацювання науково-методологічної бази впровадження новітніх технологій забезпечення кібербезпеки;

вивчення актуальних проблем гарантування кібербезпеки України та обґрунтування шляхів їх вирішення.

Структурно цей механізм включає в себе: РНБО України, Міністерство освіти і науки України, а також профільні наукові установи (Національний інститут стратегічних досліджень та ін.) та ВНЗ [138].

Актуальними проблемами функціонування вказаного механізму є:

відсутність системності в розробці термінологічного апарату проблематики гарантування кібербезпеки України. Зауважимо, що наявні розбіжності у вживанні термінів у нормативно-правових актах [65], що регламентують забезпечення кібербезпеки України, стримує розробку та практичне впровадження сучасних технологій реагування на загрози кібербезпеці та обмежує можливості підвищення ефективності СЗКБ;

відсутність систематизованих знань з проблематики загроз

кібербезпеці різного характеру та реагування на них, зокрема відсутність абстрактно-логічної моделі кібервійни, моделі каскадних ефектів реалізації загроз кібербезпеці негативно впливають на прийняття державно-управлінських рішень щодо реагування на вказані загрози;

відсутність методик діагностування та прогнозування тенденцій розвитку загроз кібербезпеці, а також потенційних каскадних ефектів реалізації вказаних загроз унеможливлюють належну оцінку поточного стану кібербезпеки та визначення майбутнього безпекового кіберсередовища. Такий стан справ у цій сфері вкрай негативно впливає на формування політики забезпечення кібербезпеки України;

відсутність науково обґрунтованих технологій реагування на загрози кібербезпеці, а також відсутність типології діяльності в СЗКБ перешкоджає належному функціонуванню механізмів реагування на загрози кібербезпеці України;

відсутність науково обґрунтованих перспективних функціональної, інформаційної та інституційної моделей СЗКБ унеможливлює проектування та державне конструювання згаданої системи;

9) механізм міжнародного й міждержавного співробітництва з питань забезпечення кібербезпеки. Цей механізм передбачає реалізацію комплексу заходів політичного, економічного та управлінського характеру, спрямованих на гарантування кібербезпеки держав-учасників згаданого співробітництва. Вказаний механізм структурно представлено Верховною Радою України [149], Кабінетом міністрів України [144], Міністерством цифрових трансформацій [137], Міністерством закордонних справ України [122], Міністерством оборони України [154], Державною службою спеціального зв’язку [141].

10) механізм інтеграції кіберпростору України у світовий інформаційний простір, що передбачає реалізацію комплексу заходів спрямованих на входження України у світовий інформаційний простір.

Вказаний механізм структурно представлено Кабінетом міністрів

України [144], Міністерством цифрових трансформацій [137], Міністерством закордонних справ України [122].

11) механізм інформаційно-технологічного забезпечення реагування на загрози кібербезпеці, що передбачає реалізацію комплексу заходів спрямованих на створення умов безпечного використання інформаційних та аналітичних технологій в ході реагування на загрози у згаданій сфері.

Наразі цей механізм сформовано й представлено такими інституціями, як-от: Головним ситуаційним центром України [164], Національним координаційним центром кібербезпеки [160], ситуаційними центрами сил сектору безпеки і оборони України, які наразі перебувають на стадії формування й набуття спроможностей щодо виконання завдань за призначенням;

12) механізм забезпечення управлінської взаємодії суб'єктів забезпечення кібербезпеки структурно представлено такими інституціями, як-от: Головним ситуаційним центром України [164], Національним координаційним центром кібербезпеки [160], ситуаційними центрами сил сектору безпеки і оборони України.

Наразі вказаний механізм перебуває на стадії формування, оскільки мережа ситуаційних центрів ще остаточно не сформована. Ситуаційні центри сил безпеки і оборони України, які введено в експлуатацію на поточний момент набувають спроможностей щодо виконання завдань за призначенням;

13) механізм забезпечення комунікації суб'єктів забезпечення кібербезпеки, що призначений для реалізації такої функції вищої аналітики як стратегічний та оперативний контроль виконання визначених завдань в офіційному дискурсі по забезпеченню кібербезпеки. Цей механізм структурно представлено такими інституціями, як-от: Головним ситуаційним центром України [164], Національним координаційним центром кібербезпеки [160], ситуаційними центрами сил сектору безпеки і оборони України.

Вище зазначене, а також результати наших досліджень [77; 78], аналіз результатів наукових досліджень [8; 9; 18; 48; 51] та джерел [149; 154] дозволило нам виявити актуальні проблеми публічного управління кібербезпекою України, а саме:

проблему забезпечення кібербезпеки України в умовах російсько-української війни, що зумовлені браком систематизованих знань про сучасні технології кібервійни, а також браком аналітичної інформації необхідної для своєчасного й ефективного реагування на виклики та загрози кібербезпеці;

проблему своєчасної адаптації нормативно-правової бази у сфері забезпечення кібербезпеки з урахуванням появи нових викликів, загроз, небезпек кібернетичного характеру;

проблему інституційних розривів між суміжними інститутами зовнішнього та внутрішнього інституціонального середовища публічного управління кібербезпекою, інституційного розриву між загальним станом інститутів кібербезпеки і забезпечення кібербезпеки та складністю безпекового кіберсередовища;

проблему розривів в організації діяльності суб'єктів забезпечення кібербезпеки України;

проблему удосконалення структури, уточнення функцій та конкретизація завдань СЗКБ, а також проблему удосконалення державних механізмів забезпечення кібербезпеки;

проблему низької загальної ефективності механізмів державного реагування на загрози кібербезпеці України.

Є сенс зауважити, що останніми роками СЗКБ України функціонувала в умовах [5; 6]:

вкрай обмежених кадрових, фінансових, організаційних можливостей, а також неготовності всієї СЗНБ України до своєчасного й адекватного реагування на принципово нові загрози, які постали перед Україною в ході російсько-української війни;

низької ефективності діяльності сил сектору безпеки і оборони України у сфері реагування на загрози різного характеру;

глибокої інфільтрації в органах державної влади та структурах сектору безпеки і оборони України російської агентури;

прихованого і відвертого саботажу з боку корупціонерів;

спотворення механізмів державного управління, які покликані були забезпечувати:

верховенство права й неухильне дотримання законодавства щодо захисту прав і свобод громадян, гарантування національної безпеки України;

прозорість видатків на національну безпеку і оборону України й суспільний розвиток;

дієвий контроль у сфері національної безпеки і оборони на основі партисипаторного управління у цій специфічній сфері.

Вищевикладене дозволяє констатувати: в Україні СЗКБ остаточно не сформована й не готова діяти як єдина функціональна структура. Це дає взнаки, що державні механізми забезпечення кібербезпеки України також остаточно не сформовані, й в сучасних умовах російсько-української війни вони не задовольняють потреби СЗКБ щодо своєчасного та адекватного реагування на виклики та загрози кібербезпеці України.

Висновки до другого розділу

1. В розділі доведено, що кібервійна має значну, а інколи й визначальну роль в структурі сучасного геополітичного інформаційного протиборства, а також визначено цілі згаданої війни.

Також в розділі сформульовано закони та закономірності інформаційної глобалістики, інформаційної геополітики, інформаційної війни та кібервійни на основі яких визначено закономірності розвитку СКБ та СЗКБ:

за умов втрати державою спроможності щодо захисту державного

суверенітету, зокрема інформаційного та цифрового суверенітету – обмежуються спроможності її конструктивного впливу на процеси забезпечення інформаційної безпеки та кібербезпеки, інформаційного розвитку суспільства в цілому;

сучасні геополітичні центри сили намагаються підірвати інформаційну могутність своїх конкурентів за допомогою економічних та інформаційно-технічних інструментів, що негативно позначить на функціонуванні та удосконаленні СКБ та СЗКБ країн-конкурентів;

результативність СКБ та ефективність СЗКБ забезпечується врахуванням при проектуванні та конструюванні вказаних систем динаміки трансформацій безпекового кіберсередовища.

Використовуючи модель взаємообумовленості законів, закономірностей і принципів державного управління розглянуто механізм опредмечування закономірностей публічного та державного управління кібербезпекою та виокремлено:

а) дві групи принципів публічного управління кібербезпекою:

принципи, які визначають зміст публічного управління у цій сфері;

принципи організації процесу публічного управління кібербезпекою;

б) дві групи принципів державного управління кібербезпекою:

принципи, які визначають зміст державного управління у цій сфері;

принципи організації процесу державного управління кібербезпекою.

2. В розділі доведено, що наразі механізми формування і реалізації політики забезпечення кібербезпеки країн-членів НАТО і ЄС є досить ефективними й адаптивними в умовах сучасного геополітичного інформаційного протиборства. Позитивним моментом є те, що державно-управлінська еліта країн-членів НАТО і ЄС у своїй діяльності щодо забезпечення кібербезпеки приділяє рівнозначну увагу питанням довгострокової та поточної політики у цій сфері. Зокрема, довгострокова державна політика забезпечення кібербезпеки спрямована на вирішення важливих стратегічних питань – прогнозування змін безпекового

кіберсередовища та майбутніх тенденцій розвитку загроз кібернетичного характеру, побудова принципово нової СЗКБ, яка б враховувала майбутні трансформації безпекового кіберсередовища (нові загрози та виклики кібербезпеці). В рамках довгострокової політики забезпечення кібербезпеки формується інституційне середовище управління кібербезпекою НАТО та ЄС, в країнах-членів згаданих організацій, а також розробляються стратегічні документи у цій специфічній. Спільними рисами вказаних документів є: визначення спільної відповідальності усіх суб'єктів забезпечення кібербезпеки, а саме держави, бізнесу та громадян; визначення доцільності регулювання питання кібербезпеки на національному, регіональному та міжнародному рівнях, що обумовлено транскордонним характером кіберпростору, комплексним характером кіберзагроз та їхньою гібридизацією в умовах сучасного геополітичного інформаційного протиборства; реалізація принципів партисипаторного управління та демократичного управління сектором безпеки і оборони, управління ризиками та проактивного реагування на кіберзагрози, національної стійкості; сертифікація кібербезпеки в галузі інформаційних та комунікаційних технологій; використання в практиці управління кібербезпекою країн-членів ЄС та НАТО «Глобального індексу кібербезпеки» та «Національного індексу кібербезпеки» для моніторингу та порівняльної оцінки спроможностей країн до реагування на кіберзагрози.

Поточна державна політика забезпечення кібербезпеки НАТО та ЄС спрямована на вирішення тактичних та оперативних питань державної політики у цій сфері – реактивне та проактивне реагування на загрози кібербезпеці.

У розділі було перевірено гіпотезу дисертаційного дослідження, яка підтвердила, що систематизовані знання щодо законів, закономірностей, принципів інформаційної глобалістики, геополітичного інформаційного протиборства, інформаційної війни та кібервійни стали основою визначення перспективних моделей СКБ та СЗКБ. Впровадження вказаних

моделей в практику управління кібербезпекою НАТО та ЄС, країн-членів вказаних організацій дозволило їм розбудувати результативні СКБ та ефективні СЗКБ.

Досвід країн-членів ЄС та НАТО у сфері забезпечення кібербезпеки може бути використаний в Україні щодо:

а) проектування СКБ шляхом визначення перспективної моделі СКБ на основі задіяння компонентів забезпечення кібербезпеки, як-от:

досконала нормативно-правова база в галузі гарантування національної кібербезпеки країн-членів ЄС та НАТО, кібербезпеки згаданих регіональний інтеграційних інституцій;

національна стійкість СЗКБ;

високі технологічні спроможності сил СЗКБ держави;

ефективні системи державно-приватного партнерства у сфері забезпечення кібербезпеки;

ефективна система планування політики забезпечення кібербезпеки у різних секторах;

високий рівень професійної освіти фахівців у сфері кібербезпеки.

б) формування інституційного середовища публічного управління кібербезпекою з урахуванням вимог динамічного безпекового кіберсередовища до національної СКБ;

в) державне конструювання СКБ та її складової СЗКБ.

3. В розділі встановлено, що в ході російсько-української війни, яку розв’язала росія, були застосовані новітні технології боротьби з державністю, а саме технології інформаційної війни та кібервійни. За таких умов, що склалися існує нагальна необхідність удосконалення СЗКБ України з урахуванням появи нових загроз кібербезпеці.

Аналіз інституціональних процесів у сфері забезпечення кібербезпеки України дозволяє зробити висновки про те, що:

інституціональне середовище публічного управління кібербезпекою України остаточно не сформоване, що, в свою чергу, визначальним чином

впливає на формування СКБ та СЗКБ, інституціональної матриці й механізмів забезпечення кібербезпеки;

механізми державного реагування на загрози кібербезпеці також остаточно не сформовані, й відповідно в сучасних умовах російсько-української війни вони в повній мірі не задовольняють потреби вітчизняної СЗКБ щодо своєчасного та адекватного реагування на виклики та загрози кібербезпеці України.

Отже, оцінка сучасного стану СЗКБ України показала, що ця система остаточно не сформована, що не забезпечує її готовність діяти як єдина функціональна структура.

Наразі уповноважені інституції здійснюють лише окремі види забезпечення кібербезпеки, що знижує можливу інтегральну ефективність їхній дій. За таких умов, це може призвести до небезпечної різноспрямованості заходів державного реагування на виклики та загрози кібербезпеці України.

Проведений аналіз сучасного стану СЗКБ та окремих механізмів забезпечення кібербезпеки України дозволяє констатувати:

в Україні функціонує СЗКБ, проте станом на сьогодні вона не готова в повному обсязі виконувати функції та завдання, які на неї покладено згідно чинного законодавства;

функціонування механізмів забезпечення кібербезпеки України відбувається в умовах обмежених ресурсних можливостей, й водночас в умовах неготовності СЗКБ до своєчасного і адекватного державного реагування на загрози кібернетичного характеру;

в Україні не завершено формування механізму інформаційно-аналітичного забезпечення кібербезпеки, що дає взнаки у відсутності дієвої системи моніторингу загроз кібербезпеці, державної методики оцінки загроз кібербезпеці України, а також у незавершеності процесу технологізації інформаційно-аналітичного забезпечення кібербезпеки;

в системі публічного управління кібербезпекою України в повній

мірі не забезпечується необхідна структура процесу узгодження інтересів в тріаді «людина – суспільство – держава» у сфері кібербезпеки;

в системі державного управління кібербезпекою України в повній мірі не забезпечується необхідна структура процесу формування та реалізації стратегічних рішень у сфері кібербезпеки.

Основні результати другого розділу дисертаційного дослідження висвітлено у низці публікацій автора [77; 78; 81; 83].

РОЗДІЛ 3
НАПРЯМИ УДОСКОНАЛЕННЯ ДЕРЖАВНИХ МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ З УРАХУВАННЯМ ДОСВІДУ КРАЇН-ЧЛЕНІВ ЄС ТА НАТО

3.1. Актуальні завдання щодо удосконалення державних механізмів забезпечення кібербезпеки України в сучасних умовах євроінтеграції та зовнішньої агресії

На підставі аналізу результатів наукових досліджень [8; 18; 48; 51; 92; 93; 96; 214] та офіційного дискурсу публічного управління національною безпекою України [44; 136-139; 141-148; 150-153; 155-165], нормативно-правової бази в галузі кібербезпеки України [149; 154] констатуємо, що в умовах динамічного безпекового середовища та гібридної війни функціонує вітчизняна СКБ, що має певні переваги та недоліки.

Перевагами вітчизняної СКБ є:

концептуально-доктринальна визначеність кібербезпеки в офіційному дискурсі публічного управління національною безпекою;

чітке визначення суб'єктів забезпечення кібербезпеки, функції та завдання СЗКБ, а також завдання щодо формування інформаційної стійкості;

визначеність функціональної та організаційно-штатної структури СЗКБ та системи інформаційної стійкості з чітким розподілом компетенції органів, їх повноважень (формування політики забезпечення кібербезпеки та інформаційної стійкості, підготовка і прийняття державно-управлінських рішень у цій сфері, безпосереднє керівництво, інформаційно-аналітичний супровід політики забезпечення кібербезпеки, контроль виконання рішень у сфері забезпечення кібербезпеки), підпорядкування і взаємодія на макро- (держава), мезо-(відомчі,

міжвідомчі відносини) та мікро- (сили сектору безпеки і оборони) рівнях;

сформованість процедурної бази (нормативно визначеного та програмно реалізованого алгоритму) виконання функції управління СЗКБ та системою інформаційної стійкості;

визначеність місця та ролі інститутів громадянського суспільства в публічному управлінні СЗКБ та системою інформаційної стійкості та у виконанні органами влади своїх повноважень у цій сфері;

визначеність етапів, завдань впровадження СЗКБ та системи інформаційної стійкості в публічно-управлінську практику забезпечення національної безпеки;

активна позиція структур українського громадянського суспільства та експертного середовища щодо спонукання органів державної влади та силових структур до виконання своїх функціональних обов'язків у сфері забезпечення кібербезпеки.

Недоліками вітчизняної СКБ є:

не готовність СЗКБ, як складової СКБ України, в повному обсязі виконувати функції та завдання, які на неї покладено згідно чинного законодавства;

механізми забезпечення кібербезпеки України функціонують в умовах обмежених ресурсних можливостей, й водночас в умовах неготовності власне СЗКБ до своєчасного і адекватного державного реагування на загрози кібернетичного характеру;

в Україні не завершено формування систем моніторингу загроз кібербезпеці, розробку державної методики оцінки загроз кібербезпеці України, а також процес технологізації інформаційно-аналітичного забезпечення кібербезпеки;

в системі публічного управління кібербезпекою України в повній мірі не забезпечується необхідна структура процесу формування стратегічних рішень у сфері кібербезпеки.

Слід наголосити, що СЗКБ України, як складова СЗНБ остаточно не

сформована, що не дозволяє останній функціонувати як єдина функціональна структура. Це спонукає до висновку про необхідність виконання певних невідкладних дій щодо реформування вказаної системи.

Сучасний стан СЗКБ України спонукає до висновку про нагальну необхідність термінових дій щодо:

1) удосконалення когнітивної складової інституціонального середовища публічного управління кібербезпекою України шляхом систематизації знань про сучасні технології інформаційної війни, й зокрема кібервійни та мережо-центричної війни;

2) удосконалення організаційної складової інституціонального середовища публічного управління кібербезпекою України:

шляхом завершення інституціоналізації аналітичної діяльності в СЗКБ;

шляхом оптимізації структури, уточнення функцій та конкретизації завдань СЗКБ та механізмів забезпечення кібербезпеки відповідно до умов динамічного безпекового середовища;

шляхом подолання розривів в організації діяльності суб'єктів забезпечення кібербезпеки України;

шляхом подолання розривів між соціальними інститутами, які є базовими й визначальним чином впливають на зміни в інституціональному середовищі публічного управління кібербезпекою України, а також інституційних розривів між суміжними інститутами зовнішнього та внутрішнього інституціонального середовища публічного управління кібербезпекою України, інституційного розриву між загальним станом інституту аналітичної діяльності в СЗКБ та складністю кібернетичної складової безпекового середовища;

3) удосконалення правової складової інституціонального середовища публічного управління кібербезпекою України:

шляхом своєчасної адаптації нормативно-правової бази у сфері забезпечення кібербезпеки України з урахуванням появи нових викликів,

загроз, небезпек кібернетичного характеру;

4) удосконалення самоорганізаціної складової інституціонального середовища публічного управління кібербезпекою України шляхом завершення інституалізації соціального партнерства між державою, інституціями громадянського суспільства та ІТ-бізнесом та подальшим розвитком потенціалу соціального партнерства задля узгодження інтересів учасників розробки політики забезпечення кібербезпеки України;

5) удосконалення соціокультурної складової інституціонального середовища публічного управління кібербезпекою України:

шляхом розвитку інформаційної культури суспільства та культури безпекового поводження в кіберпросторі;

шляхом підвищення цифрової грамотності громадян, що передбачає надання їм відповідних знань, навичок і здібностей, що є необхідними для підтримки цілей кібербезпеки, які визначено в офіційному дискурсі публічного управління кібербезпекою України

шляхом концептуалізації ідейно-світоглядного напрямку протидії загрозам кібербезпеці Україні, що передбачає впровадження проектів підвищення рівня обізнаності суспільства щодо загроз кібербезпеці;

шляхом інституалізації ціннісних основ кібербезпеки.

Варто зазначити, що механізми забезпечення кібербезпеки в Україні сьогодні функціонують в умовах вкрай обмежених ресурсних можливостей та неготовності всієї СЗНБ до своєчасного й адекватного державного реагування на принципово нові виклики, які постали перед Україною в сучасних умовах зовнішньої агресії росії.

За таких умов, що склалися у сфері забезпечення кібербезпеки України, завданнями держави у цій сфері є:

1. Для удосконалення державно-політичного механізму забезпечення кібербезпеки України необхідним є:

розробка та впровадження у вітчизняну публічно-управлінську практику структурно-функціональної моделі публічного управління

кібербезпекою, що дозволить сформулювати терміни цілепокладання, доцільності, диференціації, інтеграції, нормування, обґрунтування засад розбудови, функціонування і шляхів розвитку СКБ та СЗКБ в умовах динамічного безпекового середовища;

чітке розмежування публічного управління кібербезпекою на три складових – публічно-політичну, адміністративну, оперативну;

концептуалізація напрямів державного проектування та конструювання перспективної моделі СЗКБ України та механізмів забезпечення кібербезпеки.

2. Для удосконалення правового механізму забезпечення кібербезпеки необхідним є:

внесення змін до Стратегії кібербезпеки України [154] в частині визначення загроз кібербезпеці з урахуванням реальних та потенційних загроз кібербезпеці України в умовах зовнішньої агресії росії, а також ризиків у сфері кібербезпеки України;

ухвалити законопроект про внесення змін до чинного законодавства України в галузі національної безпеки, яким передбачити:

чіткі механізми запобігання діям громадських організацій і ІТ-компаній, спрямованих на підрив національної безпеки України;

чіткий механізм соціального партнерства між державою, громадськими організаціями та ІТ-бізнесом з питань гарантування кібербезпеки України;

законодавчо визначити адміністративну та кримінальну відповідальність за протиправну діяльність громадських організацій у кібернетичній сфері, що становлять небезпеку для держави, суспільства та окремих громадян.

3. Удосконалення соціально-психологічного механізму усвідомлення проблем забезпечення кібербезпеки, а саме в аспекті організації виконання функціональних завдань системою наукових центрів та вищих навчальних закладів (державних / недержавних), що здійснюють підготовку фахівців

для сектору безпеки й оборони та ІТ-фахівців. Варто зазначити, що рівень розвитку наукових досліджень в Україні в галузі вивчення найбільш актуальних проблем кібербезпеки і їх зв'язку з проблемами національної безпеки і подальшого інформаційного розвитку українського суспільства нині представляється явно недостатнім. Тут необхідно стимулювати проведення цілої низки фундаментальних і прикладних досліджень, спрямованих на формування науково-методологічної бази ефективної політики у сфері забезпечення кібербезпеки. Ця політика повинна, з одного боку, враховувати комплексний характер цієї проблеми, а, з іншого боку, – бути адекватною сучасним викликам і загрозам кібербезпеці.

