НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПУБЛІЧНОГО ПРАВА
НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПУБЛІЧНОГО ПРАВА

Кваліфікаційна наукова
праця на правах рукопису

МОНАСТИРЕЦЬКИЙ ВІТАЛІЙ ЛЕОНІДОВИЧ

УДК 342.9 (477)

ДИСЕРТАЦІЯ

АДМІНІСТРАТИВНО-ПРАВОВІ ЗАСАДИ ДІЯЛЬНОСТІ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ ЩОДО ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

12.00.07 – адміністративне право і процес;
фінансове право; інформаційне право

Подається на здобуття наукового ступеня кандидата юридичних наук

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

Науковий керівник **– Сокуренко Олена Анатоліївна**, кандидат юридичних наук, доцент

Київ – 2025

АНОТАЦІЯ

Монастирецький В. Л. Адміністративно-правові засади діяльності Служби безпеки України щодо захисту об'єктів критичної інфраструктури. – *Кваліфікаційна наукова праця на правах рукопису.*

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». – Науково-дослідний інститут публічного права, Науково-дослідний інститут публічного права, Київ, 2025.

У дисертаційній роботі наведено теоретичне узагальнення та нове вирішення наукового завдання, яке полягало в тому, щоб встановити сутність та розкрити особливості адміністративно-правових засад діяльності Служби безпеки України щодо захисту об'єктів критичної інфраструктури, на основі чого надати обґрунтовані пропозиції та рекомендації, спрямовані на вдосконалення адміністративного законодавства в цій сфері з урахуванням викликів і загроз, обумовлених військовою агресією.

Доведено, що захист критичної інфраструктури – комплексна, систематична, багатовекторна діяльність, яка реалізується в процесі створення та управління об'єктом критичної інфраструктури та спрямовується на профілактику, попередження, виявлення та припинення загроз безпеці функціонування та власне факту існування такого об'єкта, відшкодування шкоди та виправлення негативних наслідків у разі реалізації загроз.

Встановлено, що державна політика у сфері захисту критичної інфраструктури – це стратегічні й тактичні вектори діяльності органів державної влади та інших уповноважених суб'єктів публічного управління щодо організації та ефективної реалізації діяльності у сфері захисту критичної інфраструктури в Україні, які обумовлені об'єктивними умовами суспільно-політичного, економічного розвитку, безпекової ситуації тощо.

Аргументовано, що суб'єкти загальнодержавного рівня забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури виконують широкі функції та відповідають за реалізацію глобальних цілей, пов'язаних із формуванням і провадженням державної політики у сфері критичної інфраструктури; визначенням об'єктів, які належать до системи останньої; здійсненням координації та управління іншими суб'єктами захисту, а також організацією їх взаємодії; розробленням і затвердженням стратегічних документів, пов'язаних із проведенням заходів захисту;

Зауважено, що Служба безпеки України має досить вузьке спрямування діяльності у сфері забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури. Служба є спеціалізованим правоохоронним органом, уповноваженим протидіяти загрозам, що мають підвищений рівень публічної небезпеки та які здатні завдати шкоди не лише окремим об'єктам критичної інфраструктури, а й життєво важливим інтересам суспільства та держави загалом.

Констатовано, що принципи забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури Службою безпеки України – це нормативно закріплені та засновані на загальновизнаних цінностях і призначенні права, базові юридичні засади, які визначають зміст, організацію та порядок діяльності Служби безпеки України щодо запобігання загрозам, охорони й підтримання стабільного функціонування об'єктів критичної інфраструктури.

Обґрунтовано, що стан нормативних засад забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури в діяльності Служби безпеки України можна оцінити як загалом сформований, але такий, що залишається недостатньо систематизованим і орієнтованим передусім на безпекові та контррозвідувальні аспекти. Досліджуване нормативне регулювання забезпечує Службу безпеки України необхідними повноваженнями для виявлення та нейтралізації загроз об'єктам критичної

інфраструктури, однак воно переважно зосереджене на реагуванні на загрози, а не на комплексному забезпеченні стійкості та безперервності їх функціонування. Водночас спостерігається недостатня деталізація механізмів координації з іншими суб'єктами захисту критичної інфраструктури й обмежена регламентація превентивних заходів, що знижує ефективність практичної реалізації відповідних повноважень