Починати цю роботу треба буде з формування сучасного термінологічного апарату, який потрібний для вивчення цієї проблеми. Адже до теперішнього часу немає досить чітких наукових визначень змісту таких найважливіших понять, як «публічне управління кібербезпекою», «механізм державного реагування на загрози кібербезпеці» та низки інших. Деякі визначення цих термінів запропоновані в дисертаційній роботі, але вони, звичайно ж, вимагають спеціального обговорення і уточнення. В контексті зазначеного нами пропонується упровадити в публічно-управлінську практику структурно-логічні моделі реалізації функцій «комунікація», «планування», «мотивація», «інформаційно-аналітичне забезпечення прийняття державно-управлінських рішень», «контроль» у публічному управлінні кібербезпекою.

Що ж до тематики самих наукових досліджень проблем забезпечення кібербезпеки, то вони повинні проводитися не лише науковцями в галузі ІТ-технологій, але також й фахівцями інших гуманітарних наук – філософії, політології, соціології, психології, освіти, права, безпекознавства та публічного управління. При цьому представляється необхідним стимулювати проведення міждисциплінарних досліджень у сфері забезпечення кібербезпеки, зокрема дослідження технологій

кібервійни та мереже-центричної війни, дослідження ролі і місця кібернетичного чинника в моделях геополітичного інформаційного протиборства.

4. Удосконалення механізму розробки політики забезпечення кібербезпеки в аспекті:

а) визначення національних цілей у сфері забезпечення кібербезпеки, а також напрямів та принципів діяльності у вказаній сфері в рамках ризик-орієнтованого підходу до забезпечення кібербезпеки та проактивного підходу до нейтралізації кіберзагроз [154];

б) удосконалення механізму партисипаторної (громадської) взаємодії в СЗКБ, що має на меті ефективну взаємодію органів державної влади, які є суб'єктами забезпечення кібербезпеки з громадськими організаціями та ІТ-компаніями в процесі розробки політики забезпечення кібербезпеки передбачає:

подальше забезпечення умов для інституціоналізації інтересів громадських організацій, ІТ-компаній та врахування їх у процесі формування політики забезпечення кібербезпеки України в умовах соціальних трансформацій українського суспільства та динамічного безпекового середовища.

5. Удосконалення комплексного механізму реалізації політики забезпечення кібербезпеки, що структурно містить: механізм науково-методичного забезпечення кібербезпеки, фінансовий, інформаційний, кадровий, інформаційно-аналітичний механізми, механізм партисипаторної взаємодії, механізми державного реагування на загрози кібербезпеці, механізм забезпечення управлінської взаємодії суб'єктів забезпечення кібербезпеки, механізм інформаційно-технологічного забезпечення реагування на загрози кібербезпеці; механізм міжнародного й міждержавного співробітництва з питань забезпечення кібербезпеки, механізм інтеграції кіберпростору України у світовий кіберпростір, механізм забезпечення комунікації суб'єктів забезпечення кібербезпеки, а

саме:

а) Удосконалення кадрового механізму забезпечення кібербезпеки, а саме удосконалення системи підготовки фахівців-управлінців у сфері забезпечення національної безпеки.

Є сенс зауважити, що поточний аналіз сучасного наповнення навчальних планів показує, що проблематика кібербезпеки відсутня у нормативній та варіативній частинах спеціальності «Публічне управління та адміністрування». Такий стан справ вимагає удосконалення змісту навчальних дисциплін підготовки магістрів публічного управління вказаної спеціальності.

З метою подальшого удосконалення підготовки магістрів публічного управління за спеціальністю «Публічне управління та адміністрування» до змісту навчальних дисциплін пропонуємо включити:

спеціальну тему з проблем забезпечення кібербезпеки, а саме кейс-стаді «Паспортизація загроз кібербезпеці»;

до кейс-стаді «Технології державного реагування на загрози національній безпеці» спеціальне питання «Технологія державного реагування на загрози кібербезпеці».

Ми також підтримуємо пропозицію Л.А. Арсеновича щодо впровадження у службову діяльність фахівців у сфері кібербезпеки моделі проведення обов’язкової періодичної атестації (переатестації) персоналу [10].

б) Удосконалення інформаційно-аналітичного механізму забезпечення кібербезпеки, передбачає [80]:

впровадження в практику інформаційно-аналітичного забезпечення кібербезпеки автоматизованих систем збирання й структуризації інформації;

розвиток науково-методичного апарату інформаційно-аналітичного забезпечення кібербезпеки, що передбачає:

- визначення системи показників оцінки рівня загроз кібербезпеки;
- визначення системи критеріїв оцінки ефективності механізмів державного реагування на загрози кібербезпеці;
- розробку та впровадження в практику публічно-управлінську практику забезпечення кібербезпеки паспортів загроз кібербезпеці.

в) Удосконалення механізмів державного реагування на виклики та загрози кібербезпеці, передбачає [79; 80; 82]:

технологізацію вказаного реагування. Зауважимо, що структура технології державного реагування на загрози кібербезпеці має містити наступні елементи:

- теоретичну концепцію державного реагування на загрози кібербезпеці;
- об'єкт державно-управлінського впливу, головний суб'єкт забезпечення кібербезпеки, предмет державно-управлінського впливу;
- технології державного реагування на загрози кібербезпеці;
- контроль досягнутого результату;

визначення сутності й змісту реактивного та проактивного реагування на загрози кібербезпеці, а саме норм, засобів, способів та методів за допомогою яких суб'єкти забезпечення здійснюють вплив на ризики, виклики та загрози кібербезпеці.

г) Удосконалення організаційно-адміністративного механізму забезпечення кібербезпеки України передбачає:

розробку та впровадження в публічно-управлінську практику гарантування кібербезпеки України національної рамки реагування на загрози кібербезпеці;

зобов'язання профільних відомств та органів, відповідальним за кібербезпеки, здійснювати регулярний моніторинг ситуації в кібернетичному середовищі з метою своєчасного виявлення загроз кібербезпеці і вжиття адекватних заходів реагування на виявлені загрози;

завершення впровадження в публічно-управлінську практику забезпечення кібербезпеки партнерської моделі суспільно-інформаційних відносин в Україні з урахуванням позитивного досвіду держав-членів НАТО і ЄС у цій сфері.

д) Удосконалення інформаційного механізму забезпечення кібербезпеки передбачає:

визначення імперативів діяльності ЗМІ в інтересах забезпечення кібербезпеки України, а саме – об'єктивне, відповідальне інформування українського суспільства про стан справ у кібернетичній сфері;

дотримання науково обґрунтованих принципів стратегічних комунікацій у сфері супроводження політики забезпечення кібербезпеки [204; 224], а саме методологічних, організаційних та методичних, які будуть розкриті у п. 3.4 дисертаційного дослідження.

є) Удосконалення механізму партисипаторної (громадської) взаємодії в СЗКБ, що має на меті ефективну взаємодію органів державної влади, які є суб'єктами забезпечення кібербезпеки з громадськими організаціями та ІТ-компаніями в процесі реалізації політики забезпечення кібербезпеки передбачає:

визначення змісту механізму партисипаторної взаємодії між державою і громадськими організаціями, ІТ-компаніями, а саме норм, засобів, способів та методів за допомогою яких здійснюється взаємодія між суб'єктами забезпечення кібербезпеки [41; 116];

унормування політико-правового статусу рішень [202], які приймаються дорадчо-консультативними радами, громадськими радами при центральних органах виконавчої влади, що є суб'єктами забезпечення кібербезпеки.

е) Удосконалення механізму забезпечення комунікації суб'єктів забезпечення кібербезпеки передбачає створення умов для інформаційної взаємодії між згаданими суб'єктами на основі науково обґрунтованих принципів, які будуть розкриті в п. 3.4 дисертаційного дослідження [92; 93;

198; 199].

Є сенс зауважити, що на інформаційну взаємодію між суб'єктами забезпечення кібербезпеки України покладено завдання забезпечення ситуаційної обізнаності, доведення до керівництва сил сектору безпеки і оборони України, що опікуються питаннями забезпечення кібербезпеки об'єктивної інформації щодо:

стану кібербезпеки, всебічно обґрунтованих оцінок загроз кібербезпеці, прогнозів виникнення та розвитку кризових ситуацій у сфері кібербезпеки;

проектів управлінських рішень щодо реагування на загрози кібербезпеці;

взаємодії з Головним ситуаційним центром України, Урядовим ситуаційним центром та Національним координаційним центром кібербезпеки РНБО України, іншими ситуаційними центрами держави.

Зауважимо, що наведені невідкладні дії з удосконалення державних механізмів забезпечення кібербезпеки України потребують реалізації в контексті завдань реформування СЗНБ України, які визначені в офіційному дискурсі національної безпеки України [145; 153].

3.2. Структурно-функціональна модель публічного управління кібербезпекою

У процесі розробки структурно-функціональної моделі публічного управління кібербезпекою будемо дотримуватися основних принципів наукового дослідження, проектування та конструювання систем публічного управління, а саме:

принципу ієрархічності пізнання;

принципів цілісності, організованості, внутрішніх закономірностей та цілеспрямованості дій;

принципу визначеності життєвого циклу;

положення про наявність низки варіантів побудови системи;

принципу відбору кращого варіанту з низки альтернатив;

положення про врахування невизначеностей у системі публічного управління та в зовнішньому і внутрішньому середовищі [1, с. 164-148].

Вихідними ідеями для розробки структурно-функціональної моделі публічного управління кібербезпекою є ідеї:

ідея забезпечення кібербезпеки України як результату функціонування соціальних інститутів – кібернетична безпека, суспільно-інформаційні відносини, публічне управління;

ідея забезпечення кібербезпеки України як результату діяльності суб'єктів забезпечення кібербезпеки щодо запобігання та врегулювання конфліктів у сфері суспільно-інформаційних відносин;

ідея партисипаторної взаємодії тріади «держава – ІТ-бізнес – суспільство» як основи становлення неконфронтаційних суспільно-інформаційних відносин та чинника забезпечення кібербезпеки.

Також для вирішення завдань нашого дослідження будемо використовувати стратифікаційну модель реалізації функцій публічного управління кібербезпекою, яка представлена нами у вигляді семи страт [11]:

страти процесу публічно-управлінської діяльності, на якому розкриваються сутність та зміст публічного управління кібербезпекою;

страт функцій «комунікація», «прийняття публічно-управлінських рішень», «планування», «організація», «контроль», «мотивація» на яких розкриваються уявлення про обмін релевантною інформацією між учасниками суб'єктами забезпечення кібербезпеки, про СКБ, СЗКБ, соціального партнерства, суспільно-інформаційні відносини, політику забезпечення кібербезпеки, організацію публічного управління кібербезпекою.

Проте, досліджуючи проблему публічного управління кібербезпекою, варто враховувати також вплив безпекового середовища та

кіберсередовища, що представлено теоретичними моделями геополітичного інформаційного протиборства та конфліктологічною моделлю міжнародних інформаційних відносин [50; 51; 102].

Структурно-функціональна модель публічного управління кібербезпекою представлено на рис. 3.1.

Наразі Українська держава як суб'єкт забезпечення кібербезпеки:

1) є гарантом громадянських прав і свобод;

2) визначає мету розвитку системи суспільно-інформаційних відносин в українському суспільстві;

3) виробляє та реалізовує політику забезпечення кібербезпеки;

4) є організатором та координатором відносин із суб'єктами міжнародної інформаційної безпеки та кібербезпеки, ІТ-бізнесом, громадянським суспільством, розробляє правові та нормативні документи, що регламентують вказані відносини.

Виступаючи регулятором системи суспільно-інформаційних відносин, Українська держава за допомогою соціального діалогу намагається узгодити інтереси різних учасників згаданих відносин, а також бере участь у переговорах, консультаціях з метою розробки та реалізації політики у сфері забезпечення кібербезпеки.

Використовуючи результати наукових досліджень [20; 48; 50; 51; 225; 230] розглянемо питання теоретичних засад формування СКБ та СЗКБ. Відповідно для розбудови СКБ та СЗКБ України в умовах гібридної війни пропонуємо використовувати підходи, які розкриті в основному в теоріях публічного управління, державного управління, національної безпеки, гібридної війни, кібервійни, кібербезпеки та інституціоналізму. У сучасних умовах центральну методологічну роль у розбудові вказаних систем відіграє інституціональний підхід.

Місією СКБ України пропонуємо визначити гарантування безпечного функціонування кіберпростору та його використання в інтересах особи, суспільства і держави.

Місією СЗКБ пропонуємо визначити своєчасне й адекватне реагування суб’єктів забезпечення кібербезпеки на загрози кібербезпеці.

Національними цілями забезпечення кібербезпеки України пропонуємо визначити:

кіберзахист державних електронних інформаційних ресурсів, інформаційної інфраструктури, а також інформації, вимога щодо захисту якої встановлена законом;

організаційна та інституційна стійкість СЗКБ;

кібероборона України;

боротьба із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю;

міжнародне співробітництво у сфері кібербезпеки та кіберзахтисту; партисипаторна взаємодія в інтересах забезпечення кібербезпеки тріади «держава – ІТ-бізнес – громадські організації» в контексті гарантованого законом задоволення інформаційних потреб особи, суспільства і держави.

На основі аналізу результатів наукових досліджень [20; 48; 50; 51; 67; 225; 230] перспективною моделлю СЗКБ пропонуємо визначити модель креативного типу. Адже, власне СЗНБ креативного типу має не лише негативний зворотній зв'язок, що надає їй характерних рис адаптивної системи, а й позитивний зворотній зв'язок. Це дозволяє їй активно впливати на внутрішнє та зовнішнє безпекове середовище у власних інтересах, а також оперативно змінювати цілі, структуру та завдання своєї діяльності відповідно до вимог динамічного безпекового середовища Української держави, тобто забезпечувати національну стійкість.

Для визначення функціональних складових та структури СЗКБ здійснимо аналіз функцій згаданої системи, а саме:

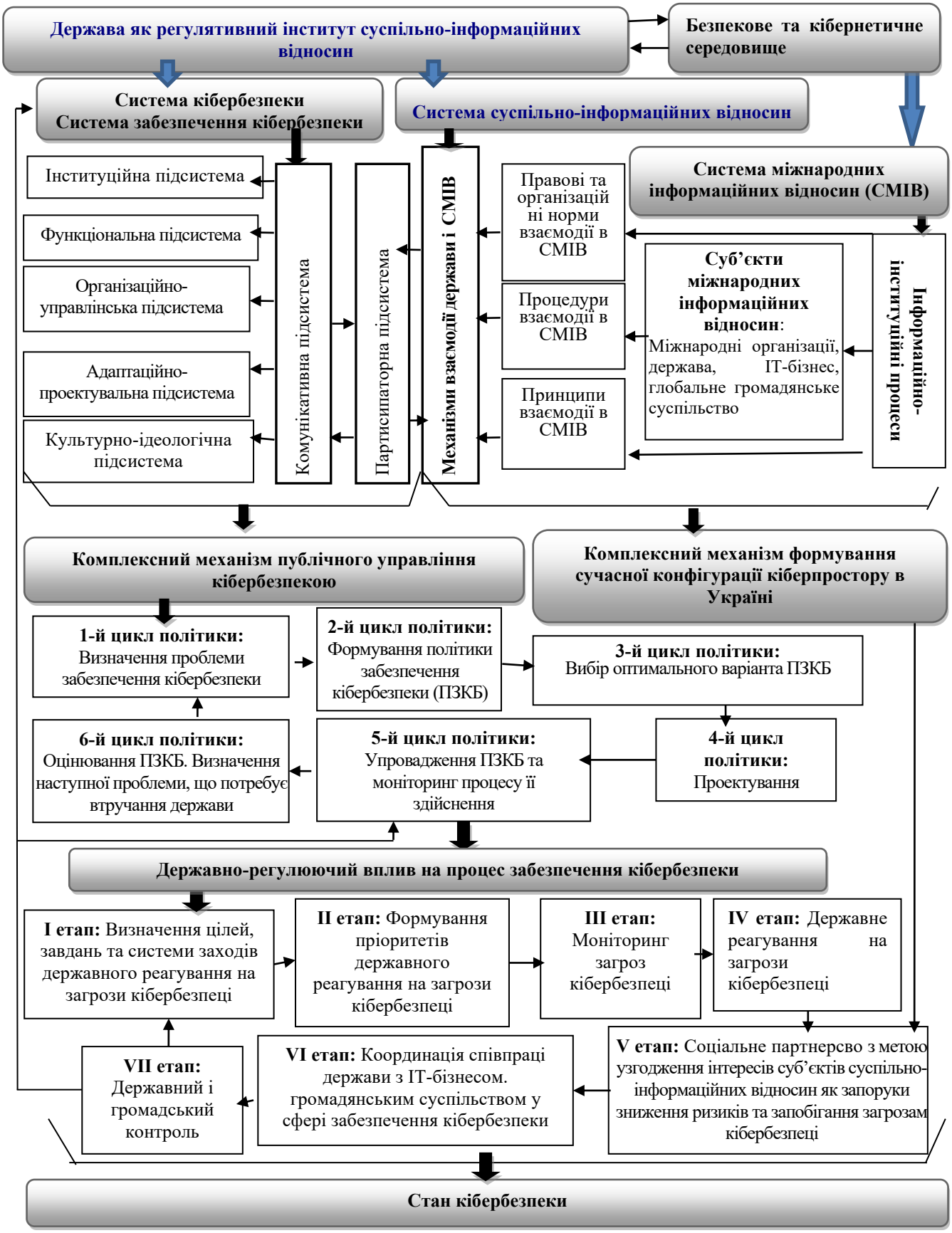

Рис. 3.1. Структурно-функціональна модель публічного управління кібербезпекою

функції цілепокладання, що реалізовує смислоутворювальний зміст публічно-управлінської практики забезпечення кібербезпеки, який включає в себе цілеформування й обумовлює потребу в цілералізації;

функції цілеформування, що передбачає визначення цілей публічного управління кібербезпекою;

функції цілереалізації, що забезпечує державне проектування та конструювання СЗКБ;

основоположної функції, що регулює заходи у сфері забезпечення кібербезпеки;

нормативно-управлінської функції, що регламентує діяльність та взаємодію суб'єктів забезпечення кібербезпеки;

організаційно-управлінської функції, що забезпечує управління кібербезпекою;

інтеграційної функції, що регулює взаємодію СЗКБ України зі структурами міжнародної та регіональної кібербезпеки;

діагностичної функції, що забезпечує виявлення та оцінку загроз кібербезпеці;

прогностичної функції, що забезпечує прогнозування тенденцій розвитку загроз кібербезпеці;

функції планування, що регулює розвиток СЗКБ в контексті зміни цільових настанов політики забезпечення кібербезпеки в умовах динамічного безпекового середовища;

програмно-адаптивної функції, що регулює питання розвитку нормативно-правової бази та організаційної структури СЗКБ в контексті появи нових викликів та загроз кібербезпеці, а також удосконалення інструментів державного реагування на виявлені загрози кібербезпеці;

науково-адаптивної функції, що регулює розвиток підсистеми науково-методичного забезпечення кібербезпеки в контексті появи нових викликів і загроз кібернетичного характеру;

координаційної функції, що забезпечує координацію діяльності

суб’єктів забезпечення кібербезпеки на основі оцінки стану кібербезпеки;

функція моніторингу, що спрямована на виявлення викликів, загроз та небезпек кібербезпеці;

соціально-адаптивної функції, що забезпечує розвиток інформаційної культури та цифрової грамотності особистості та населення;

ідеологічної функції, що спрямована на поширення ідеології соціального партнерства в контексті забезпечення кібербезпеки, а також на реалізацію заходів стратегічних комунікацій у сфері супроводження політики забезпечення кібербезпеки;

партисипаторної функції, що забезпечує інституалізацію соціального партнерства в контексті забезпечення кібербезпеки;

функції контролю, що забезпечує державний та громадський контроль виконання визначених завдань по забезпеченню кібербезпеки.

СЗКБ структурно містить такі підсистеми:

інституційна підсистема, в якій реалізовуються функції цілепокладання, цілевизначення та цілереалізації, а також нормативно-управлінська функція;

функціональна підсистема, в якій реалізовуються основоположна функція, а також аналітична функція;

організаційно-управлінська підсистема, в якій реалізовуються організаційно-управлінська, координаційна та інтеграційна функції;

адаптаційно-проектувальна підсистема, в якій реалізовуються функція планування, науково-адаптаційна, програмно-адаптаційна, функція прогнозування;

культурно-ідеологічна підсистема, в якій реалізовуються соціально-адаптивна та ідеологічна функції;

партисипаторна підсистема, в якій реалізовується партисипаторна функція;

комунікативна підсистема, в якій реалізовується функції моніторингу та контролю.

Визначимо завдання СЗКБ в ході реалізації своїх функцій.

В ході реалізації функції цілепокладання завданням СЗКБ є концептуалізація національних інтересів у кібернетичній сфері.

В ході реалізації функції цілевизначення СЗКБ виконує завдання по формуванню національних цілей забезпечення кібербезпеки в умовах змін у зовнішньому та внутрішньому безпековому середовищі держави, а також кібернетичному середовищі.

В ході реалізації функції цілереалізації СЗКБ виконує завдання по:

захисту недоторканості національних цілей забезпечення кібербезпеки на протязі дії Стратегії забезпечення кібербезпеки;

визначенню форм взаємодії між державою, ІТ-бізнесом та громадськими організаціями в контексті забезпечення кібербезпеки;

державному проектуванню та конструюванню СКБ та СЗКБ

В ході реалізації організаційно-управлінської функції СЗКБ виконує завдання по:

організації функціонування СЗКБ в цілому; прийняття публічно-управлінських рішень; відповідальність за прийняті рішення;

організації реалізації концепцій, доктрин, стратегій і програм у сфері забезпечення кібербезпеки;

організації функціонування механізму реактивного реагування на загрози кебірбезпеці;

організації функціонування механізму проактивного реагування на загрози кібербезпеки.

В ході реалізації прогностичної функції СЗКБ виконує завдання по:

стратегічному прогнозуванню у сфері політики забезпечення кібербезпеки;

стратегічному прогнозуванню напрямків розвитку конфліктів у сфері суспільно-інформаційних відносин та тенденцій розвитку загроз кібербезпеці;

прогнозуванню можливих наслідків впровадження міжнародного та

зарубіжного досвіду щодо забезпечення кібербезпеки у вітчизняну публічно-управлінську практику.

В ході реалізації фундаментальної (основоположної) функції СЗКБ виконує завдання по:

вжиттю конкретних заходів реактивного й проактивного реагування на загрози національній кібербезпеці;

вжиттю заходів щодо відстоювання національних інтересів України у кібернетичній сфері на міжнародній арені;

вжиттю комплексу заходів щодо запобігання та врегулювання конфліктів та криз у сфері суспільно-інформаційних відносинах;

вжиттю конкретних заходів з кібероборони та кіберстійкості;

вжиттю конкретних заходів щодо протидії кіберзлочинності та кібертероризму.

В ході реалізації нормативно-управлінської функції СЗКБ виконує завдання:

регламентація згідно норм чинного законодавства діяльності суб’єктів забезпечення кібербезпеки;

нормативне управління розвитком СКБ та СЗКБ в контексті вимог динамічного безпекового кіберсередовища щодо своєчасного та адекватного реагування на загрози кібербезпеці;

нормативне управління впровадженням стандартів НАТО кризового реагування у вітчизняну практику реагування на загрози кібербезпеці.

В ході реалізації програмно-адаптивної функції СЗКБ виконує завдання:

розроблення або уточнення концептуально-доктринальних документів, документів національного програмування розвитку СЗКБ;

розробка технологій реактивного та проактивного реагування на загрози кібербезпеки;

удосконалення організаційної структури СЗКБ в контексті вимог динамічного безпекового кіберсередовища.

В ході реалізації функції планування СЗКБ виконує завдання:

стратегічне планування у сфері забезпечення кібербезпеки;

планування конкретних заходів щодо реактивного та проактивного реагування на загрози кібербезпеці.

В ході реалізації науково-адаптивної функції СЗКБ виконує завдання:

розвиток галузі знань «Публічне управління та адміністрування» з метою науково-методичного забезпечення кібербезпеки в умовах глобальних викликів, динамічного безпекового та кібернетичного середовища;

формування експертно-консультативного середовища з питань кібербезпеки.

В ході реалізації інтеграційної функції СЗКБ виконує завдання:

розвиток співробітництва між СЗКБ України із системами забезпечення регіональної та міжнародної кібербезпеки;

інтеграція кіберпростору України у світовий інформаційний простір.

В ході реалізації координаційної функції СЗКБ виконує завдання по координації діяльності суб’єктів забезпечення кібербезпеки на основі оцінки рівня кібербезпеки та ефективності політики забезпечення кібербезпеки.

В ході реалізації діагностичної функції СЗКБ виконує завдання:

ідентифікація та оцінка рівня загроз кібербезпеці;

оцінка рівня кібербезпеки, досягнутого СЗКБ на поточний момент;

оцінка результативності дій реактивного та проактивного реагування на загрози кібербезпеці;

оцінка ефективності політики забезпечення кібербезпеки.

В ході реалізації функції моніторингу СЗКБ виконує завдання:

стратегічний моніторинг процесів, що відбуваються в національному та міжнародному кіберпросторі;

спостереження за проявами кіберзлочинності та кібертероризму;

виявлення зовнішніх та внутрішніх викликів, загроз та небезпек кібербезпеці;

виявлення внутрішніх ризиків ефективності функціонування СЗКБ.

В ході реалізації соціально-адаптивної функції СЗКБ виконує завдання:

формування мотивації особистості та населення країни до своєчасного й адекватного реагування на загрози кібербезпеці;

формування ситуаційної обізнаності особистості та населення країни з питань кібербезпеки з рахуванням трансформацій безпекового кіберпростору;

формування інформаційної культури, культури кібербезпеки, управлінської культури у сфері забезпечення кібербезпеки, цифрової грамотності населення країни.

В ході реалізації ідеологічної функції СЗКБ виконує завдання:

поширення ідеології соціального партнерства між державою, ІТ-бізнесом та громадянським суспільством в інтересах забезпечення кібербезпеки;

стратегічні комунікації у сфері супроводження політики забезпечення кібербезпеки.

В ході реалізації партисипаторної функції СЗКБ виконує завдання:

інституалізація соціального партнерства між державою, ІТ-бізнесом та громадянським суспільством в інтересах забезпечення кібербезпеки;

представництво інтересів громадян в органах державної влади;

узгодження інтересів соціальних груп і держави в процесі розробки політики забезпечення кібербезпеки.

В ході реалізації функції контролю СЗКБ виконує завдання:

здійснення державою контролю за виконанням нормативно визначених в офіційному дискурсі завдань по забезпеченню кібербезпеки;

здійснення контролю громадянським суспільством результатів реалізації політики забезпечення кібербезпеки.

Структурно-функціональна модель публічного управління кібербезпекою функціонує наступним чином. Держава формує інституціональне середовище публічного управління кібербезпекою, що визначає модель СЗКБ та модель системи суспільно-інформаційних відносин. На модель системи суспільно-інформаційних відносин також впливає на інституціональне середовище міжнародних інформаційних відносин. У свою чергу, інституціональне середовище публічного управління кібербезпекою опредмечуються в законодавчій базі згідно вимог якої здійснюється державне проектування та конструювання СЗКБ та розбудова система суспільно-інформаційних відносин. Модель системи суспільно-інформаційних відносин безпосередньо впливає на формування механізму взаємодії держави і ІТ-бізнесу та громадянського суспільства, який є чинником забезпечення кібербезпеки.

СЗКБ представлено як інтегровану систему, до складу якої входять:

інституційна, організаційно-управлінська, адаптивно-проектувальна, функціональна, комунікативна, культурно-ідеологічна та партисипаторна підсистеми;

цикли політики забезпечення кібербезпеки;

етапи справляння державно-регулюючого впливу на процес забезпечення кібербезпеки.

Вказані підсистеми СЗКБ функціонують як самостійні складові СЗКБ, що керовані відповідними інституціями держави. При цьому на основі взаємодії СЗКБ та системи суспільно-інформаційних відносин утворюється комплексний механізм публічного управління кібербезпекою. Водночас, на основі взаємодії системи суспільно-інформаційних відносин та системи міжнародних інформаційних відносин утворюється комплексний механізм формування сучасної моделі кіберпростору в Україні.

У рамках цієї моделі визначено цикли формування та реалізації політики забезпечення кібербезпеки:

1) визначення проблеми забезпечення кібербезпеки;

2) формування політики забезпечення кібербезпеки;

3) вибір оптимального варіанту політики забезпечення кібербезпеки;

4) проектування політики забезпечення кібербезпеки;

5) упровадження політики забезпечення кібербезпеки та моніторинг процесу її здійснення;

6) визначення наступної проблеми забезпечення кібербезпеки, що потребує втручання держави.

Моніторинг результативності політики забезпечення кібербезпеки є самостійною експертно-аналітичною процедурою, що базується на показниках (індикаторах) визначення стану кібербезпеки (високий, задовільний, низький). Для визначення відповідних індикаторів кібербезпеки пропонуємо встановити такі критерії:

рівень захисту об’єкта кібербезпеки;

напрям дій викликів і загроз (зовнішні та внутрішні) кібербезпеці;

період дії загроз кібербезпеці (коротко-, середньо- та довготривалі, постійні);

масштаб можливих наслідків реалізації загроз кібербезпеці (загальнодержавний, регіональний, локальний).

Державно-регулюючий вплив на процес забезпечення кібербезпеки здійснюється в такий спосіб:

1-й етап: визначення цілей, завдань та системи заходів державного реагування на загрози кібербезпеці;

2-й етап: формування пріоритетів державного реагування на загрози кібербезпеці;

3-й етап: моніторинг загроз кібербезпеці;

4-й етап: соціальне партнерство з метою узгодження інтересів суб’єктів суспільно-інформаційних відносин як запоруки зниження ризиків та запобігання загрозам кібербезпеці;

5-й етап: координація співпраці держави з ІТ-бізнесом та громадянським суспільством у сфері забезпечення кібербезпеки;

6-й етап: державний та громадський контроль.

На наше переконання, упровадження в публічно-управлінську практику структурно-функціональної моделі публічного управління кібербезпекою, яка ґрунтується на принципах партисипаторної взаємодії, сприятиме підвищенню ефективності СЗКБ України в умовах динамічного безпекового та кібернетичного середовища.

3.3. Пропозиції щодо розробки та впровадження в публічно-управлінську практику гарантування національної безпеки України перспективної моделі системи забезпечення кібербезпеки

Для розв’язання проблем, пов’язаних із вдосконаленням СЗКБ України в умовах динамічного безпекового середовища, необхідним є впровадження в публічно-управлінську практику гарантування національної безпеки України перспективної моделі СЗКБ, яка містить такі складові, як-от:

функціональна модель;

інформаційна модель;

інституційна модель (див. рис. 3.2.).

Вимоги до перспективної функціональної моделі СЗКБ України визначаються стратегічними цілями формування нової якості СКБ, які визначені в офіційному дискурсі національної безпеки України [149], а саме:

для формування потенціалу стримування СКБ необхідними є досягнення стратегічних цілей – дієва кібероборона, ефективна протидія кіберзлочинності та кібертероризму, розвідувально-підривній діяльності у кібернетичному просторі, розвиток асиметричних інструментів стримування;

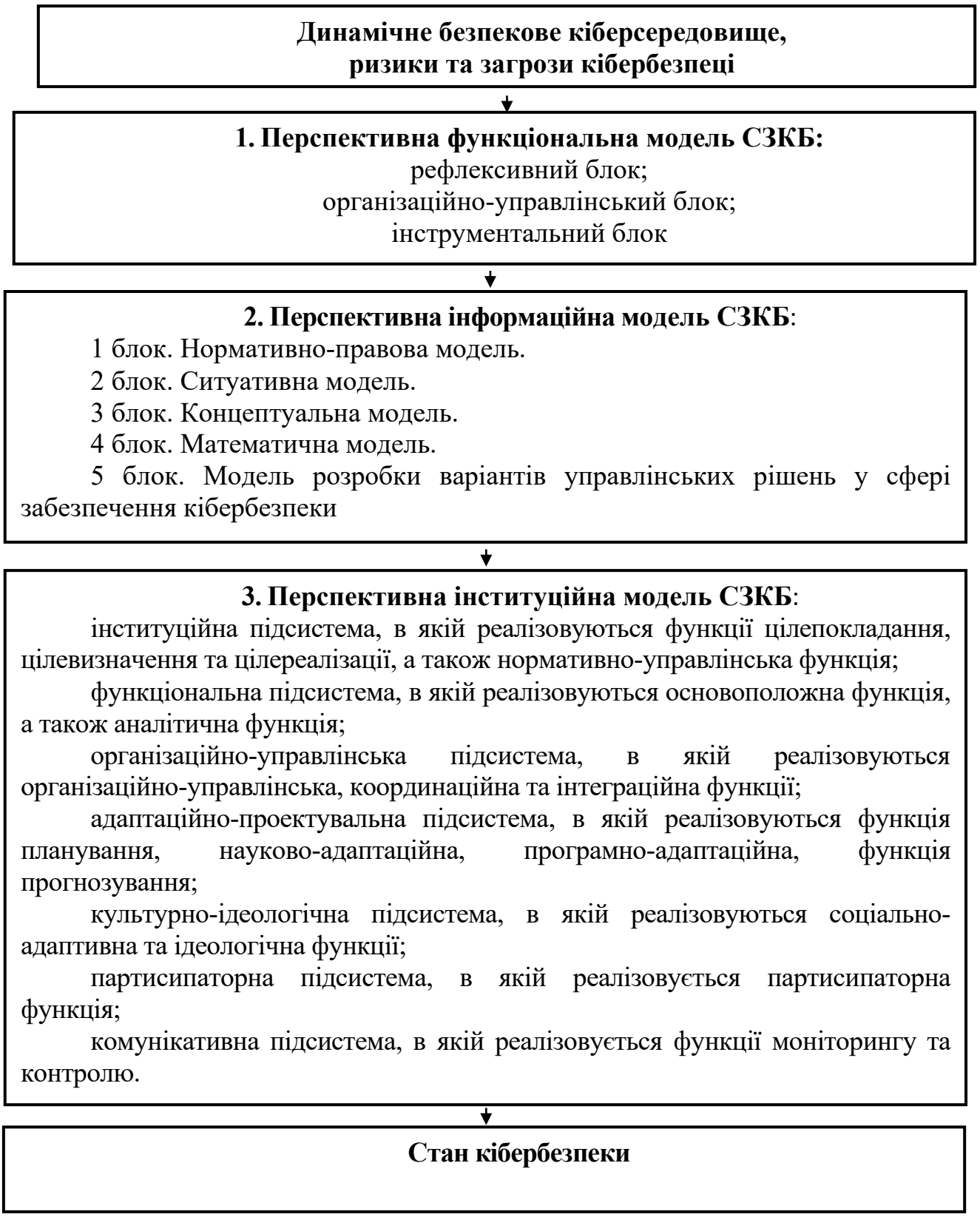

Рис. 3.2. Структура перспективної моделі СЗКБ

Джерело: [розробка автора].

для набуття кіберстійкості СКБ необхідним є досягнення стратегічних цілей: національна кіберготовність та надійний кіберзахист,

науково-технічне забезпечення кібербезпеки, високий рівень обізнаності суспільства з питань кібербезпеки, високий рівень професіоналізму фахівців у сфері кібербезпеки, безпечні цифрові послуги;

для вдосконалення взаємодії суб'єктів забезпечення кібербезпеки необхідним є досягнення стратегічних цілей: зміцнення системи координації, формування нової моделі суспільно-інформаційної відносин у сфері кібербезпеки, прагматичне міжнародне співробітництво.

Також вимоги до перспективної функціональної моделі СЗКБ України визначаються низкою чинників, а саме:

нагальною необхідністю забезпечення організаційної стійкості, тобто здатності суб'єктів забезпечення кібербезпеки ідентифікувати загрози та своєчасно й адекватно реагувати на них, а також адаптуватися до трансформацій безпекового кіберсередовища й підтримувати стале функціонування СЗКБ в умовах криз різного характеру [159];

нагальною необхідністю розвитку СЗКБ задля гарантування кіберстійкості національних інформаційних ресурсів [159];

нагальною необхідністю обґрунтування та державного конструювання механізмів організації і координації дій суб'єктів забезпечення кібербезпеки у сфері кризового менеджменту [159];

нагальною необхідністю впровадження в публічно-управлінську практику ризик-орієнтованого підходу до забезпечення кібербезпеки та проактивного підходу до нейтралізації кіберзагроз [154];

нагальною необхідністю посилення спроможностей СКБ та СЗКБ щодо протидії сучасним кіберзагрозам [154];

нагальною необхідністю впровадження у вітчизняну практику державного реагування на загрози національній безпеці стандартів НАТО щодо кризового реагування й неопрацьованістю підходів щодо їх впровадження;

динамізмом безпекового кіберсередовища, що обумовлено трансграничним характером загроз кібербезпеці України в умовах сучасної

російсько-української війни, що вимагає комплексне поєднання заходів реактивного і проактивного реагування на вказані загрози;

нагальною необхідністю удосконалення моделі державно-приватного партнерства у сфері забезпечення кібербезпеки на основі урахування змін у сфері публічного управління національною безпекою [154].

Перспективна функціональна модель СЗКБ України передбачає функціонування цієї системи у таких режимах, як-от:

проактивне реагування на потенційні загрози кібербезпеці;

реактивне реагування на реальні загрози кібербезпеці.

Перспективну функціональну модель СЗКБ України нами представлено трьома блоками:

Рефлексивний блок, який структурно містить:

соціально-психологічний механізм усвідомлення проблем забезпечення кібербезпеки, що передбачає створення умов для усвідомлення актуальних проблем забезпечення кібербезпеки;

державно-політичний механізм, що уособлює собою сукупність процесів обґрунтування засад політико-правового проектування та державного конструювання СЗКБ, а також функціонування вказаної системи;

механізм науково-методичного забезпечення реагування на загрози кібербезпеці та інформаційно-аналітичний механізм забезпечення кібербезпеки, які призначені для розробки та практичного використання діагностичної й прогностичної моделей загроз кібербезпеці.

Організаційно-управлінський блок містить такі механізми, як-от: правовий, інституційний, організаційно-адміністративний механізми, механізми розробки та реалізації державної політики у сфері кібербезпеки, механізми кадрового, адміністративного, інформаційно-технічного, фінансового та ресурсного забезпечення кібербезпеки.

Інструментальний блок, який структурно містить:

механізми реактивного та проактивного реагування на загрози

кібербезпеці;

механізми партисипаторної взаємодії, міжнародного й міждержавного співробітництва у сфері забезпечення кібербезпеки;

механізм інтеграції національного кіберпростору у світовий інформаційний простір.

Інформаційна модель СЗКБ України у загальних рисах може бути представлена схемою руху управлінської інформації щодо стану кібербезпеки: аналіз (опис) середовища кібербезпеки → діагностування і прогнозування стану кібербезпеки → цілепокладання / цілевизначення / цілереалізація у сфері забезпечення кібербезпеки → планування у сфері забезпечення кібербезпеки → програмування у сфері забезпечення кібербезпеки → рішення щодо забезпечення кібербезпеки → контроль за виконанням прийнятого рішення → зворотній зв'язок.

Вимоги до перспективної інформаційної моделі СЗКБ України визначаються:

необхідністю вдосконалення нормативно-правової бази у сфері забезпечення кібербезпеки, а також необхідністю прискорення імплементації положень європейського законодавства у згаданій сфері [154];

нагальною необхідністю розбудови дієвої системи інформаційно-аналітичного забезпечення кібербезпеки [154];

необхідністю формування бази відповідних релевантних знань в галузях публічного управління, національної безпеки і оборони, кібервійни та геополітичного інформаційного протиборства, кібербезпеки, що дозволило б вищому керівництву держави в умовах російсько-української війни оперативно приймати обґрунтовані рішення у сфері реагування на загрози кібернетичного характеру;

суперечностями, що існують сьогодні в системі інформаційно-аналітичної діяльності в СЗКБ, а саме: між новітніми загрозами

кібербезпеці в умовах динамічного безпекового кіберсередовища і відсутністю відповідного аналітичного інструментарію опрацювання практичних проблем реагування України на кіберзагрози як необхідної умови ефективного функціонування СКБ;

нагальною необхідністю підвищення рівня обізнаності фахівців-управлінців сектору безпеки і оборони, службовців органів державної влади та місцевого самоврядування, представників інститутів громадянського суспільства з вимогами інформаційної безпеки [159];

необхідністю впровадження стандартів НАТО щодо кризового менеджменту, а саме протоколів реагування у вітчизняну практику забезпечення кібербезпеки та не розробленістю паспортів загроз кібербезпеці, технологій реагування на них.

Перспективна інформаційна модель СЗКБ України передбачає:

1) комплексне застосування технологій первинної, вищої, масової, військової та безпекової, стратегічної та ситуаційної аналітики в контексті завдань реактивного та проактивного реагування на кіберзагрози [282];

2) розробку та впровадження в практику публічного управління кібербезпекою паспортів загроз кібербезпеці та технологій реагування на них [80].

Зауважимо, що первинна аналітика, яка передбачає моніторинг та ситуаційний аналіз, виконує функцію моніторингу сфері забезпечення кібербезпеки.

Вища аналітика, яка передбачає діагностичний аналіз кіберзагроз та прогноз їх розвитку, а також вироблення варіантів управлінських рішень щодо реагування на них, виконує діагностичну, прогностичну та інструментальну функції.

Перспективну інформаційну модель СЗКБ України представлено такими блоками, як-от:

1 блок. Нормативно-правова модель: чинне законодавство, що регулює діяльність суб’єктів забезпечення кібербезпеки. На основі цього

законодавства також формується та функціонує СКБ.

2 блок. Ситуативна модель:

блок даних – достовірна й релевантна інформація про кіберзагрози;

блок ситуацій – опис можливих загроз кібербезпеці.

3 блок. Концептуальна модель**:**

блок цілі – формулювання цілей реактивного та проактивного реагування на кіберзагрози;

блок вибору – вибір критерію оптимальності дій реактивного та проактивного реагування на кіберзагрози.

4 блок. Математична модель: система математичних співвідношень, які описують процес забезпечення кібербезпеки.

5 блок. Модель розробки варіантів управлінських рішень щодо гарантування кібербезпеки, у рамках яких визначаються напрями політики забезпечення кібербезпеки, пріоритети розвитку СКБ та СЗКБ в контексті появи нових викликів і загроз кібербезпеці.

Розглянемо перспективну інституційну модель СЗКБ України.

Вимоги до перспективної інституційної моделі СЗКБ України визначаються:

потребою в посиленні спроможностей СЗКБ [154];

потребою в забезпеченні інституційної стійкості, що передбачає чітке визначення місії, функцій та завдань СЗКБ;

потребою в обґрунтуванні механізмів забезпечення кібербезпеки в умовах динамічного безпекового кіберсередовища і відсутністю ефективних напрямів реалізації цього процесу на практиці;

необхідністю завершення заходів з упровадження організаційно-технічної моделі кіберзахисту, яка відповідатиме сучасним викликам і загрозам кібернетичного характеру [154];

нагальною необхідністю розбудови дієвої системи інформаційно-аналітичного забезпечення кібербезпеки [154];

нагальною необхідністю підвищення кваліфікації фахівців з питань

кібербезпеки та кіберзахисту [154];

необхідністю розвитку комунікації та координації діяльності між суб'єктами забезпечення національної кібербезпеки [154];

необхідністю розвитку комунікації, координації та партнерства між суб'єктами забезпечення кібербезпеки міжнародному рівні [154];

необхідністю впровадження сучасних принципів та механізмів публічного управління у сфері кібербезпеки [154].

Перспективна інституційна модель СЗКБ України структурно має містити такі підсистеми, як-от:

1) інституційна підсистема, в якій реалізовуються функції цілепокладання, цілевизначення та цілереалізації, а також нормативно-управлінська функція. Вказана підсистема СЗКБ структурно містить такі механізми забезпечення кібербезпеки, як-от:

механізм соціально-психологічного усвідомлення проблематики забезпечення кібербезпеки;

державно-політичний механізм забезпечення кібербезпеки;

правовий механізм забезпечення кібербезпеки;

інституційний механізм забезпечення кібербезпеки;

механізм партисипаторної взаємодії між державою, громадянським суспільством та ІТ-бізнесом;

механізм розробки політики забезпечення кібербезпеки;

б) функціональна підсистема, в якій реалізовуються основоположна функція, а також аналітична функція. Вказана підсистема СЗКБ структурно містить такі механізми забезпечення кібербезпеки, як-от:

комплексний механізм реалізації політики забезпечення кібербезпеки, й зокрема інформаційно-аналітичний механізм та механізми державного реагування на загрози кібербезпеці;

в) організаційно-управлінська підсистема, в якій реалізовуються організаційно-управлінська, координаційна та інтеграційна функції. Вказана підсистема СЗКБ структурно містить:

організаційно-адміністративний механізм забезпечення кібербезпеки;

механізм міжнародного й міждержавного співробітництва з питань забезпечення кібербезпеки;

механізм інтеграції кіберпростору України у світовий інформаційний простір;

механізм інформаційно-технологічного забезпечення реагування на кіберзагрози;

механізм забезпечення управлінської взаємодії суб'єктів забезпечення кібербезпеки;

г) адаптаційно-проектувальна підсистема, в якій реалізовуються функція планування, науково-адаптаційна, програмно-адаптаційна, функція прогнозування. Вказана підсистема СЗКБ структурно містить:

механізм науково-методичного забезпечення кібербезпеки;

механізм розробки політики забезпечення кібербезпеки;

інформаційно-аналітичний механізм забезпечення кібербезпеки;

д) культурно-ідеологічна підсистема, в якій реалізовуються соціально-адаптивна та ідеологічна функції. Ця підсистема СЗКБ структурно містить:

інформаційний механізм забезпечення кібербезпеки;

є) партисипаторна підсистема, в якій реалізовується партисипаторна функція. Ця підсистема СЗКБ структурно містить:

механізм партисипаторної взаємодії між державою, громадянським суспільством та ІТ-бізнесом;

е) комунікативна підсистема, в якій реалізовується функції моніторингу та контролю. Ця підсистема СЗКБ структурно містить механізм забезпечення комунікації суб'єктів забезпечення кібербезпеки.

На наше переконання, очікуваними результатами впровадження перспективних функціональної, інформаційної та інституційної моделей СЗКБ України стане:

набуття інституційних спроможностей суб'єктами забезпечення кібербезпеки на стратегічному, оперативному та тактичному рівнях. Це, в

свою чергу, забезпечить функціональну стійкість СЗКБ, що передбачає своєчасне й адекватне реагування на кіберзагрози;

імплементована організаційна структура СЗКБ України забезпечить інституційну стійкість вітчизняної СЗКБ й відповідатиме стандартам НАТО у сфері кризового менеджменту;

належний рівень технічного оснащення сил сектору безпеки й оборони, що значно підвищить рівень ефективності реалізації функцій СЗКБ України та забезпечить інтеграцію з іншими системами державного реагування на загрози національній безпеці;

належний рівень інформаційно-аналітичного забезпечення реагування на загрози кібербезпеці, що забезпечуватиме функціональну стійкість СЗКБ України.

3.4. Пропозиції щодо удосконалення державних механізмів забезпечення кібербезпеки на сучасному етапі державного будівництва

Обґрунтування пропозицій щодо удосконалення державних механізмів забезпечення кібербезпеки України зумовлена наявністю проблем державного реагування у сфері кібербезпеки України, що спричинені низкою протиріч:

між динамікою зростання рівня загроз кібербезпеці України та потребою удосконалення національної СЗКБ з урахуванням каскадного та синергетичного ефектів реалізації згаданих загроз;

між необхідністю своєчасного виявлення загроз кібербезпеці та знаннями реальних шляхів проактивного та реактивного реагування на них;

між існуючою системою умов і чинників гарантування кібербезпеки та необхідними умовами і чинниками, що забезпечують організаційну та інституційну стійкість СЗКБ.

Аналіз результатів наукових досліджень з питань гарантування

кібербезпеки України [20; 48; 51; 93] дозволяє констатувати відсутність єдиного підходу до обґрунтування організаційної та інституційної стійкості СЗКБ, до розуміння сутності проактивного та реактивного реагування на загрози кібербезпеці. Водночас, недостатня наукова обґрунтованість механізмів забезпечення кібербезпеки України обумовлюють необхідність синтезу нових наукових знань щодо розбудови та функціонування згаданих механізмів.

Є сенс зауважити, що результати аналізу нормативно-правової бази України в галузі кібербезпеки [149; 154] дозволяють зробити висновок про наявність в офіційному дискурсі номенклатури загроз кібербезпеці України, правових засад державного реагування на виявлені загрози. Проте, в сучасних умовах російсько-української війни державне реагування на загрози кібербезпеки України не набуло ознак системності, що в свою чергу, досить негативно впливає на ефективність функціонування СЗКБ України.

Саме тому метою підрозділу є обґрунтування пропозицій щодо удосконалення державних механізмів забезпечення кібербезпеки України в сучасних умовах, а саме державно-політичного механізму забезпечення кібербезпеки, правового механізму забезпечення кібербезпеки, механізму розробки політики забезпечення кібербезпеки, організаційно-адміністративного механізму забезпечення кібербезпеки України, інформаційно-аналітичного механізму забезпечення кібербезпеки, механізмів державного реагування на загрози кібербезпеці, механізму міжнародного й міждержавного співробітництва з питань забезпечення кібербезпеки.

З метою удосконалення державно-політичного механізму забезпечення кібербезпеки пропонуємо чітко розмежувати публічне управління кібербезпекою на три складових:

а) публічно-політична складова, яка включає в себе:

актуалізацію інтересу або проблеми гарантування кібербезпеки;

усвідомлення проблеми гарантування кібербезпеки суб’єктом громадянського суспільства;

формування публічної політики забезпечення кібербезпеки;

легітимізація публічної політики забезпечення кібербезпеки;

формування державної політики забезпечення кібербезпеки (програми / проекту) на основі публічної політики забезпечення кібербезпеки;

моніторинг і контроль за реалізацією державної політики забезпечення кібербезпеки;

публічний аудит публічного управління кібербезпекою суб’єктами публічної сфери та громадянського суспільства;

б) адміністративна складова, що включає в себе:

організаційно-управлінське, фінансове і ресурсне забезпечення реалізації рішень щодо реагування на загрози кібербезпеці;

в) оперативна складова, що передбачає:

створення ієрархії управління силами та засобами сектору безпеки та оборони України з питань реагування на загрози кібербезпеці.

Для удосконалення правового механізму забезпечення кібербезпеки необхідним є внесення змін до Стратегії кібербезпеки України [154] в частині:

визначення загроз кібербезпеці з урахуванням реальних та потенційних загроз кібербезпеці України в умовах зовнішньої агресії росії;

визначення ризиків у сфері кібербезпеки України. Зокрема, до Стратегії кібербезпеки України пропонуємо внести перелік внутрішніх ризиків у сфері кібербезпеки, під якими будемо розуміти ризики, імовірність виникнення яких безпосередньо пов’язана із виконанням СЗКБ України покладених на неї функцій і завдань.

Номенклатура внутрішніх ризиків у сфері кібербезпеки України може містити такі ризики:

ризик неадекватної оцінки стану кібербезпеки, і як наслідок помилкове визначення цілей реагування на виявлені загрози кібербезпеці – ухвалення стратегічно помилкових рішень у сфері кібербезпеці на підставі неякісного аналізу реальних і потенційних загроз кібербезпеці різного характеру;

ризик розробки неадекватної реальним умовам і можливостям моделі реагування на загрози кібербезпеці – недостатній рівень взаємодії між суб'єктами забезпечення кібербезпеки України та відсутність належної координації їх дій з іноземними партнерами з питань гарантування кібербезпеки.

Цей перелік внутрішніх ризиків у сфері кібербезпеки України є неостаточним й може бути доповнений в контексті трансформацій безпекового кіберсередовища.

З метою удосконалення механізму розробки політики забезпечення кібербезпеки пропонуємо використати ідею визначення імперативів політики національної безпеки в умовах трансформації безпекового середовища [59]. Використовуючи результати наукових розробок [59; 198] представимо функціональну модель визначення імперативів політики забезпечення кібербезпеки України. Вказана модель містить сім стадій визначення імперативів згаданої політики:

І стадія: характеристика сучасних тенденцій кібервійни та розвитку загроз кібербезпеці, оцінка майбутнього стану безпекового кіберсередовища в контекстній залежності появи нових загроз кібербезпеці України та ризиків у цій сфері.

ІІ стадія: діагностика стану кібербезпеки України – об'єктивна характеристика причино-наслідкових зв'язків виникнення ризиків та загроз кібербезпеці, закономірностей забезпечення кібербезпеки, опис майбутнього безпекового кіберсередовища, визначення спроможностей СЗКБ щодо державного реагування на загрози кібербезпеці.

ІІІ стадія: визначення цілей політики забезпечення кібербезпеки.

IV стадія: визначення пріоритетів політики забезпечення кібербезпеки.

V стадія: визначення стратегічних, тактичних та оперативних завдань державного реагування на загрози кібербезпеці.

VI стадія: визначення принципів реалізації політики забезпечення кібербезпеки.

VII стадія: визначення засобів та інструментів забезпечення кібербезпеки.

Організаційно-адміністративний механізм забезпечення кібербезпеки України являє собою сукупність правил і процедур щодо забезпечення організаційної стійкості СЗКБ, під якою пропонуємо розуміти здатність суб'єктів забезпечення кібербезпеки ідентифікувати, своєчасно й адекватно реагувати на загрози, адаптуватися до вимог динамічного безпекового кіберсередовища, підтримувати стале функціонування СЗКБ в умовах кризових ситуацій, що загрожують кібербезпеці задля збереження її стійкового функціонування й інституційного розвитку. Частково це питання розглянуто в [220].

На нашу думку, розробка та офіційне затвердження національної рамки реагування на загрози кібербезпеці дозволить удосконалити організаційно-адміністративний механізм забезпечення кібербезпеки України.

Під поняттям «національна рамка реагування на загрози кібербезпеці» – це документ, що регламентує застосування суб'єктами забезпечення кібербезпеки відповідних видів державного реагування на загрози кібербезпеці в контекстній залежності від рівня загрози (потенційна або реальна загроза).

Цей документ має містити:

1) місію СЗКБ;

2) загальний алгоритм державного реагування на загрози кібербезпеці;

3) системний і структурований опис процесів організації державного

реагування на загрози кібербезпеці та власне процесів реактивного та проактивного реагування на згадані загрози;

4) розподіл відповідальності суб'єктів забезпечення кібербезпеки на загальнодержавному, відомчому та внутрішньовідомчому рівнях за організацію та результати державного реагування на загрози кібербезпеки.

Місією СЗКБ нами визначено своєчасне й адекватне реагування суб'єктів забезпечення кібербезпеки на загрози кібербезпеці.

Вказана місія СЗКБ реалізовується за допомогою фундаментальної функції вказаної системи – державне реагування на загрози кібербезпеці.

Під поняттям «державне реагування на загрози кібербезпеці» пропонуємо розуміти інтегровану форму дій за єдиним замислом та планом суб'єктів забезпечення кібербезпеки у взаємодії з іншими суб'єктами забезпечення національної безпеки України відповідно до їх повноважень визначених в рамках чинного законодавства, що репрезентує свій кінцевий результат у вигляді:

1) профілактики та запобігання загрозам кібербезпеці;

2) мінімізації, локалізації і ліквідації негативних наслідків реалізації загроз кібербезпеці.

Загальний алгоритм державного реагування на загрози кібербезпеці містить такі операційні ланцюги:

1) формулювання проблеми державного реагування на загрози кібербезпеці;

2) діагностика стану кібербезпеки – визначення параметрів загрози кібербезпеці, що включає в себе визначення джерел (факторів) виникнення загроз, визначення виду загрози та стадію її реалізації – потенційна або реальна загроза.

Етапами діагностики є:

1 етап – антикризовий моніторинг – раннє виявлення ознак загроз кібербезпеці, постійний збір інформації за допомогою «слабких сигналів», нагромадження даних для експрес-діагностики (моніторинг викликів,

небезпек і загроз);

2 етап – експрес-діагностика – ідентифікація та оцінка рівня загроз кібербезпеці;

3 етап – фундаментальна діагностика – визначення й оцінка факторів, які впливають на реалізацію загроз кібербезпеці, встановлення їх взаємозв'язку і взаємозалежності;

3) прогнозування тенденцій розвитку загроз кібербезпеці та наслідків її реалізації для національної безпеки і оборони;

4) розробка стратегічного задуму державного реагування на загрози кібербезпеці;

5) визначення цілей, засобів та результатів державного реагування на загрози кібербезпеці;

6) розробка варіантів державно-управлінських рішень щодо реагування на ідентифіковані загрози кібербезпеці та оцінка наслідків прийняття відповідних рішень для гарантування кібербезпеки;

7) прийняття державно-управлінського рішення щодо реагування на загрози кібербезпеці;

8) планування заходів по реалізації державно-управлінського рішення щодо реагування на загрози кібербезпеці;

9) організація та здійснення заходів проактивного та реактивного реагування на загрози кібербезпеці;

10) оцінка стану кібербезпеки після державно-управлінського впливу на загрози кібербезпеці;

11) підсумкова оцінка досягнення запланованого результату державного реагування на загрози кібербезпеці;

12) здійснення корегування цілей та засобів державного реагування на загрози кібербезпеці в контексті залежності від результатів попередньо реалізованого реагування.

Видами державного реагування на загрози кібербезпеці в контекстній залежності від рівня загрози пропонуємо визначити:

1) для реагування на реальні загрози кібербезпеці – реактивне реагування на вказані загрози. Під останнім пропонуємо розуміти сукупність процесів, які ініційовані і реалізуються суб'єктами забезпечення кібербезпеки комплексна дія яких стосовно реальних загроз кібербезпеці репрезентувала свій кінцевий результат у вигляді мінімізації, локалізації і ліквідації негативних наслідків реалізації вказаних загроз.

Підвидами реактивного реагування на загрози кібербезпеці є:

припинення реалізації загрози кібербезпеці – це безпосередній вплив силами і засобами СЗКБ на процес реалізації загрози кібербезпеці;

локалізація загрози кібербезпеці – це процес локалізації силами і засобами СЗКБ негативних наслідків реалізації загрози кібербезпеці;

нейтралізація загрози кібербезпеці – це процес зведення силами і засобами СЗКБ негативних наслідків реалізації загрози кібербезпеці до їх мінімального рівня.

2) для реагування на потенційні загрози кібербезпеці – проактивне реагування на вказані загрози. Під останнім пропонуємо розуміти сукупність процесів, які ініційовані і реалізуються суб'єктами забезпечення кібербезпеки комплексна дія яких стосовно потенційних загроз кібербезпеці репрезентувала свій кінцевий результат у вигляді профілактики та запобігання вказаних загроз.

Підвидами проактивного реагування на загрози кібербезпеці є:

запобігання загрозам кібербезпеці – це вплив силами і засобами СЗКБ на процес підготовки до реалізації загрози, на її джерело або її носія / супротивника;

профілактика загроз кібербезпеці – це вплив силами і засобами СЗКБ на процеси в кібербезпековому середовищі з метою створення умов, які унеможливлюють виникнення загроз кібербезпеці.

На нашу думку, з метою скорочення часу на впровадження в практику забезпечення кібербезпеки національної рамки доцільно використовувати міжнародні та національні стандарти розвинутих країн в

галузі менеджменту інформаційної безпеки, а саме: ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27000:2009, ISO/IEC 27003:2010, ISO/IEC 27004:2009, ISO/IEC 27005:2008, ISO/IEC 27006:2007, ISO/IEC 17021:2006, ISO 19011:2002 [179; 180].

Наразі в Україні активно впроваджуються системи менеджменту інформаційної безпеки на основі міжнародного стандарту ISO/IEC 27001, що пояснюється популярністю згаданого стандарту та нагальною потребою організацій у захисту своїх нематеріальних активів [179; 180].

Розподіл відповідальності суб'єктів забезпечення кібербезпеки на загальнодержавному рівні за організацію та результати державного реагування на загрози кібербезпеки ґрунтується на основі чинного законодавства в галузі національної безпеки України та кібербезпеки України [145; 149; 153; 154], зокрема:

1) на загальнодержавному рівні в реагуванні на кіберзагрози воєнного характеру, загрози інформаційній інфраструктурі України, джерелом яких є системні та масштабні дій проти інтересів України у кіберпросторі іноземних держав, приймають участь такі сили сектору безпеки і оборони України, як-от:

Міністерство оборони України та ЗСУ – головні виконавці;

Державна служба спеціального зв'язку та захисту інформації України, розвідувальні органи України, СБУ – безпосередня участь;

Управління державної охорони України, органи загальної компетенції (ВРУ, КМУ, РНБО, МЗС), Міністерство внутрішніх справ України та підпорядковані йому сили сектору безпеки: Державна прикордонна служба України, Національна гвардія України, Державна міграційна служба України, Державна служба надзвичайних ситуацій – допоміжна роль сприяння у виконанні завдань щодо реагування;

оборонно-промисловий комплекс – забезпечення виконання завдань за призначенням;

2) на загальнодержавному рівні в реагуванні на кіберзагрози

кримінального, терористичного та іншого характеру, приймають участь такі сили сектору безпеки і оборони України, як-от:

СБУ – головний виконавець;

Державна служба спеціального зв'язку та захисту інформації України, Міністерство оборони України та ЗСУ, розвідувальні органи України – безпосередня участь;

Управління державної охорони України, органи загальної компетенції (ВРУ, КМУ, РНБО, МЗС), Міністерство внутрішніх справ України та підпорядковані йому сили сектору безпеки: Державна міграційна служба України, Державна служба надзвичайних ситуацій, Національна гвардія України, Державна прикордонна служба України – допоміжна роль сприяння у виконанні завдань щодо реагування;

оборонно-промисловий комплекс – забезпечення виконання завдань за призначенням;

3) на загальнодержавному рівні в реагуванні на загрози злому систем комп'ютерної безпеки приймають участь такі сили сектору безпеки і оборони України, як-от:

СБУ – головний виконавець;

розвідувальні органи України, Державна служба спеціального зв'язку та захисту інформації України, Міністерство оборони України та ЗСУ – безпосередня участь;

Управління державної охорони України, органи загальної компетенції (ВРУ, КМУ, РНБО, МЗС), Міністерство внутрішніх справ України та підпорядковані йому сили сектору безпеки: Національна гвардія України, Державна служба надзвичайних ситуацій, Державна прикордонна служба України, Державна міграційна служба України – допоміжна роль сприяння у виконанні завдань щодо реагування;

оборонно-промисловий комплекс – забезпечення виконання завдань за призначенням;

4) на загальнодержавному рівні в реагуванні на загрози системних

порушень у сферах криптографічного і технічного захисту інформації, що загрожують національній безпеці України, приймають участь такі сили сектору безпеки і оборони України, як-от:

розвідувальні органи України, Державна служба спеціального зв'язку та захисту інформації України – головні виконавці;

СБУ – безпосередня участь;

Міністерство оборони України та ЗСУ, Управління державної охорони України, органи загальної компетенції (ВРУ, КМУ, РНБО, МЗС), Міністерство внутрішніх справ України та підпорядковані йому сили сектору безпеки: Державна служба надзвичайних ситуацій, Національна гвардія України, Державна міграційна служба України, Державна прикордонна служба України, оборонно-промисловий комплекс – допоміжна роль сприяння у виконанні завдань щодо реагування.

Розподіл відповідальності суб’єктів забезпечення кібербезпеки України на відомчому та внутрішньовідомчому рівнях за організацію та результати державного реагування на загрози кібербезпеки в дисертаційній роботі нами не розглядаються.

З метою удосконалення інформаційного механізму забезпечення кібербезпеки України пропонуємо дотримуватися науково обґрунтованих принципів стратегічних комунікацій у сфері супроводження політики забезпечення кібербезпеки, як-от [204; 224], а саме:

методологічних принципів стратегічних комунікацій у сфері супроводження політики забезпечення кібербезпеки:

принципу науковості стратегічних комунікацій у сфері супроводження політики забезпечення кібербезпеки, який означає використання теоретичних засад, висновків і рекомендацій безпекознавста, суспільних та гуманітарних наук, стратегічних комунікацій в процесі формування системи стратегічних комунікацій у сфері забезпечення кібербезпеки, планування, здійснення та оцінки результатів заходів стратегічних комунікацій;

принципу єдності теорії і практики стратегічних комунікацій у сфері супроводження політики забезпечення кібербезпеки, який передбачає розвиток теоретичних засад вказаної діяльності, й водночас систематизацію, узагальнення та поширення позитивного досвіду стратегічних комунікацій у цій сфері;

принципу верховенства права та законності в організації заходів стратегічних комунікацій у сфері супроводження політики забезпечення кібербезпеки;

принципу підпорядкованості мети, функцій та завдань стратегічних комунікацій у сфері супроводження політики забезпечення кібербезпеки положенням Закону України «Про основні засади забезпечення кібербезпеки України» [149], Стратегії кібербезпеки України [154] та вітчизняного законодавства, що регулює питання національної безпеки і оборони;

принципу безпосереднього зв'язку із суспільним життям країни та практикою суспільно-інформаційних відносин;

принципу взаємозв'язку стратегічних комунікацій у сфері супроводження політики забезпечення кібербезпеки із практикою стратегічних комунікацій у інших сферах національної безпеки;

організаційних принципів стратегічних комунікацій у сфері супроводження політики забезпечення кібербезпеки:

принципу оптимальної відповідності цілей системи стратегічних комунікацій у сфері супроводження політики забезпечення кібербезпеки, її структурі та функціям, динаміці і організаційним процесам. Цей принцип передбачає відповідність загальних можливостей реалізації функцій системи стратегічних комунікацій у сфері супроводження цілям політики забезпечення кібербезпеки, темпам і змістовним змінам у практиці публічного управління кібербезпекою;

принципам плановості і послідовності реалізації стратегічних комунікацій у сфері супроводження політики забезпечення кібербезпеки;

принципу оперативності, що передбачає своєчасність та адекватність заходів стратегічних комунікацій у сфері супроводження політики забезпечення кібербезпеки, що пов’язано із динамічними змінами безпекового середовища [140, с. 12];

принципу підконтрольності стратегічних комунікацій у сфері супроводження політики забезпечення кібербезпеки органам державної влади, що безпосередньо опікуються питаннями забезпечення кібербезпеки;

принципу взаємодоповнюючого використання державних та недержавних ЗМІ в інтересах забезпечення кібербезпеки з метою поширення у суспільній свідомості ідей цифрової грамотності та актуальності кібербезпеки в інформаційному суспільстві;

методичних принципів стратегічних комунікацій у сфері супроводження політики забезпечення кібербезпеки:

принципу оптимального поєднання заходів інформування та пропаганди в інтересах забезпечення кібербезпеки;

принципу здійснення інформування громадян України з питань кібербезпеки по всіх можливих каналах.

Ці принципи взаємозв'язані і реалізуються в єдності.

З метою удосконалення механізму забезпечення комунікації суб’єктів забезпечення кібербезпеки пропонуємо здійснювати інформаційну взаємодію між згаданими суб’єктами на основі принципів [92; 199]:

верховенства права й законності з питань гарантування інформаційної безпеки громадян, суспільства й держави;

значущості управлінської інформації – оперативності, відповідності інформації для розробки єдиного стратегічного задуму (рішення, плану тощо) та реалізації заходів проактивного та реактивного реагування на загрози кібербезпеці;

об’єктивності, системності, неперервності, узгодженості, верифікації, «здорової» конкурентності у сфері інформаційно-аналітичного забезпечення державного реагування на загрози кібербезпеці;

єдиних критеріїв оцінки загроз кібербезпеці та наслідків їх реалізації на основі діагностичних та прогностичних моделей вказаних загроз;

взаємодії аналітики – розвідки – політики з питань організації проактивного і реактивного реагування на загрози кібербезпеці;

єдності технологічної та інформаційної платформ реагування на загрози кібербезпеки;

єдиних аналітичних стандартів, які призначені для розробки аналітичних документів у сфері реагування на загрози кібербезпеки;

адаптивної ефективності інформаційно-аналітичного забезпечення державного реагування на загрози кібербезпеки.

З метою удосконалення механізму інформаційно-аналітичного забезпечення кібербезпеки пропонуємо розробити та впровадити в публічно-управлінську практику забезпечення кібербезпеки:

паспорти загроз кібербезпеці;

моделі загроз кібербезпеці на основі аналізу сучасних тенденцій кібервійни, а саме: моделей загроз кібербезпеці воєнного, терористичного, кримінального характеру;

діагностичної та прогностичної моделей загроз кібербезпеці, що слугуватиме основою для розробки технологій проактивного та реактивного реагування на згадані загрози.

З метою удосконалення механізмів реагування на загрози кібербезпеці пропонуємо розробити та впровадити в публічно-управлінську практику забезпечення кібербезпеки:

технології проактивного реагування на загрози у цій сфері;

технології реактивного реагування на загрози у цій сфері.

Варто зазначити, що нами в [79; 80] доведено, що паспортизація загроз кібербезпеці, технологізація державного реагування на загрози

кібербезпеці слугують теоретичною основою удосконалення СЗКБ загалом, й зокрема механізму інформаційно-аналітичного забезпечення кібербезпеки, механізмів проактивного та реактивного реагування на виявлені загрози кібербезпеці.

З метою удосконалення механізму міжнародного й міждержавного співробітництва з питань забезпечення кібербезпеки України пропонуємо здійснювати згадане співробітництво основі принципів [203, с. 68-71]:

принцип рефлексії, що передбачає з'ясування проблем співробітництва у відповідній сфері в контекстній залежності від трансформацій зовнішнього та внутрішнього безпекового середовища;

принцип самоорганізації, що передбачає віднаходження у флюктуаціях зовнішнього безпекового середовища корисні стимули для системи співробітництва у відповідній сфері й посилення їх у контурах позитивного зворотного зв'язку. За таких умов відбувається самопосилення та стабілізація системи співробітництва у відповідній сфері;

принцип безупинної адаптації, що передбачає врахування вимог динамічного безпекового середовища щодо своєчасного та адекватного реагування на загрози різного характеру.

На наше переконання впровадження в публічно-управлінську практику забезпечення кібербезпеки України наданих пропозицій дозволить забезпечити організаційну та інституційну стійкість СЗКБ України.

Висновки до третього розділу

1. В умовах, коли СЗКБ України залишається остаточно не сформованою і не готовою функціонувати як єдина функціональна структура, існує нагальна необхідність виконання певних невідкладних дій щодо реформування вказаної системи, а саме:

удосконалення когнітивної, організаційної, правової, самоорганізаційної та соціокультурної складових інституціонального середовища публічного управління кібербезпекою України, що в свою чергу стане запорукою удосконалення структури та змісту інституціональної матриці згаданого управління;

удосконалення механізмів забезпечення кібербезпеки – державно-політичного, правового, інформаційного, інформаційно-аналітичного, інституційного, організаційного, соціально-психологічного, кадрового, фінансового, механізму партисипаторної взаємодії, механізму державного реагування на загрози кібербезпеці.

2. У розділі запропоновано структурно-функціональну модель публічного управління кібербезпекою, а також взаємозв'язок функцій СЗКБ, соціально-інформаційних відносин, що значним, а інколи й визначальним чином детермінуються змінами в безпековому кіберсередовищі.

Встановлено, що упровадження структурно-функціональної моделі публічного управління кібербезпекою в практику гарантування кібербезпеки сприятиме підвищенню ефективності СЗКБ.

3. Обґрунтовано, що проектування СЗКБ України має здійснюватися в рамках загальної теорії систем, інституційної теорії, теорії державного управління, теорії публічного управління, теорій національної, інформаційної та кібернетичної безпеки, теорій гібридної, інформаційної війн та кібервійни. При цьому проектування СЗКБ має ґрунтуватися на системній, нормативно-правовій, інституціональній, інноваційній парадигмах проектувальної діяльності.

Удосконалення СЗКБ України в сучасних умовах російсько-української війни передбачає впровадження в практику публічного управління кібербезпекою України перспективної моделі СЗКБ, складовими якої є функціональна, інформаційна, інституційна моделі.

Перспективна функціональна модель СЗКБ України структурно містить:

Рефлексивний блок: соціально-психологічний механізм усвідомлення проблематики забезпечення кібербезпеки, інформаційно-аналітичний механізм, державно-політичний механізм, механізм науково-методичного забезпечення реагування на загрози кібербезпеці.

Організаційно-управлінський блок: правовий, інституційний та організаційно-адміністративний механізми, механізми розробки та реалізації державної політики у сфері кібербезпеки, механізми кадрового, технічного, ресурсного та фінансового забезпечення кібербезпеки.

Інструментальний блок: механізми реактивного та проактивного реагування на загрози кібербезпеці; механізми партисипаторної взаємодії, міжнародного й міждержавного співробітництва у сфері забезпечення кібербезпеки; механізм інтеграції національного кіберпростору у світовий кіберпростір.

Перспективна інформаційна модель СЗКБ України представлено блоками:

1 блок. Нормативно-правова модель: чинне законодавство, що регулює діяльність суб’єктів забезпечення кібербезпеки та регламентує формування та функціонування СКБ та її складової – СЗКБ.

2 блок. Ситуативна модель: блок даних – організація аналітичної інформації про кіберзагрози; блок ситуацій –опис можливих сценаріїв реалізації загроз кібербезпеці.

3 блок. Концептуальна модель: блок цілі – формулювання цілей реактивного та проактивного реагування на кіберзагрози; блок вибору – вибір критерію оптимальності дій реагування на кіберзагрози.

4 блок. Математична модель: система математичних співвідношень, які описують процес забезпечення кібербезпеки.

5 блок. Модель розробки варіантів управлінських рішень у сфері забезпечення кібербезпеки, у рамках яких визначаються напрями політики забезпечення кібербезпеки та пріоритети розвитку СЗКБ.

Перспективна інституційна модель СЗКБ України структурно має містити такі підсистеми та відповідні механізми забезпечення кібербезпеки, як-от:

а) інституційну підсистему СЗКБ, яка структурно містить: механізм соціально-психологічного усвідомлення проблематики забезпечення кібербезпеки; державно-політичний механізм забезпечення кібербезпеки; правовий механізм забезпечення кібербезпеки; інституційний механізм забезпечення кібербезпеки; механізм партисипаторної взаємодії між державою, громадянським суспільством та ІТ-бізнесом; механізм розробки політики забезпечення кібербезпеки;

б) функціональну підсистему СЗКБ, яка структурно містить комплексний механізм реалізації політики забезпечення кібербезпеки;

в) організаційно-управлінську підсистему СЗКБ, яка структурно містить: організаційно-адміністративний механізм забезпечення кібербезпеки; механізм міжнародного й міждержавного співробітництва з питань забезпечення кібербезпеки; механізм інформаційно-технологічного забезпечення реагування на загрози кібербезпеці; механізм інтеграції кіберпростору України у світовий кіберпростір; механізм забезпечення управлінської взаємодії суб’єктів забезпечення кібербезпеки;

г) адаптаційно-проектувальну підсистему СЗКБ, яка структурно містить: механізм науково-методичного забезпечення кібербезпеки; механізм розробки політики забезпечення кібербезпеки; інформаційно-аналітичний механізм забезпечення кібербезпеки;

д) культурно-ідеологічну підсистему СЗКБ, яка структурно містить інформаційний механізм забезпечення кібербезпеки;

є) партисипаторну підсистему СЗКБ, яка структурно містить: механізм партисипаторної взаємодії між державою, громадянським суспільством та

ІТ-бізнесом;

е) комунікативну підсистему СЗКБ, яка структурно містить механізм забезпечення комунікації суб'єктів забезпечення кібербезпеки.

4. З метою удосконалення державно-політичного механізму забезпечення кібербезпеки запропоновано чітко розмежувати публічне управління кібербезпекою на три складових, а саме на: публічно-політичну, адміністративну, оперативну складові.

З метою удосконалення соціально-психологічного механізму усвідомлення проблем забезпечення кібербезпеки запропоновано розробити та упровадити в публічно-управлінську практику структурно-логічних моделей реалізації функцій «планування», «комунікація», «мотивація», «прийняття публічно-управлінських рішень», «контроль» у публічному управлінні кібербезпекою.

З метою удосконалення механізму розробки політики забезпечення кібербезпеки запропоновано функціональну модель визначення імперативів політики забезпечення кібербезпеки в умовах трансформації безпекового кіберсередовища.

Для удосконалення правового механізму забезпечення кібербезпеки запропоновано внести зміни до Стратегії кібербезпеки України в частині визначення загроз кібербезпеці з урахуванням реальних та потенційних загроз кібербезпеці України в умовах зовнішньої агресії росії та визначення ризиків у сфері кібербезпеки України.

З метою удосконалення організаційно-адміністративного механізму забезпечення кібербезпеки запропоновано розробити та офіційно затвердити національну рамку реагування на загрози кібербезпеці.

З метою удосконалення інформаційного механізму забезпечення кібербезпеки України пропонуємо дотримуватися науково обґрунтованих принципів стратегічних комунікацій у сфері супроводження політики забезпечення кібербезпеки.

З метою удосконалення механізму забезпечення комунікації

суб’єктів забезпечення кібербезпеки запропоновано здійснювати інформаційну взаємодію між згаданими суб’єктами на основі відповідних науково обґрунтованих принципів.

З метою удосконалення інформаційно-аналітичного механізму забезпечення кібербезпеки запропоновано розробити та упровадити в публічно-управлінську практику паспорти загроз кібербезпеці, моделі загроз кібербезпеці.

З метою удосконалення механізму державного реагування на загрози кібербезпеці запропоновано розробити та упровадити в публічно-управлінську практику технології проактивного та реактивного реагування на загрози кібербезпеці.

З метою удосконалення механізму міжнародного й міждержавного співробітництва з питань забезпечення кібербезпеки України запропоновано здійснювати згадане співробітництво на основі відповідних науково обґрунтованих принципів.

З метою удосконалення кадрового механізму забезпечення кібербезпеки запропоновано внести зміни до програми підготовки фахівців-управлінців у сфері національної безпеки.

В розділі підтверджено гіпотезу дослідження, яка полягає в тому, що впровадження позитивного досвіду НАТО та ЄС щодо управління кібербезпекою у вітчизну державно-управлінські практику у цій сфері значною мірою вдосконалить інституційну структуру СЗКБ України. Це стане запорукою надійного захисту національних інтересів у цій специфічній сфері.

Основні результати третього розділу дисертаційного дослідження висвітлено у низці публікацій автора [79; 80; 82].

ВИСНОВКИ

В дисертації вирішено актуальне науково-практичне завдання в галузі знань «Публічне управління та адміністрування», яке полягає в обґрунтуванні науково-теоретичних засад державних механізмів забезпечення кібербезпеки в сучасних умовах російсько-української війни і розробка на цій основі пропозицій щодо підвищення результативності їх функціонування. Отримані результати дослідження, реалізовані мета й завдання дослідження дозволили сформулювати такі висновки й пропозиції:

1. Аналіз джерел та результатів наукових досліджень із проблематики публічного управління кібербезпекою України, дозволяє констатувати, що: в офіційному дискурсі кібербезпеки України визначено правові засади розбудови СКБ і діяльності суб'єктів забезпечення кібербезпеки; науковий дискурс забезпечення кібербезпеки України представлено такими напрямами наукових досліджень, як-от – правовим, інформаційно-технічним, державно-управлінським та публічно-управлінським. Останній є найбільш «молодим», а тому менше розроблений порівняно з рештою; встановлено, що в науковому дискурсі забезпечення кібербезпеки України проектування та державне конструювання СКБ, результативне та ефективне функціонування СЗКБ України, адаптація вказаних систем до вимог динамічного безпекового кіберсередовища щодо своєчасного й адекватного реагування на кіберзагрози різного характеру залишаються найгострішими проблемами сучасності.

2. Уточнено зміст категорій та понять, які стосуються публічно-управлінської проблематики забезпечення кібербезпеки, що дало змогу побудувати стратифікаційну модель реалізації функцій публічного управління кібербезпекою. Цю модель подано у вигляді семи страт: а) страти процесу публічного управління кібербезпекою, на якій розкриваються уявлення про зміст та суб'єкти, цілі, засоби, результати

публічного управління у цій специфічній сфері; б) страти функцій «комунікація», «планування», «організація», «контроль», «мотивація», «прийняття публічно-управлінських рішень», на яких розкриваються уявлення про діяльність та взаємодію суб'єктів забезпечення кібербезпеки, а також механізми забезпечення кібербезпеки.

Стратифікаційне та ешелоноване відображення основних функцій публічного управління кібербезпекою дозволило здійснити системний аналіз і опис процесів реалізації згаданих функцій, а також системно відобразити процес створення інституціонального середовища публічного управління кібербезпекою та удосконалення СЗКБ з урахуванням рухомості інституціонального середовища публічного управління, трансформацій безпекового кіберсередовища.

3. Обґрунтовано, що проектування та державне конструювання СЗКБ, як багаторівневої та багатоструктурованої сукупності механізмів забезпечення кібербезпеки має здійснюватися в рамках загальної теорії систем, інституційної теорії, теорій державного й публічного управління, теорій національної та інформаційної безпеки, кібербезпеки, теорій інформаційної війни та кібервійни. При цьому проектування СЗКБ має ґрунтуватися на системній, інноваційній, нормативно-правовій та інституціональній парадигмах проектувальної діяльності.

Обґрунтовано, що функціонування державних механізмів забезпечення кібербезпеки має здійснюватися в рамках теорії ефективності механізму державного реагування на загрози національній безпеці.

4. Доведено, що кібервійна має значну, а інколи й визначальну роль в структурі сучасного геополітичного інформаційного протиборства. Сучасна кібервійна може бути інтерпретована як система узгоджених за ціллю, місцем та часом інформаційних дій у кіберпросторі із використанням програмних кодів задля захоплення управління (часткове, повне) або руйнування інформаційного зв'язку, що перешкоджає штатному функціонуванню систем управління інформацією у сферах

публічного, державного та військового управління, в бізнесі й приватній сфері життєдіяльності людини.

Цілями кібервійни можуть бути: знищення або перехоплення даних з метою перекриття доступу до інформаційних джерел конкурентам / супротивнику; захоплення інформаційних ресурсів супротивника або конкурентів; переведення «чужої» системи автоматизованого управління в режим, який відповідає інтересам активної сторони інформаційного протиборства; призупинення функціонування «чужої» автоматизованої системи управління або її знищення задля зміни характеристик зовнішнього кіберсередовища; руйнування цілісності інформаційної інфраструктури банківської та економічної систем, системи публічного та державного управління задля створення хаосу у різних сферах суспільного життя; руйнування цілісності інформаційної інфраструктури систем воєнної безпеки держави та військового управління; руйнування цілісності інформаційної інфраструктури приватного життя людини / громадянина, зокрема викрадення персональних даних та ін.; зміна характеристик безпекового кіберсередовища.

На основі вивчення законів та закономірностей інформаційної глобалістики, інформаційної геополітики, інформаційної війни та кібервійни було визначено закономірності розвитку СКБ та СЗКБ, а саме: за умов втрати державою спроможності щодо захисту державного суверенітету, зокрема інформаційного та цифрового суверенітету – обмежуються спроможності її конструктивного впливу на процеси забезпечення інформаційної безпеки та кібербезпеки, інформаційного розвитку суспільства в цілому; сучасні геополітичні центри сили намагаються підірвати інформаційну могутність своїх конкурентів за допомогою економічних та інформаційно-технічних інструментів, що негативно позначить на функціонуванні та удосконаленні СКБ та СЗКБ країн-конкурентів; результативність СКБ та ефективність СЗКБ забезпечується врахуванням при проектуванні та конструюванні вказаних систем поточних змін та майбутнього безпекового

кіберсередовища.

5. З’ясовано, що наразі механізми формування і реалізації політики у сфері кібербезпеки країн-членів НАТО і ЄС є досить ефективними й адаптивними в умовах сучасного геополітичного інформаційного протиборства. Позитивним моментом є те, що наразі державно-управлінська еліта країн-членів НАТО і ЄС у своїй діяльності у сфері забезпечення кібербезпеки приділяє рівнозначну увагу як питанням довгострокової, так і поточної політики у цій сфері. Зокрема, довгострокова державна політика забезпечення кібербезпеки спрямована на вирішення важливих стратегічних питань – прогнозування змін безпекового кіберсередовища та майбутніх тенденцій розвитку загроз кібернетичного характеру, побудова принципово нової СЗКБ, яка б враховувала майбутні трансформації безпекового кіберсередовища й була спроможною до проактивного реагування на нові загрози та виклики. Поточна державна політика забезпечення кібербезпеки спрямована на вирішення тактичних та оперативних питань реактивного реагування на загрози кібербезпеці.

З’ясовано, що керівництвом країн-членів НАТО і ЄС досягнуло значних результатів в розбудові національних СЗКБ, а саме: а) реалізовано перспективну модель СКЗБ на основі задіяння компонентів забезпечення кібербезпеки, які визначено в керівних документах ЄС і НАТО; б) сформовано інституційне середовище публічного управління кібербезпекою, яке структурно містить правовий, організаційний, когнітивний, самоорганізаційний та соціокультурний компоненти.

Обґрунтовано доцільність використання у практиці публічного управління кібербезпекою України досвіду країн-членів НАТО і ЄС щодо: визначення перспективної моделі СЗКБ; формування інституційного середовища публічного управління кібербезпекою з урахуванням вимог зовнішнього та внутрішнього безпекового кіберсередовища до національної СЗКБ.

6. Доведено, що в Україні функціонує СЗКБ з усіма її перевагами і недоліками. Наразі вказана система залишається остаточно не сформованою, й в сучасних умовах російсько-української війни в повній мірі не задовольняє потреби щодо своєчасного та адекватного реагування на виклики та загрози кібербезпеці України. Суб'єкти забезпечення кібербезпеки здійснюють лише окремі види забезпечення кібербезпеки, що значно знижує можливу інтегральну ефективність СЗКБ. Такий стан справ у цій специфічній сфері може призвести до небезпечної різноспрямованості заходів державного реагування на загрози кібербезпеці України.

Виявлено актуальні проблеми функціонування державних механізмів забезпечення кібербезпеки України, як-от: проблема забезпечення кібербезпеки України в умовах російсько-української війни, що зумовлені браком систематизованих знань про сучасні технології кібервійни, а також браком аналітичної інформації необхідної для прийняття рішень щодо ефективного реагування на виклики та загрози кібербезпеці; проблема своєчасної адаптації нормативно-правової бази у сфері забезпечення кібербезпеки з урахуванням появи нових викликів, загроз, небезпек кібернетичного характеру; проблема наявних розривів між базовими соціальними інститутами, які визначають зміни в інституціональному середовищі публічного управління кібербезпекою, а також інституційних розривів між суміжними інститутами зовнішнього та внутрішнього інституціонального середовища публічного управління кібербезпекою, інституційного розриву між загальним станом інституту аналітичної діяльності в СЗКБ та складністю безпекового кіберсередовища; проблема наявних розривів в організації діяльності суб'єктів забезпечення кібербезпеки України; проблема удосконалення структури, уточнення функцій та конкретизація завдань СЗКБ, а також проблема удосконалення державних механізмів забезпечення кібербезпеки; проблема низької загальної ефективності механізму державного реагування на загрози

кібербезпеці України та інформаційно-аналітичного механізму забезпечення кібербезпеки України.

Показано, що створення державних механізмів забезпечення кібербезпеки є поетапним, поступовим, тривалим за часом процесом, який включає змістовну складову і вимагає проведення відповідної роботи у нормативно-правовому, організаційно-управлінському, фінансовому, безпековому, кадровому та освітньому аспектах.

7. З метою вдосконалення механізмів забезпечення кібербезпеки України в умовах євроінтеграції та зовнішньої агресії росії перспективною моделлю СЗКБ визначено креативну модель та сформульовано пропозиції органам державної влади щодо її упровадження в публічно-управлінську практику, як-от:

1 група пропозицій щодо визначення пріоритетних напрямів вдосконалення інституціонального середовища публічного управління кібербезпекою України:

теоретичний напрям, що передбачає формування базових засад формування інституціонального середовища публічного управління кібербезпекою, зокрема загальні положення, базові категорії і поняття публічно-управлінської проблематики забезпечення кібербезпеки; теоретичні підходи до формування інституціонального середовища публічного управління кібербезпекою;

правовий напрям, що спрямований на вдосконалення нормативно-правового забезпечення формування інституціонального середовища публічного управління кібербезпекою, а також внесення змін до Стратегії кібербезпеки України в частині визначення загроз кібербезпеці з урахуванням реальних та потенційних загроз кібербезпеці України в умовах зовнішньої агресії росії та визначення ризиків у сфері кібербезпеки України;

організаційний напрям, що передбачає створення інституціональної матриці й удосконалення механізмів забезпечення кібербезпекою;

2 група пропозицій щодо вдосконалення: 1) державно-політичного механізму забезпечення кібербезпеки, що передбачає розробку та впровадження у вітчизняну публічно-управлінську практику структурно-функціональної моделі публічного управління кібербезпекою, а також чітке розмежування публічного управління кібербезпекою на три складових, а саме на: публічно-політичну, адміністративну, оперативну складові; 2) механізму розробки політики забезпечення кібербезпеки, що передбачає розробку та впровадження у вітчизняну публічно-управлінську практику функціональну модель визначення імперативів політики забезпечення кібербезпеки в умовах трансформації безпекового кіберсередовища;

3 група пропозицій щодо удосконалення соціально-психологічного механізму усвідомлення проблем забезпечення кібербезпеки, що передбачає розроблення та упровадження в публічно-управлінську практику структурно-логічних моделей реалізації функцій «комунікація», «планування», «мотивація», «прийняття публічно-управлінських рішень», «контроль» у публічному управлінні кібербезпекою;

4 група пропозицій щодо удосконалення кадрового механізму забезпечення кібербезпеки, що передбачає внесення відповідних змін до програми підготовки фахівців-управлінців у сфері національної безпеки;

5 група пропозицій щодо удосконалення СЗКБ України в сучасних умовах російсько-української війни, що передбачає впровадження в публічно-управлінську практику перспективної моделі СЗКБ, яка структурно містить складові, як-от: функціональна, інформаційна, інституційна моделі.

6 група пропозицій щодо удосконалення інформаційно-аналітичного механізму забезпечення кібербезпеки, що передбачає впровадження в публічно-управлінську практику інформаційно-аналітичної діяльності автоматизованих систем збирання й структуризації інформації, а також розвиток науково-методичного апарату інформаційно-аналітичного

забезпечення політики забезпечення кібербезпеки, зокрема: визначення системи показників оцінки рівня загроз кібербезпеки; визначення системи критеріїв оцінки ефективності механізмів державного реагування на загрози кібербезпеці; розробку та впровадження в публічно-управлінську практику забезпечення кібербезпеки паспортів загроз у цій сфері;

7 група пропозицій щодо удосконалення механізму державного реагування на виклики та загрози кібербезпеці, що передбачає: розробку та впровадження у публічно-управлінську практику технологій державного реагування на загрози кібербезпеці; визначення змісту механізмів реактивного та проактивного реагування на загрози кібербезпеці.

8 група пропозицій щодо удосконалення організаційно-адміністративного механізму забезпечення кібербезпеки передбачає розробку та офіційне затвердження національної рамки реагування на загрози кібербезпеці.

9 група пропозицій щодо удосконалення інформаційного механізму забезпечення кібербезпеки України передбачає дотримання науково обґрунтованих принципів стратегічних комунікацій у сфері супроводження політики забезпечення кібербезпеки.

10 група пропозицій щодо удосконалення механізму забезпечення комунікації суб’єктів забезпечення кібербезпеки передбачає здійснення інформаційної взаємодії між згаданими суб’єктами на основі відповідних науково обґрунтованих принципів.

11 група пропозицій щодо удосконалення механізму міжнародного й міждержавного співробітництва з питань забезпечення кібербезпеки України, що передбачає здійснення згаданого співробітництва на основі відповідних науково обґрунтованих принципів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абрамов В.І. Духовність суспільства: методологія системного вивчення: монографія. К.: КНЕУ, 2004. 236 с.

2. Абрамов В. І., Зюзя О. В. Удосконалена базова модель міждержавного протиборства з урахуванням сучасних тенденцій російсько-української війни. *Державне управління: удосконалення та розвиток*. 2022. № 5. URL: http://www.dy.nayka.com.ua/?op=1&z=2679

3. Абрамов В.І. Мережева архітектура публічного управління: проблеми концептуалізації і практики забезпечення національної безпеки. *Державна служба та публічна політика: проблеми і перспективи розвитку* : матеріали щоріч. всеукр. наук.-практ. конф. за міжнар. участю, м. Київ, 27 трав. 2016 р. / за заг. ред. А.П. Савкова, М.М. Білинської, С.В. Загороднюка. К.: НАДУ, 2016. С. 241-243.

4. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 26 березня 2021 р.). [Електронне видання]. Київ : НА СБУ, 2021. 346 с. URL: https://academy.ssu.gov.ua/uploads/p_57_53218641.pdf

5. Аналітична доповідь Національного інституту стратегічних досліджень до щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України» (2020). URL: https://www.president.gov.ua/storage/j-files-storage/00/95/25/4d9f69fcaf6e5c6605b334c09fecad60_1603202563.pdf

6. Аналітична доповідь Національного інституту стратегічних досліджень до щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України» (2021). URL: https://niss.gov.ua/publikatsiyi/poslannya-prezydenta-ukrayiny/analitychna-dopovid-do-shchorichnoho-poslannya

7. Аналітичний огляд проблем інформаційного й електронного права в Україні URL:

http://www.itsway.kiev.ua/index.php?language=ru&main_managemen=about&managemen=eGov_Zak.

8. Антонюк В. В. Інформаційна війна в структурі сучасного геополітичного протиборства: нові контексти та інтерпретації. *Державне управління: удосконалення та розвиток*. 2021. № 7. URL: http://www.dy.nayka.com.ua/?op=1&z=2121

9. Антонюк В.В. Організаційно-правові засади формування та реалізації державної політики інформаційної безпеки України: автореф. дис... канд. наук держ. упр.: 25.00.02 / НАДУ. К., 2017. 20 с.

10. Арсенович Л.А. Шляхи удосконалення функціонування національної системи кібербезпеки в освітній сфері. *Публічне управління і адміністрування в Україні*. 2023. Вип. 33. С. 35-41

11. Бакуменко В. Д. Формування державно-управлінських рішень: проблеми теорії, методології, практики: монографія. К. : Вид-во УАДУ, 2000. 328 с.

12. Балан М.І. Державне реагування на загрози суспільно-політичній стабільності в Україні : дис. … докт. філософії: спец. 281 / НАДУ. К., 2020. 222 с.

13. Бараненко Р.В., Задорожна А. Ю. Кібервійна як новий вид протистояння держав. *Південноукраїнський правовий часопис*. 2017. № 1. С. 53-56.

14. Баловсяк Н. Як ведуться сучасні кібервійни. Попередній аналіз. URL: https://tyzhden.ua/iak-vedutsia-suchasni-kibervijny-poperednij-analiz/

15. Безопасная Европа в мире, который должен стать лучше. Европейская стратегия безопасности. URL: http://www.consilium.europa.eu/uedocs/cmsUpload/031208ESSIIRU.pdf.

16. Бортнікова О.Г. Взаємодія релігії і політики: теорія і методологія: монографія. К.: ПАЛИВОДА А.В., 2017. 338 с.

17. Брижко В. М., Гальченко О.М., Цимбалюк В. С., Орєхов О. А.,

Чорнобров А. М. Інформаційне суспільство. Дефініції. К., 2002. 220 с.

18. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. К. : НАУ. 2013. 432 с.

19. Бурячок В.Л., Богуш В.М. Кібербезпека та захист критичної інформаційної інфраструктури. *Ukrainian Scientific Journal of Information Security.* 2014. № 2. С. 119–148.

20. Бухарєв В.В. Адміністративно-правові засади забезпечення кібербезпеки України: дис. ... канд. юрид. наук : 12.00.07 / Сумський держ. ун-т. Суми, 2018. 221 с.

21. Валевський О. Л. Держава і реформи в Україні: аналіз державної політики в умовах трансформації суспільства: монографія. К. : НАДУ, 2007. 316 с.

22. Виноградова Н. Л. Взаємообумовленність принципів і закономірностей державного управління: теоретико-методологічний аспект: автореф. дис... канд. наук з держ. упр.: 25.00.01 / Виноградова Наталія Леонідівна; Дніпропетровський регіональний ін-т держ. управління Національної академії держ. управління при Президентові України. Д., 2008. 20 с.

23. Військовий стандарт 01.004.004 (Видання 1). Воєнна політика, безпека та стратегічне планування. Інформаційна безпека держави у воєнній сфері. Терміни та визначення. К.: НУОУ, 2014. 24 с.

24. Власилюк В.Я., Килимчук С.О. Інформаційна безпека держави: курс лекцій. К.: видавничий дім «Скіф», 2008 136с.

25. Воєнно-історичний опис російсько-української війни (вересень 2022 р.) / кол. авт.: керівник авторського колективу В. Залужний. К.: МОУ, ГШЗСУ, 2022. 169 с.

26. Вторжение в Украину : Хроника российской агрессии / Группа «Информационное сопротивление». К.: Брайт Стар Паблишинг, 2016. 240 с.

27. Габрелян А.Ю., Стороженко С.В. Інформаційна безпека: проблеми боротьби з кібер-тероризмом. *Соціум. Наука. Культура:* матеріали Всеукраїнської інтернет-конференції. URL: http://intkonf.org/gabrelyan-ayu-storozhenko-sv-informatsiyna-bezpeka-problemi-borotbi-z-kiber-terorizmom/

28. Гаращенко Ю. В. Державна політика у сфері кібербезпеки України. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне управління*. 2019. № 1. Т. 30 (69). С. 140-145.

29. Глобалізація і безпека розвитку : монографія / О.Г. Білорус, Д.Г. Лук'яненко та ін.; Керівник авт. колективу і наук. ред. О.Г. Білорус. К.: КНЕУ, 2001. 733 с.

30. Глобальные трансформации: политика, экономика, культура: монография / Д. Хелд, Э. Макгрю, Д. Гольдблатт, Д. Перратон ; пер. с англ. В.В. Сапова и др. Мосвка: Праксис, 2004. 576 с.

31. Гнатюк С. Кіберскладник російсько-української війни: уроки та оцінки міжнародної спільноти. URL: https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/kiberskladnyk-rosiysko-ukrayinskoyi-viyny-uroky-ta-otsinky

32. Годлевська В.Ю., Кононенко В.В. Кібербезпека: державне управління у сфері національної безпеки Іспанії. *Дніпровський науковий часопис публічного управління, психології, права*, 2021, № 6. URL: https://chasopys-ppp.dp.ua/index.php/chasopys/article/view/144/129

33. Голубь В. Ефективна держава як модель суспільного розвитку. *Актуальні проблеми державного управління*. 2015. Вип. 2 (62). С. 8-12. URL: http://www.oridu.odessa.ua/9/buk/Zbirnuk-2(62).pdf#page=8

34. Гончар С.Ф. Актуальность исследования и разработки систем защиты информации территориально-распределенных автоматизированных систем управления технологическими процессами. *Кібербезпека-2013*: материали міжнародної науково-практичної конференції, Київ-Ялта, 2013. С. 33-37.

35. Гончар С.Ф. Особенности обеспечения кибербезопасности индустриальных систем управления: тези доповідей міжнародної науково-практичної конференції «*Проблеми та перспективи розвитку енергетики, електротехнологій та автоматики в АПК*», Київ, 2013. С. 36-37.

36. Горбулін В.П., Качинський А.Б. Системно-концептуальні засади стратегії національної безпеки України: монографія. К.: ДП «НВЦ «Євроатлантикінформ», 2007. 592 с.

37. Горбулін В.П., Качинський А.Б. Стратегічне планування: вирішення проблем національної безпеки: монографія. К.: НІСД, 2011. 288 с.

38. Горлинський В.В. Філософія безпеки і сталого людського розвитку: ціннісний вимір: монографія. К.: ПАРАПАН, 2011. 378 с.

39. Горовий С.С., Пряміцин В.Ю. Актуальні питання правового забезпечення кібербезпеки України. *Юридичний науковий електронний журнал*. 2021. № 6. URL: http://www.lsej.org.ua/6_2021/34.pdf

40. Государственное управление в сфере национальной безопасности: словарь-справочник / Под общ. ред. Г.П. Сытника. К.: НАДУ, 2012. 496 с.

41. Громадська організація «Центр національної стійкості і розвитку». URL: https://opendatabot.ua/c/43981126

42. Гурковський В.І. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки: дис. … канд. наук з держ. упр.: спец. 25.00.02. / Гурковський Володимир Ігорович. Київ., 2004. 205 с.

43. Давиденко О.Г. Державне управління системою профілактики та протидії загрозам суспільно-політичній стабільності України: теоретичний аспект: дис. ... канд. наук з держ. упр. : 25.00.01 / НАДУ. К., 2021, 286 с.

44. Данілов О.: В Україні має бути утворений Національний центр координації стійкості. URL: https://www.rnbo.gov.ua/ua/Diialnist/4743.html

45. Декларація саміту НАТО в Страсбурзі. URL: http://www.nato.int.

46. День інформаційного суспільства – 2016 : матеріали щоріч. наук.-практ. конф. за міжнар. участю, м. Київ, 19 трав. 2016 р. / упоряд. : О.Б. Кукарін, Н.О. Дмитренко, С.Г. Соловйов; за заг. ред. А.І. Семенченка. К.: НАДУ, 2016. 284 с.

47. Дзюндзюк В.Б. Кіберзлочинність: загроза національній безпеці. *Державне управління та місцеве самоврядування*: зб. тез XVIII Міжнар. наук. конгресу, 29 березня 2012 р. Х. : Вид-во ХарРІ НАДУ «Магістр», 2012. С. 108-109.

48. Діордіца О.В. Адміністративно-правове регулювання кібербезпеки України: автореф. дис. … док. юр. н.: спец. 12.00.07. / Запорізький національний університет. Запоріжжя.: ЗНУ, 2018. 32 с.

49. Дорошко М. Неоголошена війна Росії проти України у XX – на початку XXI ст.: причини і наслідки. Київ: Ніка-Центр, 2018. 196 с.

50. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва: монографія. К. : НІСД, 2014. 328 с.

51. Дубов Д.В. Геополітичне суперництво у кіберпросторі як чинник впливу на національну безпеку України : дис. … док. політ. наук.: 21.01.01. / НІСД. К., 2016. 434 с.

52. Дубов. Д. В. Стратегічні аспекти кібербезпеки України. *Стратегічні пріоритети.* 2013. № 4. С. 119–127.

53. Експерти обговорили першу в світі кібервійну на науково-практичній конференції в Академії. URL: https://academy.ssu.gov.ua/ua/news-1-8-384-eksperti-obgovorili-pershu-v-sviti-kiberviynu-na-naukovo-praktichniy-konferencii-v-akademii

54. Енциклопедичний словник з державного управління / уклад.: Ю.П. Сурмін, В.Д. Бакуменко, А.М. Михненко та ін.; за ред. Ю.В. Ковбасюка, В.П. Трощинського, Ю.П. Сурміна. К.: НАДУ, 2010. 820 с.

55. Енциклопедія державного управління: у 8 т. / Нац. акад. держ.

упр. при Президентові України ; наук.-ред. колегія : Ю. В. Ковбасюк (голова) та ін. К. : НАДУ, 2011. Т. 1 : Теорія державного управління / наук.-ред. колегія : В. М. Князєв (співголова), І. В. Розпутенко (співголова) та ін. 2011. 748 с.

56. Енциклопедія державного управління: у 8 т. / Нац. акад. держ. упр. при Президентові України ; наук.-ред. колегія : Ю. В. Ковбасюк (голова) та ін. К. : НАДУ, 2011. Т. 2 : Методологія державного управління / наук.-ред. колегія : Ю. П. Сурмін, П. І. Надолишній та ін. 2011. 692 с.

57. Євдоченко Л.О. Удосконалення системи державного забезпечення інформаційної безпеки України в умовах глобалізації: дис. … канд. наук з держ. упр.: спец. 25.00.01. / Євдоченко Леонід Олександрович. Львів., 2011. 225 с.

58. Єрменчук О.П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України : монограф. / О. П. Єрменчук. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.

59. Житник О.М. Формування державної політики національної безпеки в умовах трансформацій у військовій сфері. Автореферат дис. … к. держ. упр. 25.00.02 – механізми державного управління. К.: МАУП, 2021. 20 с.

60. Запорожець Т.В. Цифрова платформа інтелектуального управління у безпековій сфері. *Цифрове врядування* : монографія / за ред. О. В. Карпенка ; О. В. Карпенко, Ж. З. Денисюк, В. В. Наместнік [та ін.] ; Нац. акад. держ. упр. при Президентові України. Київ : ІДЕЯ ПРИНТ, 2020. С. 267-280.

61. Звіт про науково-дослідну роботу «Інституціональні засади розвитку державної системи кризового реагування в Україні» (заключний) / за ред. Т.В. Запорожець. К.: НАДУ, 2018. 110 с.

62. Звіт про науково-дослідну роботу «Дослідження можливих шляхів удосконалення системи забезпечення інформаційної безпеки

Міністерства оборони України та Збройних Сил України». шифр «Глаукус». К.: НУОУ, 2019. 201 с.

63. Звіт про науково-дослідну роботу «Обґрунтування вимог до спроможностей суб'єктів Міністерства оборони України та Збройних Сил України, які залучаються до виконання завдань кібероборони України». шифр «Хорнет». К.: НУОУ, 2020. 158 с.

64. Звіт про науково-дослідну роботу «Розробка науково-методичних засад забезпечення інформаційної безпеки держави у воєнній сфері». шифр «Інфо-ЗІБ». К.: НУОУ, 2013. 86 с.

65. Звіт про науково-дослідну роботу «Удосконалення понятійно-категорійного апарату у сфері кібероборони». шифр «Дефініція». К.: НУОУ, 2020. 203 с.

66. Зеленін В.В. По той бік правди: нейролінгвістичне програмування як зброя інформаційно-пропагандистської війни: навч. посіб. Том 1. НЛП – XX століття. 2-е видання, виправлене та доповнене. К.: Вид-во «Люта справа», 2015. 384 с.

67. Зозуля О.С., Шевченко М.М. Системи забезпечення національної безпеки адаптивного та креативного типів: порівняльний аналіз. *Інвестиції: практика та досвід*. 2015. № 16 С. 125-129.

68. Зозуля О.С., Лєпіхов А.В., Храпач Г.С., Шевченко М.М. Російсько-українська війна: особливості реалізації загроз державному суверенітету України та перспективи виходу з війни. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського*. № 2 (75). 2022. С. 6-15.

69. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора Б. Толубка. К.: ДУТ, 2015. 288 с.

70. Інформаційний вимір гібридної війни: досвід України: матеріали міжнарод. наук.-практ. конф. К. НУОУ, 2017. 104 с.

71. Камчатний М. В. Нормативно-правове закріплення питань кібербезпеки у міжнародному праві URL: http://dspace.nlu.edu.ua/bitstream/123456789/9826/1/Kamchatnuy.pdf

72. Камчатний М.В. Основні ознаки поняття «кібервійна» в сучасному міжнародному праві. *Альманах міжнародного права*. 2017. Вип. 15. С. 12-22. URL: http://nbuv.gov.ua/UJRN/amp_2017_15_4

73. Карпенко О. В. Механізми формування та реалізації сервісно-орієнтованої державної політики в Україні : автореф. дис. д-ра наук з держ.упр. : 25.00.02 / О. В. Карпенко ; НАДУ. К., 2016. 39 с.

74. Кибертерроризм и защита персональных данных. К.: УАЗПД, 2013. 50 с.

75. Кіндзерський Ю. В. Кібербезпека та становлення цифрової економіки: проблеми взаємозв'язку. URL: https://ev.nmu.org.ua/docs/2020/3/EV20203_018-026.pdf

76. Клименко Н. Г. Теоретико-методологічні засади механізму взаємодії органів публічної влади та недержавних інституцій у сфері національної безпеки: автореф. дис. ... д. держ. упр. : 25.00.05 - Державне управління у сфері державної безпеки та охорони громадського порядку / Н. Г. Клименко ; Приватне акціонерне товариство «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом». 2021. 41 с.

77. Коваленко О.В. Державні механізми забезпечення кібербезпеки України в умовах євроінтеграційних та глобалізаційних викликів. *Інституціоналізація публічного управління в Україні в умовах євроінтеграційних та глобалізаціних викликів*: матеріали щорічної науково-практичної конференції за міжнародною участю (Київ, 24 травня 2019 року) / за загальною редакцією А.П.Савкова, М.М. Білинської, О.М. Петроє. Київ, НАДУ, 2019, том 3, С. 48-50.

78. Коваленко О.В. Заходи з протидії негативним інформаційним впливам на групову, масову та індивідуальну свідомість громадян України, які здійснюються російськими спецслужбами в рамках гібридної війни.

Становлення публічного адміністрування в Україні: матеріали X конференції студентів та молодих учених за міжнародною участю (м. Дніпро, 10 травня 2019 року) / за загальною редакцією О.Б. Кірєєвої. Д. : ДРІДУ НАДУ, 2019. С. 138-141.

79. Коваленко О.В. Концептуальні засади державно-управлінської діяльності у сфері забезпечення кібербезпеки України. *Україна 2030: публічне управління для сталого розвитку*: матеріали щорічній Всеукр. наук.-практ. конф. за міжнар. участю. К. : НАДУ, 2020. Том №3. С. 40-41.

80. Коваленко О.В. Концептуальні засади розвитку національної системи кібербезпеки України на сучасному етапі державного будівництва. *Державне управління: удосконалення та розвиток*. 2020. № 6. URL: http://www.dy.nayka.com.ua/?op=1&z=1694

81. Коваленко О.В. Методологічні засади формування управлінської культури кібербезпекою України. *Актуальні питання, проблеми та перспективи розвитку гуманітарного знання у сучасному інформаційному просторі: національний та інтернаціональний аспекти*: зб. наук. праць / за заг. ред. д.філос.н. Журби М.А. Монреаль: СРМ «ASF», 2020. С. 90-93.

82. Коваленко О.В. Механізми формування та реалізації державної політики у сфері інформаційної безпеки України: особливості розбудови в умовах гібридної війни та сучасний стан. *Інформаційно-психологічна протидія у ЗСУ: історія, сучасний стан та перспективи вдосконалення:* матеріали науково-практичного семінару / за ред.. В.М. Мороза. К.: НДЦГПЗСУ, 2021. С. 30-38.

83. Коваленко О.В. Розбудова системи кібербезпеки Іспанії: уроки для України. *Інвестиції: практика та досвід*. 2020. № 17–18. С. 149–153.

84. Коваленко О.В. Теоретико-методологічні засади формування механізмів забезпечення кібербезпеки України на сучасному етапі державного будівництва. *Věda a perspektivy.* 2022. №6 (13). С. 21–33.

85. Коваленко О.В. Теоретичні засади проектування системи забезпечення кібербезпеки України. *Державне управління: удосконалення та розвиток*. 2022. № 10. URL: https://www.nayka.com.ua/index.php/dy/article/view/636

86. Коваль З.В. Динаміка світової управлінської реакції на кіберзагрози: уроки для України. *Демократичне врядування*. 2014. Вип. 14 URL: http://nbuv.gov.ua/UJRN/DeVr_2014_14_5.

87. Козаков В. М. Соціально-ціннісні засади державного управління в Україні: монографія. К.: Вид-во НАДУ, 2007. 284 с.

88. Кольцов М., Аушев Є. Пропозиції до політики щодо реформування сфери кібербезпеки в Україні. URL: https://parlament.org.ua/wp-content/uploads/2017/10/Policy-Paper_Kiberbezpeka-1-1.pdf

89. Конституція України. *Урядовий кур'єр*. 1996. 13 липня. С. 1– 8.

90. Корченко О.Г., Гнатюк С.О. Актуальні проблеми забезпечення кібербезпеки цивільної авіації. *Захист інформації і безпека інформаційних систем* : матеріали II міжнар. наук.-техн. конф. Львів : Національний університет «Львівська політехніка», 2013. С. 10-12.

91. Корченко О.Г., Гнатюк С.О. Протидія кібертероризму на авіаційному транспорті. *Боротьба з Інтернет-злочинністю* : матеріали міжнар. наук.-техн. конф. Донецьк : ДЮІ МВС України, 2013. С. 85-87.

92. Костенко Д.М. Формування мережевої архітектури публічного управління в контексті забезпечення національної безпеки: дис. … докт. філософії: спец. 281 / НАДУ. К., 2021. 245 с.

93. Котух Є.В. Теоретико-методологічні засади забезпечення кібербезпеки у публічному секторі. Дисертація на здобуття наукового ступеня доктора наук з державного управління за спеціальністю 25.00.02 «Механізми державного управління». – Національний університет цивільного захисту України, Харків, 2022. 479 с.

94. Кримський С.Б. Запити філософських смислів. К.: ПАРАПАН,

2003. 240 с.

95. Лалак О.А. Виклики і ризики кібербезпеки: досвід України та Польщі. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/download/3001/2692

96. Левченко О. В. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування : монографія /О. В. Левченко. Житомир : Видавець ПП "Євро-Волинь", 2021. 172 с.

97. Леонов О. В. Інтернет як інструмент ведення кібернетичної війни. *Стратегічна панорама*. 2002. № 3. С. 122-127.

98. Литвиненко О.В. Спеціальні інформаційні операції та пропагандистські кампанії : монографія. К.: ВКФ «Сатсанта», 2000. 222 с.

99. Ліпкан В.А. Стратегія державної інфрасруктурної політики України: словник. К.: В.А. Ліпкан, 2023. 252 с.

100. Ліпкан В., Діордіца І. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. *Підприємництво, господарство і право*. 2017. № 5. С. 174-180.

101. Лопушинський І.П. «Цифровізація» як основа державного управління на шляху трансформації та реформування українського суспільства. *Теорія та практика державного управління і місцевого самоврядування.* 2018. № 2. URL: http://el-zbirn-du.at.ua/2018_2/20.pdf

102. Лук'яненко О.М. Геополітичне інформаційне протиборство: сутність і варіанти захисту. *Університетська кафедра.* 2016. № 5. С. 173-184.

103. Лук'яненко О.М. Соціальне проектування механізмів розробки та реалізації соціально-інформаційної політики України. *Sciences of Europe. Praha, Czech Republic*. 2020. Vol 4, № 52. С. 38-43.

104. Лук'яненко О.М. Актуальні проблеми формування інформаційної культури українського суспільства в інтересах забезпечення інформаційної безпеки. *Ефективність державного механізму реагування на загрози національним інтересам України в умовах євроінтеграції*: матеріали наук.-

практ. семінару (9 грудня 2015 р.). К. 2016. С. 80-85.

105. Лук'яненко О.М. Сучасні технології інформаційної агресії. *Досвід застосування збройних сил у світових війнах і воєнних конфліктах XX – початку XXI ст.: тенденції та закономірності*: Зб. наук. пр. К. 2016. Вип. 5. С. 212–216.

106. Манжай О. В. Використання кіберпростору в оперативно-розшуковій діяльності URL: file:///C:/Users/%D0%95%D0%B2%D0%B3%D0%B5%D0%BD%D0%B8%D1%8F/Downloads/Pib_2009_4_50.pdf

107. Марутян Р. Організаційна зброя у гібридній війні. *Актуальні проблеми управління інформаційною безпекою держави* : зб. тез наук. доп. наук.-практ. конф. (Київ, 04 квіт. 2019 р.). Київ : Нац. акад. СБУ, 2019. С. 89–91.

108. Марутян Р.Р. Інтелектуально-ресурсне забезпечення державного управління у сфері національної безпеки України : монографія. Київ : ЦП «Компринт», 2020. 410 с.

109. Марутян Р. Інтелектуально-кадрове лідерство у сфері національної безпеки: порівняльний аналіз американської та російської моделей аналітичних центрів. *Інвестиції: практика та досвід*. 2022. № 23. С.88-94.

110. Марутян Р.Р. Інтелектуальні ресурси державного управління у сфері національної безпеки України: дис. … док. наук з держ. упр.: спец. 25.00.01. / Марутян Рена Рубенівна. К.: НАДУ, 2020. 458 с.

111. Мельник С.В., Тихомиров О.О., Лєнков О.С. До проблеми формування понятійно-термінологічного апарату кібербезпеки *Актуальні проблеми управління інформаційною безпекою держави* : зб. матер. наук.-практ. конф., (Київ, 22 березня 2011 р.). К. : Вид-во НА СБ України, 2011. Ч. 2. С. 43-48.

112. Методи інформаційного захисту простору. Інформаційна безпека України. URL: http://www.ua. textreferat.com/referat-7471.html

113. Методичні рекомендації щодо категоризації об'єктів критичної

інфраструктури, порядку формування переліку об'єктів критичної інформаційної інфраструктури та формування державного реєстру об'єктів критичної інформаційної інфраструктури. К, 2021. 92 с.

114. Методологія державного управління як галузі науки : наук. розробка / авт. кол. : Ю. П. Сурмін, В. Д. Бакуменко, А. О. Краснейчук. К. : НАДУ, 2010. 32 с.

115. Методологія стратегічного планування в умовах глобальних загроз національній безпеці та міжнародній стабільності : монографія / авт. кол.: В.І. Абрамов, Т. В. Запорожець, Р. Р. Марутян та ін.; за заг. ред. Л. М. Шипілової. Київ: НАДУ, 2018. 232 с.

116. Михайловська О.М. Концепція громадського прогресу в науці публічне управління: монографія. Мена: Домінант, 2020. 308 с.

117. Мінін Д.С. Підходи до визначення поняття «кібербезпека» URL: http://istfak.org.ua/tendentsii-rozvytkusuchasnoi-systemy-mizhnarodnykh-vidnosyn-ta-svitovohopolitychnoho-protsesu/185-heopolitychna-dumka-taheostratehichni-protsesy-v-khkhi-st/971-pidkhody-dovyznachennya-ponyattya-kiberbezpeka.

118. Національні системи оцінювання ризиків і загроз: кращі світові практики, нові можливості для України : аналіт. доп. / [Резнікова О. О., Войтовський К. Є. Лепіхов А. В.] ; за заг. ред. О. О. Резнікової. К.: НІСД, 2020. 84 с.

119. Неклесса О. Осислюючи майбутнє. Світ як незавершений проект. Пер. з рос. М. Лаюка, К. Сінченко. К.: ДУХІ ЛІТЕРАРА, 2018. 208 с.

120. Нестеряк Ю. В. Розвиток національного інформаційного простору України (2005–2014 рр.). *Вісн. НАДУ при Президентові України. Серія «Державне управління»*. 2018. № 3. С. 181–188.

121. НІСД. Аналітичні матеріали URL: https://niss.gov.ua/analitichni-materiali

122. Нормативно-правова база в галузі безпеки і оборони України: видання друге, доповнене / А. Гриценко, М. Кожієл, А. Єрмолаєв, Ф. Флурі. К.: Центр дослідження армії, конверсії та роззброєння, 2012. 820 с.

123. Обґрунтування концептуальних та організаційно-правових засад розробки паспортів загроз національній безпеці України : навч.-метод. посіб. / [Г.П. Ситник, В.І. Абрамов, М.М. Шевченко та ін.] за заг. ред. Г.П. Ситника К.: НАДУ, 2012. 52 с.

124. Оболенський О.Ю. Публічне управління: цивілізаційний тренд, наукова теорія і напрям освіти. *Публічне управління : шляхи розвитку* : матеріали наук.-практ. конф. за міжнар. участю, м. Київ, 26 листоп. 2014 р. : у 2 т. / за наук. ред. Ю.В. Ковбасюка, С.А. Романюка, О.Ю. Оболенського. К. : НАДУ, 2014. Т. 1. С. 3-10 с.

125. Ожеван М.А., Дубов Д.В. Homo ex Machina. Філософські, культурологічні та політичні передумови формування конвергентного суспільства : монографія. К.: НІСД, 2017. 272 с.

126. Олексюк Л. Кращі практики управління кібербезпекою. Оглядовий звіт. URL: https://www.undp.org/sites/g/files/zskgke326/files/migration/ua/Report_on_Cybersecurity_04.pdf

127. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України : аналіт. доп. / [Бобро Д. Г., Іванюта С. П., Кондратов С. І., Суходоля]; за заг. ред. О.С. Суходолі. – К.: НІСД, 2019. – 224 с.

128. Орел М.Г. Теоретико-методологічні засади формування системи державного управління у сфері політичної безпеки.: автореф. дис. ... д. держ. упр. : 25.00.01 - Теорія і історія державного управління / М. Г. Орел ; Приватне акціонерне товариство «Вищий навчальний заклад "Міжрегіональна Академія управління персоналом». 2019. 37 с.

129. Орел М.Г. Теоретичні основи державного управління у сфері політичної безпеки: монографія. К.: «Поліграф плюс», 2019. 320 с.

130. Оцінювання ефективності державного механізму реагування на загрози національним інтересам України: державно-управлінський аспект : навчальний посібник / [Г.П. Ситник, В.І. Абрамов, М.М. Шевченко та ін.] за заг. ред. Г.П. Ситника та Л.М. Шипілової. К.: НАДУ, 2014. 76 с.

131. Пашорін В.І. Термінологічні та освітні аспекти кібербезпеки. *Безпека соціально-економічних процесів в кіберпросторі*: матеріали Всеукраїнської науково-практичної конференції. URL: https://knute.edu.ua/file/NjY4NQ==/250dafc576ffd3c6a92546eebacc834d.pdf

132. Перепелиця Г.М. Україна – Росія: війна в умовах існування: монографія. К.: Стилос, 2017. 880 с.

133. Петровський Д. Перша світова кібервійна. URL: https://www.unian.ua/techno/persha-svitova-kiberviyna-yak-ukrajina-boretsya-na-drugomu-fronti-11998566.html

134. Пилипчук В.Г. Проблеми дослідження новітньої історії органів безпеки та розвідки в контексті розвитку сектору безпеки України. *Стратегічні пріоритети*. 2012. №3 (24). С. 114-119.

135. Пирожков С.І., Божок Є.В., Хамітов Н.В. Національна стійкість (резильєнтність) країни: стратегія і тактика випередження гібридних загроз. URL: https://files.nas.gov.ua/PublicMessages/Documents/0/2021/09/2109021352468 23-3802.pdf

136. Питання Апарату Ради національної безпеки і оборони України. Указ Президента України № 764/2019 URL: http://www.rnbo.gov.ua/documents/519.html.

137. Питання Міністерства цифрової трансформації. Постанова Кабінету міністрів України від 18 вересня 2019 р. № 856. URL: https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text

138. Питання Національного інституту стратегічних досліджень: Указ Президента України від 7 жовтня 2019 р. №737/2019 URL: https://niss.gov.ua/pro-institut.

139. Питання Центру протидії дезінформації. Указ Президента України від 7 травня 2021 року № 187/2021. URL: https://zakon.rada.gov.ua/laws/show/187/2021#Text

140. Почепцов Г. Віртуальні революції: використання віртуальних об'єктів при зміні влади. *Політичний менеджмент*. 2004. № 4. С. 3-16.

141. Про державну службу конфіденційного зв'язку і захисту інформації України. Закон України від 23.02.2006 р. № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15

142. Про Інформаційно-аналітичний центр. Указ Президента України № 398/2014 від 12 квітня 2014 року. URL: http://www.rnbo.gov.ua/documents/345.html

143. Про інформацію : Закон України від 02 жовтня 1992 р. № 2657–XII. URL: http://zakon3.rada.gov.ua/laws/show/2657-12

144. Про Кабінет Міністрів України: Закон України від 27.02.2014 № 794-VII (із змінами). *Відомості Верховної Ради України*. 2014. № 13. Ст. 222. URL: http://zakon2.rada.gov.ua/laws/show/794-18

145. Про національну безпеку України. Закон України від 21 червня 2018 року № 2469-VIII. URL: http://zakon5.rada.gov.ua/laws/show/2469-19

146. Про Національну гвардію України: Закон України від 12 липня 2018 р. *Відомості Верховної Ради України*. 2014. № 17. ст.594.

147. Про національну поліцію: Закон України від 2 липня 2015 р. *Відомості Верховної Ради України*. 2015. № 40-41. ст. 379.

148. Про національну програму інформатизації. Закон України. URL: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80#Text

149. Про основні засади забезпечення кібербезпеки України. Закон України від 5 жовтня 2017 року № 2163-VIII. *Відомості Верховної Ради*. 2017. № 45. Ст.403.

150. Про радіочастотний ресурс. Закон України URL: https://zakon.rada.gov.ua/laws/show/1770-14

151. Про Раду національної безпеки і оборони України. Закон України від 5.03.1998 р. № 183/98-ВР (зі змінами і доп.). *Відомості Верховної Ради (ВВР)*. 1998. № 35. Ст. 237.

152. Про рішення Ради національної безпеки і оборони України «Про Стратегію інформаційної безпеки України»: Указ Президента України від 28 грудня 2021 року № 685/2021. URL: https://www.rnbo.gov.ua/ua/Ukazy/5203.html

153. Про рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України»: Указ Президента України від 14 вересня 2020 року № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037

154. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». Указ Президента України № 96/2016 URL : https://www.president.gov.ua/documents/962016-19836.

155. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України. Указ Президента України № 47/2017 URL : https://www.president.gov.ua/documents/472017-21374.

156. Про рішення Ради національної безпеки і оборони України Указ Президента України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» від 01 травня 2014 року № 449/2014 URL: http://zakon3.rada.gov.ua/laws/show/449/2014.

157. Про рішення Ради національної безпеки і оборони України. Указ Президента України від 04.03.2016 р. № 92/2016 «Про Концепцію розвитку сектору безпеки і оборони України» URL: https://zakon.rada.gov.ua/laws/show/92/2016.

158. Про рішення Ради національної безпеки і оборони України: Указ Президента України №473/2021 від 20 серпня 2021 року «Про Стратегічний оборонний бюлетень України». URL: https://www.president.gov.ua/documents/4732021-40121

159. Про рішення Ради національної безпеки і оборони України: Указ Президента України від 20 серпня 2021 року № 479/2021 «Про запровадження національної системи стійкості». URL : https://www.president.gov.ua/documents/4792021-40181

160. Про рішення Ради національної безпеки і оборони України: Указ Президента України від 7 червня 2016 року № 242/2016 «Про Національний координаційний центр кібербезпеки». URL : https://zakon.rada.gov.ua/laws/show/242/2016#n9

161. Про рішення Ради національної безпеки і оборони України: Указ Президента України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки». URL : https://www.president.gov.ua/documents/562022-41377

162. Про розвідку. Закон України від 17.09.2020 року № 912-IX URL: https://zakon.rada.gov.ua/laws/show/912-20#Text

163. Про Службу безпеки України. Закон України. 25.03.1992 р. № 2229-XII. URL:https://zakon.rada.gov.ua/laws/show/2229-12

164. Про створення та забезпечення діяльності Головного ситуаційного центру України: Указ Президента України № 115/2015 від 28.02.2015. URL: http://zakon4.rada.gov.ua/laws/show/n0002525-15

165. Про Стратегію комунікації з питань євроатлантичної інтеграції України на період до 2025 року. Указ Президента України від 11 серпня 2021 року № 348/2021. URL: https://www.president.gov.ua/documents/3482021-39617

166. Проведено перший у світі навчальний курс щодо захисту цивільної авіації від кіберзагроз. URL: http://bit.nau.edu.ua/news.php?page=62

167. Публічне управління : термінол. слов. / уклад. : В. С. Куйбіда, М. М. Білинська, О. М. Петров та ін. ; за заг. ред. В. С. Куйбіди, М. М. Білинської, О. М. Петроє. К. : НАДУ, 2018. 224 с.

168. Публічне управління та адміністрування : словник-довідник / уклад. О.М. Руденко, О.В. Шершньова, В.Д. Бакуменко, Н.В. Філіпова, Н.В. Ткаленко; за заг. ред. О.М. Руденко. К.: Кондор-Видавництво, 2016. 178 с.

169. Публічне управління та адміністрування у сфері національної безпеки (системні, політичні та економічні аспекти): словник-довідник / уклад.: С.П. Завгородня, М.Г. Орел, Г.П. Ситник та ін.; за заг. ред. Д.В. Неліпи, Є.О. Романенка, Г.П. Ситника. К.: Видавець Кравченко. 2020. 380 с.

170. Публічне управління XXI століття: в умовах гібридних загроз : зб. наук. матер. XXII Міжнар. наук. конгресу. Х. : ННІ "Інститут державного управління" Харківського національного університету імені В.Н. Каразіна, 2022. 304 с.

171. Размєтаєва Ю. С. Кібервійна: загальнотеоретичні аспекти. *Вісник Академії митної служби України*. Серія : Право. 2015. № 1. С. 12-22. URL: http://nbuv.gov.ua/UJRN/vamsup_2015_1_4

172. Рачинський А. П. Розвиток системи забезпечення державної безпеки України: теоретико-методологічні проблеми та шляхи їх розв'язання. *Інвестиції: практика і досвід*. 2022. № 23. С. 95-101.

173. Резнікова О. Концептуальні засади національної стійкості. *Держава і право*: зб. наук. праць. Серія Політичні науки. Вип. 81. Київ: Вид-во «Юридична думка», 2018. С.135–146.

174. Розбудова безпеки і оборони: зб. матеріалів щодо Плану партнерських дій із створення інститутів оборони і безпеки (PAP-DIB) / за ред. Філліпа Х. Флурі, Віллема Ф. ван Їкелена; пер. з англ. О. Михалочко, К. Гломодзи. Женева; Київ, 2006. 383 с.

175. Роль інформаційних інфраструктур у забезпеченні цифрового

суверенітету. URL: https://ndipzir.org.ua/wp-content/uploads/2021/Tsyfrovizatsiya21/Part_4.pdf

176. Руденко О. Забезпечення державної безпеки України в системі захисту національних інтересів: *зб. наук. пр. Донецьк. держ. ун-ту упр. Серія «Державне управління».* 2019. Т. ХХ. Вип. 312. С. 42–50.

177. Савранська Г. М. Державне управління соціальним партнерством в контексті забезпечення соціальної безпеки України: автореф. дис. ... канд. наук з держ. упр.: 25.00.01 / НАДУ. Київ, 2018. 20 с.

178. Світова гібридна війна: український фронт : монографія / за заг. ред. В.П. Горбуліна. К.: НІСД, 2017. 496 с.

179. Севастьянов А.К. Международные стандарты систем менеджмента для решения проблем безопасности и устойчивого развития (International standards for management systems for solving the security and sustainable development). *Стандартизація, сертифікація, якість*. 2012. №4. С.41-49.

180. Севастьянов А.К. Анализ стандартов систем менеджмента информационной безопасностью: состояние и перспективы развития. Девятая дистанционная научно-практическая конференция с международным участием «*Системы поддержки принятия решений. Теория и практика. СППР 2013*». – Киев: Академия технологических наук Украины, Институт проблем математических машин и систем НАН Украины. 2013. С. 89-92. URL: http://conf.atsukr.org.ua/files/conf_dir_23/Sevastjianov_sppr2013.pdf

181. Семенченко А.І. Методологія стратегічного планування у сфері державного управління забезпеченням національної безпеки України: монографія. К.: НАДУ, 2008. 428 с.

182. Семенченко А.І. Стратегічне планування у сфері державного управління національною безпекою: автореф. дис. ... док. наук з держ. упр.: 25.002. Механізми державного управління / НАДУ. Київ, 2008. 36 с.

183. Семенченко А.І., Дубов Д.В., Олексюк Л.В. Потій О.В.,

Експертна Рада інформаційної та кібербезпеки як демократичний інноваційний інструмент державно-приватної взаємодії. *Науковий вісник: Державне управління*. № 2 (8). 2021. С.102-121.

184. Семенченко А.І., Потій О.В., Бакалинський О.О., Мялковський Д.В. Публічне управління інституціональним розвитком у сфері кіберзахисту в умовах трансформаційних змін сектору безпеки і оборони. *Науковий вісник: Державне управління*. № 3 (9).- 2021.С.136-162.

185. Семенченко А.І., Потій О.В., Дубов Д.В., Бакалинський О.О., Мялковський Д.В. Концептуальні засади впровадження організаційно-технічної моделі кіберзахисту України. *Захист інформації*. Том 23, № 1. 2021. С.47-59. DOI:10.18372 / 2410-7840.23.15434

186. Семенченко А.І. Розвиток інструментів державно-приватної взаємодії у сфері кібербезпеки. Основи воєнно-теоретичних досліджень: нові реалії та технології: моногр. в 4 томах. Том 1: Дослідження проблем національної безпеки держави / І.С. Романченко, В.Ю. Богданович, О.А. Ільяшов, В.С. Комаров, О.І. Соломицькій, Б.Л. Бутвін, В.М. Муженко, О.М. Семененко, М.О. Слюсаренко, А.І. Семенченко / за заг. ред. професора Романченка І.С. Київ: ЦНДІ ЗСУ України; НУЩ України, 2022. С. 225-237.

187. Семенченко А.І., Олексюк Л.В. Україна на шляху до європейського цифрового ринку: стан та інструменти впровадження європейського індексу цифрової економіки та суспільства в Україні. *Актуальні проблеми державного управління : зб. наук. праць*. Харків : ХНУ імені В. Н. Каразіна. 2022. № 2 (61). С. 129-144.

188. Семенченко А.І., Жиляєв І.Б. Організаційно-правові механізми розвитку національної системи кібербезпеки України: стан та перспективи. *Стратегічні пріоритети*. 2017. № 4. С. 55-63.

189. Семенченко А., Мялковський Д. Розвиток інституційних спроможностей суб'єктів забезпечення системи кібербезпеки та кіберзахисту України. *Theory and Practice of Public Administration*. 2020.

Том. 3. № 70. С. 40-54.

190. Семенченко А.І., Мялковський Д.В., Станіславський Т.В. Концептуальні засади огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури. *Стратегічні пріоритети*. 2018. № 3-4. С. 36-45.

191. Сенченко О. М. Інформаційно-мережеві війни: теорія, моделі, алгоритми. Київ: КВІЦ, 2017. 332 с.

192. Ситник Г. П. Сутність кризових ситуацій соціального характеру у контексті національної безпеки: філософсько-управлінський аспект. *Державне управління: удосконалення та розвиток*. URL: http://www.dy.nayka.com.ua/?op=1&z=1479.

193. Ситник Г.П. Державне управління національною безпекою України: монографія. К.: Вид-во НАДУ, 2004. 408 с.

194. Ситник Г.П. Концептуалізація "інформаційної безпеки" у контексті властивостей інформації як специфічної субстанції. *Державне управління: удосконалення та розвиток.* 2020. № 3. С. 113-121.

195. Ситник Г.П. Інформаційна компонента критичних (надзвичайних) ситуацій у контексті забезпечення державної безпеки. *Науковий вісник: Державне управління*. 2020. № 2(4). С. 327-339.

196. Ситник Г. П., Орел М. Г. Концептуальні засади диференціації типів дестабілізації суспільно-політичної системи та її аналізу у контексті забезпечення національної безпеки. Науково-інформаційний вісник Академії національної безпеки. 2016. № 3-4. С. 8-31.

197. Ситуативні центри органів державної влади : наук. розробка / авт. кол. : А. І. Семенченко, І. В. Клименко, А. В. Журавльов та ін. ; за заг. ред. д-ра наук держ. упр., проф. А. І. Семенченка. К. : НАДУ, 2013. 60 с.

198. Соколов В.А. Інституалізація аналітичної діяльності в системі забезпечення національної безпеки: зарубіжний та вітчизняний досвід: монографія. К. : НАДУ, 2021. 375 с.

199. Соколов В.А., Шевченко М.М. Методологічні підходи до оцінювання ефективності функціонування державного механізму інформаційно-аналітичного забезпечення політики національної безпеки. *Інвестиції: практика та досвід*. 2020. № 1. С. 148-154.

200. Солодка О.М. Забезпечення інформаційного суверенітету держави: правовий дискурс. *Інформація і право*. 2020. № 1 (32) С. 80-87.

201. Спільна робота для колективної безпеки – основна ціль співпраці між Держспецзв'язку та Іспанським національним інститутом кібербезпеки. URL: https://cip.gov.ua/ua/news/collaboration-for-collective-security-is-the-major-goal-of-cooperation-between-the-ssscip-and-the-spanish-national-cybersecurity-institute

202. Сторінки громадських рад на сайтах органів виконавчої влади. URL: https://www.kmu.gov.ua/gromadskosti/gromadyanske-suspilstvo-i-vlada/gromadski-radi/storinki-gromadskih-rad-na-sajtah-organiv-vikonavchoyi-vladi

203. Стратегічне управління військово-технічним співробітництвом в інтересах забезпечення воєнної безпеки України: монографія / кол. авторів: Бегма В.М., Загорка О.М., Косевцов В.О., Шемаєв В.М.; за заг. ред. Руснака І.С. К.: ІПНБ, НАОУ, 2005. 228 с.

204. Стратегічні комунікації для безпекових і державних інституцій : практичний посібник / [Л. Компанцева, О. Заруба, С. Череватий, О. Акульшин; за заг. ред. О. Давліканової, Л. Компанцевої]. – Київ: ТОВ «ВІСТКА», 2022. – 278 с.

205. Сурмин Ю. П. Социальное проектирование в кризисном обществе: методологический аспект. *Вісн. Нац. акад. держ. упр. при Президентові України*. 2014. № 3. С. 5–17.

206. Сурмін Ю.П. Проблеми та напрями змін державного управління в Україні в сучасних умовах. *Публічне управління : шляхи розвитку* : матеріали наук.-практ. конф. за міжнар. участю, м. Київ, 26 листоп. 2014 р. : у 2 т. / за наук. ред. Ю.В. Ковбасюка, С.А. Романюка,

О.Ю. Оболенського. К. : НАДУ, 2014. Т. 1. С. 10-13.

207. Таран Є.І. Поняття «національна безпека» у системі публічного управління. *Публічне управління і адміністрування в Україні*. № 28, 2022. С. *182-185.*

208. Твердохліб О.С. Формування та реалізація інформаційної політики держави в умовах новітніх загроз і викликів : монографія. Київ : ІДУ НД ЦЗ, 2022. 264 с.

209. Твердохліб О.С., Гайович Г.В. Історіографічна та джерелознавча проблематика інформаційних війн у контексті загроз і викликів для державотворчих процесів сучасної України. *Теорія та практика державного управління*. 2021. Вип. 1 (72). С. 31–39.

210. Теоретичні основи побудови та функціонування систем управління інцидентами інформаційної безпеки / Гнатюк С.О., Хохлачова Ю.Є., Охріменко А.О., Гребенькова А.К. *Захист інформації.* №1 (54). 2012. С. 121-126.

211. Теоретичні та методологічні проблеми розробки і реалізації управлінських стратегій: монографія / за заг. ред. В. М. Князєва. К.: НАДУ, 2008. 240 с.

212. Теоретико-методологічні засади формування кадрової безпеки в системі публічного управління: кол. монографія / С. О. Борисевич, В. І. Абрамов, В. Ф. Смолянюк, М. М. Шевченко; за ред. С.О. Борисевича. Київ: НАДУ, 2018. 304 с.

213. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони № 984_011. URL: http://zakon4.rada.gov.ua/laws/show/984_011/page

214. Управління та адміністрування в умовах протидії гібридним загрозам національній безпеці: Матеріали ІІ Міжнародної науково-практичної конференції (м. Київ, 7 грудня 2021 року). К.: ДУІТ, ХНУРЕ. 2021. 694 с.

215. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*. 2012. № 2. С. 162-169.

216. Хмель А., Біляєв Д. Порівняння кіберможливостей Іспанії та Італії на сучасному етапі. URL: https://eppd13.cz/wp-content/uploads/2018/2018-5-2/12.pdf

217. Центр Стратегічних комунікацій та інформаційної безпеки при Міністерстві культури та інформаційної політики. URL: https://mkip.gov.ua/content/centr-strategichnih-komunikaciy-ta-informaciynoi-bezpeki-pri-ministerstvi-kulturi-ta-informaciynoi-politiki.html

218. Чигринський В. А. Політико-правове проектування та державне конструювання системи забезпечення національної безпеки Іспанії: уроки для України. *Державне управління: удосконалення та розвиток*. 2020. № 6. URL: http://www.dy.nayka.com.ua/?op=1&z=1692

219. Шевченко М. М. Методологія компаративного аналізу систем забезпечення національної безпеки. *Збірник наукових праць Національної академії державного управління при Президентові України* / за заг. ред. Ю.В. Ковбасюка. К.: НАДУ, 2015. Вип. 1. С. 5–16.

220. Шевченко М.М., Кочерга Д.А. Кризи, що загрожують національній безпеці України та національна рамка реагування на них. *Досвід застосування збройних сил у світових війнах і воєнних конфліктах XX – початку XXI ст.: тенденції та закономірності*: матеріали міжвузівського науково-практичного семінару (Київ, 25 травня 2023 р.). Київ: ЦП «Компринт», 2023. Вип. 12. С. 284-310.

221. Шевченко М.М. Державна політика національної безпеки України та механізми її реалізації. *Національні інтереси України: ступінь реалізації та загрози*: матеріали круглого столу, м. Київ, 27 листопада 2013 р.: у 2 частинах / за ред. Г.П. Ситника, Л.М. Шипілової. К.: НАДУ, 2013. Ч.2. С. 38-47.

222. Шевченко М.М. Перемога у війнах постіндустріальної епохи:

нові контексти та інтерпретації. *Гілея: науковий вісник*: зб. наук. пр. 2018. Вип. 130 (3). С. 321-325.

223. Шевченко М.М. Поняття «технологія державного реагування на загрози національній безпеці»: смисловий простір соціально-філософського змісту. *Філософія науки: традиції та інновації*. 2017. № 2 (16). С. 183-196.

224. Шевченко М.М. Філософсько-методологічні основи визначення принципів інформаційно-пропагандистського забезпечення в збройних силах. *Схід*. 2016. № 5 (145). С. 114-120.

225. Шевченко М.М. Функції та завдання системи забезпечення національної безпеки. *Науково-інформаційний вісник Академії національної безпеки*. 2014. № 3-4. С. 14-24.

226. Шеломенцев В.П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2012. Вип. 1. С. 312–320.

227. Шеломенцев В.П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2012. № 2 (28). С. 299–309.

228. Шипілова L.., Онешко S.., Іванова V.., Таран Y.., & Суліма N. (2022). СТРАТЕГІЇ ТА ІННОВАЦІЇ В УПРАВЛІННІ ЕКОНОМІЧНИМИ СИСТЕМАМИ: УКРАЇНСЬКИЙ ДОСВІД, ВІДПОВІДІ НА СУЧАСНІ ВИКЛИКИ. *Financial and Credit Activity Problems of Theory and Practice*, *4*(45), 425–436. https://doi.org/10.55643/fcaptp.4.45.2022.3835 ***(WoC)***

229. Шмидт Э., Коэн Дж. Новый цифровой мир. Как технологии меняют жизнь людей, модели бизнеса и понятие государства / пер. с англ. С. Филина. Москва: Манн, Иванов и Фербер, 2013. 368 с.

230. Шляхи удосконалення системи державного управління

забезпеченням національної безпеки України : монографія / [кол. авт.: Г.П. Ситник, В.І. Абрамов, О.Г. Бортнікова, Д.Я. Кучма, М.М. Шевченко та ін.]; за ред. Г.П. Ситника, В.І. Абрамова. К.: МАЙСТЕР КНИГ, 2012. 536 с.

231. Шпанчук В.В. Державне управління кібербезпекою України: правовий аспект/ URL: http://www.dy.nayka.com.ua/pdf/11_2018/6.pdf

232. Юськів К. Триває перша у світі кібервійна - голова Мінцифри. URL: https://ua.korrespondent.net/ukraine/4561820-tryvaie-persha-u-sviti-kiberviina-holova-mintsyfry

233. Canada's Cyber Security Strategy. URL: http://publications.gc.ca/site /eng/379746/publication.html

234. Centro Superior de Estudios de la Defensa Nacional URL: http://www.defensa.gob.es/ceseden/

235. Constitución de España de 1978. URL: www.congreso.es/consti/

236. Cyber Security Strategy – A world-leading, resilient and vigorous cyberspace. URL : http://www.nisc.go.jp/eng/pdf/ CyberSecurityStrategy.pdf

237. Cyber Security Strategy for Germany URL : http://www.enisa. europa.eu/media/news-items/german-cyber-security-strategy-2011-1

238. Cyber Security Strategy of the Czech Republic for the 2011 – 2015 period. URL : http://www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_20112015.PDF

239. Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space. URL : // http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf

240. Cyber Security Strategy URL: http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf

241. Estrategia de Ciberseguridad Nacional. URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ES_NCSS.pdf

242. Estrategia de Seguridad Nacional. URL:

www.lamoncloa.gob.es/NR/rdonlyres/OBB61AA9

243. Executive Order - Improving Critical Infrastructure Cybersecurity // URL: http://www.whitehouse.gov/the-press-office/2013/02/12/ executive-order-improving-critical-infrastructure-cybersecurity

244. Government Resolution on National Information Security Strategy URL: http://www.lvm.fi/c/document_library/ get_file?folderId=57092&name=DLFE-5405.pdf&title= Valtioneuvoston%20 periaatep%C3%A4%C3%A4t%C3% B6s%20kansalliseksi%20tietoturvastra

245. Information Security Research and Development Strategy. URL : http://www.nisc.go.jp/eng/pdf/R_and_D_Strategy_eng.pdf

246. Instituto Español de Estudios Estratégicos URL: http://www.ieee.es/

247. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. URL : http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_ for_cyber space.pdf

248. ISO/IEC 27032, Information technology – Security techniques – Guidelines for cybersecurity. 2012. 50 p.

249. IT Emergency and Crisis Exercises in Critical Infrastructures. URL: http://www.bmi.bund.de/cae/servlet/contentblob/560098/publicationFile/27811/ kritis_3_eng.pdf

250. Ley 11/2002, de 6 de mayo reguladora del Centro Nacional de Inteligencia URL: http://www.cni.es/comun/recursos/descargas/LEY_11-2002_de_6_de_mayo_.pdf

251. National Strategy to Secure Cyberspace. URL : http://www.dhs.gov/ national-strategy-secure-cyberspace

252. On the approval of the programme for the development of electronic information security (cyber-security) for 2011–2019 URL :http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06 29_EN_PATAIS.pdf

253. Presidential Policy Directive - Critical Infrastructure Security and Resilience URL: http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

254. Strategie de la France: Défense et sécurité des systèmes d'information URL : http://www.enisa.europa.eu/media/news-items/ french-cyber-security-strategy-2011

255. Strategie nationale en matiere de cyber securite URL : Ukrainian Scientific Journal of Information Security, 2013, vol. 19, issue 2-129 http://www.gouvernement.lu/salle_presse/actualite/2011/11-novembre/23-biltgen/dossier.pdf

256. The National Cyber Security Strategy (NCSS): Success through cooperation. URL : http://www.enisa.europa.eu/ media/news-items/dutch-cyber-security-strategy-2011

257. Taran Y, Sytnyk H., Orel M., Ivanova V. & Conceptual understanding of the relationship between political and administrative processes in the context of social systems security. CUESTIONES POLITICAS. Vol. 40, Nº 74 (2022). DOI: https://doi.org/10.46398/cuestpol.4074.34 **(**WoC**)**

258. Taran Ye. State policy of providing information security for the leading world countries // Studia Społeczne | Social Studies – 2020. - № 1. – p. 73-80.

259. Taran, Y. (2022). Evolution of the world order system. Baltic Journal of Legal and Social Sciences, (2), 206-211. https://doi.org/10.30525/2592-8813-2022-2-34

260. Zaporozhets T. Genesis of the information space: from information security to cybersecurity in a digital society. Cybersecurity and Law, 2021. № 5(1). p. 25-30. http://www.cybersecurityandlaw.com/Genesis-of-the-information-space-from-information-security-to-cybersecurity-in-a,142177,0,2.html

ДОДАТКИ

Додаток А

МІНІСТЕРСТВО ОБОРОНИ
УКРАЇНИ
УПРАВЛІННЯ
РОЗВИТКУ АВТОМАТИЗАЦІЇ
АПАРАТУ ГОЛОВНОКОМАНДУВАЧА
ЗБРОЙНИХ СИЛ УКРАЇНИ
Код 26622199
«09» 11 2020 р.
№ 364/1/1998
04119, м. Київ, вул. Дегтярівська, 13/24

ДОВІДКА ПРО ВПРОВАДЖЕННЯ

Результати дисертаційного дослідження аспіранта кафедри глобалістики, євроінтеграції та управління національною безпекою Національної академії державного управління при Президентові України Коваленка Олександра Валентиновича на тему: «Державні механізми забезпечення кібербезпеки України», на здобуття наукового ступеня доктора філософії за спеціальністю 281 «Публічне управління та адміністрування» впроваджені в діяльності Управління розвитку автоматизації Апарату Головнокомандувача Збройних Сил України.

Зокрема, під час підготовки пропозицій з питань визначення шляхів підвищення рівня кібербезпеки України та протидії впливу іноземних держав в ІТ сфері використано аналітичні матеріали щодо оцінки можливостей запровадження в практику державного управління національною безпекою України зарубіжного досвіду щодо забезпечення кібербезпеки Іспанії.

Начальник Управління розвитку автоматизації
Апарату Головнокомандувача Збройних Сил України
полковник Олександр ЖИТНИК

Прим. № 1

ДОВІДКА ПРО ВПРОВАДЖЕННЯ
РЕЗУЛЬТАТІВ ДИСЕРТАЦІЙНОГО ДОСЛІДЖЕННЯ
КОВАЛЕНКА Олександра Валентиновича

Результати дисертаційного дослідження аспіранта кафедри глобалістики, євроінтеграції та управління національною безпекою Національної академії державного управління при Президентові України Коваленка Олександра Валентиновича на тему: «Державні механізми забезпечення кібербезпеки України», на здобуття наукового ступеня доктора філософії за спеціальністю 281 «Публічне управління та адміністрування» впроваджені в діяльності Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України.

Зокрема, під час підготовки пропозицій з питань визначення шляхів підвищення рівня кібербезпеки України та протидії впливу іноземних держав у ІТ сфері використано аналітичні матеріали щодо:

- паспортизації загроз кібербезпеці національних інформаційно-телекомунікаційних систем;
- технологізації державного реагування на загрози кібербезпеці;
- обґрунтування внесення змін до Закону України «Про санкції»;
- доцільності запровадження Єдиного реєстру програмного забезпечення, дозволеного для використання в державних інформаційно-телекомунікаційних системах та ЕОМ.

Заступник начальника Департаменту
контррозвідувального захисту інтересів
держави у сфері інформаційної безпеки
Служби безпеки України **Євген СУДАКОВ**

« 8 » липня 2020 року

Реєстраційний №30/3/3-6537

З А Т В Е Р Д Ж У Ю
Заступник Секретаря
Ради національної безпеки і
оборони України, кандидат
юридичних наук, доцент
С.В. ДЕМЕДЮК

«03» березня 2021 року

А К Т
упровадження результатів дисертаційного дослідження
КОВАЛЕНКА Олександра Валентиновича

Комісія у складі: голова комісії – керівник служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України Ткачук Н.А., члени комісії: заступник керівника служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України Звєрєв В.П., державний експерт служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України Котелянець О.О., – склала цей акт про впровадження пропозицій, підготовлених здобувачем наукового ступеня доктора філософії за спеціальністю 281 – публічне управління та адміністрування – в Національній академії державного управління при Президентові України, та викладених у дисертації «Державні механізми забезпечення кібербезпеки України».

Окремі результати дисертаційного дослідження Коваленка О.В. були використані під час підготовки пропозицій з питань визначення організаційно-технічної структури Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України. Зокрема, були використані аналітичні матеріали автора щодо оцінки можливостей запровадження в практику державного управління кібербезпекою України зарубіжного досвіду організації діяльності ситуаційних центрів в системах забезпечення національної безпеки США, ФРН, Італії. Також наукові напрацювання Коваленка О.В. знайшли своє відображення у матеріалах до засідань Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України у частині вдосконалення механізмів реалізації кібербезпеки держави.

Вважаємо, що ключові положення дисертаційного дослідження Коваленка Олександра Валентиновича на здобуття наукового ступеня доктора філософії мають достатній теоретичний та методологічний рівень, практичне значення та характеризуються науковою новизною.

Голова комісії, керівник служби з питань
Інформаційної та кібербезпеки РНБО України
кандидат юридичних наук **Н.А. ТКАЧУК**

Члени комісії:
заступник керівника служби
з питань інформаційної безпеки та кібербезпеки
Апарату РНБО України,
кандидат технічних наук,
старший науковий співробітник **В.П. ЗВЄРЄВ**

державний експерт служби
з питань інформаційної безпеки та кібербезпеки
Апарату РНБО України,
кандидат політичних наук **О.О. КОТЕЛЯНЕЦЬ**

«03» березня 2021 р.

Підпис Н.А. Ткачук, В.П. Звєрєва, О.О. Котелянець засвідчую
Державний експерт служби управління
персоналом Апарату Ради національної
безпеки і оборони України
03 березня 2021 р.

№ 1430/16-07/2-21
від 03.03.2021

ГОЛОВНЕ УПРАВЛІННЯ РОЗВІДКИ
МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ
ВОЄННО-ДИПЛОМАТИЧНА АКАДЕМІЯ
ІМЕНІ ЄВГЕНІЯ БЕРЕЗНЯКА
Код 14303342
«26» 12 2022 р.
№ 222/ВА/1043ВС
04050, м. Київ

ЗАТВЕРДЖУЮ
Начальник Воєнно-дипломатичної академії імені Євгенія Березняка
генерал-майор Павло КРИСЯК

АКТ

про впровадження результатів дисертаційного дослідження аспіранта кафедри глобальної та національної безпеки Навчально-наукового інституту публічного управління та державної служби Київського національного університету імені Тараса Шевченка Коваленка Олександра Валентиновича на тему: «Державні механізми забезпечення кібербезпеки України» на здобуття наукового ступеня доктора філософії за спеціальністю 281 «Публічне управління та адміністрування».

Комісія у складі:

голови комісії – заступника начальника Воєнно-дипломатичної академії імені Євгенія Березняка з навчальної роботи Хамули С.В., кандидата технічних наук, доцента;

членів комісії: начальника четвертої кафедри Воєнно-дипломатичної академії імені Євгенія Березняка Аблазова І.В. кандидата політичних наук, доцента; доцента четвертої кафедри Воєнно-дипломатичної академії імені Євгенія Березняка Олешка О.А., кандидата політичних наук, доцента; доцента четвертої кафедри Воєнно-дипломатичної академії імені Євгенія Березняка Рубель К.В., кандидата історичних наук, доцента, склали цей акт про те, що результати дисертаційного дослідження аспіранта кафедри глобальної та національної безпеки Навчально-наукового інституту публічного управління та державної служби Київського національного університету імені Тараса Шевченка Коваленка Олександра Валентиновича на тему: «Державні механізми забезпечення кібербезпеки України» були впроваджені у навчальний процес четвертою кафедрою Воєнно-дипломатичної академії імені Євгенія Березняка при підготовці лекційного курсу з навчальної дисципліни «Національна безпека», де використано матеріали та результати дисертаційного дослідження О.В. Коваленка щодо актуальних загроз кібербезпеці України, а також рекомендації аспіранта щодо реагування на загрози кібербезпеці України.

Голова комісії: полковник, к.т.н., доцент Сергій ХАМУЛА

Члени комісії: полковник, к.політ.н., доцент Іван АБЛАЗОВ

полковник ,к.політ.н., доцент Олег ОЛЕШКО

к.іст.н., доцент Каріна РУБЕЛЬ

Додаток Б

Список публікацій здобувача

Праці, які відображають основні наукові результати дисертації

1. Коваленко О.В. Концептуальні засади розвитку національної системи кібербезпеки України на сучасному етапі державного будівництва. Державне управління: удосконалення та розвиток. 2020. № 6. URL: http://www.dy.nayka.com.ua/?op=1&z=1694 (дата звернення: 15.06.2022). DOI: 10.32702/2307-2156-2020.6.102

2. Коваленко О.В. Розбудова системи кібербезпеки Іспанії: уроки для України. *Інвестиції: практика та досвід*. 2020. № 17–18. С. 149–153.

3. Коваленко О.В. Теоретико-методологічні засади формування механізмів забезпечення кібербезпеки України на сучасному етапі державного будівництва. *Věda a perspektivy.* 2022. №6 (13). С. 21–33.

4. Коваленко О.В. Теоретичні засади проектування системи забезпечення кібербезпеки України. Державне управління: удосконалення та розвиток. 2022. № 10. URL: https://www.nayka.com.ua/index.php/dy/article/view/636 (дата звернення: 28.10.2022). DOI: 0.32702/2307-2156.2022.10.12

Праці, які додатково відображають наукові результати дисертації

1. Коваленко О.В. Заходи з протидії негативним інформаційним впливам на групову, масову та індивідуальну свідомість громадян України, які здійснюються російськими спецслужбами в рамках гібридної війни. Становлення публічного адміністрування в Україні: матеріали X конференції студентів та молодих учених за міжнародною участю (м. Дніпро, 10 травня 2019 року) / за загальною редакцією О.Б. Кірєєвої. Д.: ДРІДУ НАДУ, 2019. С. 138-141.

2. Коваленко О.В. Державні механізми забезпечення кібербезпеки України в умовах євроінтеграційних та глобалізаційних викликів. *Інституціоналізація публічного управління в Україні в умовах*

євроінтеграційних та глобалізаційних викликів: матеріали щорічної науково-практичної конференції за міжнародною участю (Київ, 24 травня 2019 року) / за загальною редакцією А.П.Савкова, М.М. Білинської, О.М. Петроє. Київ, НАДУ, 2019, том 3, С. 48-50.

3. Коваленко О.В. Концептуальні засади державно-управлінської діяльності у сфері забезпечення кібербезпеки України. *Україна 2030: публічне управління для сталого розвитку*: матеріали щорічній Всеукр. наук.-практ. конф. за міжнар. участю. К. : НАДУ, 2020. Том №3. С. 40-41.

4. Коваленко О.В. Методологічні засади формування управлінської культури кібербезпекою України. *Актуальні питання, проблеми та перспективи розвитку гуманітарного знання у сучасному інформаційному просторі: національний та інтернаціональний аспекти*: зб. наук. праць / за заг. ред. д.філос.н. Журби М.А. – Монреаль: CPM «ASF», 2020. С. 90-93.

Праці, опубліковані в інших виданнях

1. Коваленко О.В. Механізми формування та реалізації державної політики у сфері інформаційної безпеки України: особливості розбудови в умовах гібридної війни та сучасний стан. *Інформаційно-психологічна протидія у ЗСУ: історія, сучасний стан та перспективи вдосконалення:* матеріали науково-практичного семінару / за ред.. В.М. Мороза. К.: НДЦГПЗСУ, 2021. С. 30-38.

Додаток В

Апробація результатів дисертації

Основні положення роботи викладено та обговорено на наукових та науково-практичних конференціях різного рівня, науково-практичних та науково-методичних семінарах:

1. X конференція студентів та молодих учених за міжнародною участю «Становлення публічного адміністрування в Україні» (м. Дніпро, 2019 р., форма участі – публікація тез);

2. Щорічна науково-практична конференція за міжнародною участю «Інституціоналізація публічного управління в Україні в умовах євроінтеграційних та глобалізаціних викликів» (Київ, 24 травня 2019 р., форма участі – усна доповідь);

3. Щорічна Всеукр. наук.-практ. конф. за міжнар. участю «Україна 2030: публічне управління для сталого розвитку» (Київ, 2020 р., форма участі – усна доповідь);

4. Міжнародна науково-практична конференція «Актуальні питання, проблеми та перспективи розвитку гуманітарного знання у сучасному інформаційному просторі: національний та інтернаціональний аспекти» (Монреаль, 2020 р., форма участі – публікація тез);

5. Міжнародна науково-практична конференція «Реалії та перспективи розвитку суспільства: соціальні, психологічні і політичні аспекти» (Сладковічево, 2016 р., форма участі – публікація тез);

6. Науково-практичного семінару «Інформаційно-психологічна протидія у ЗСУ: історія, сучасний стан та перспективи вдосконалення» (Київ, 2011 р., форма участі – публікація тез).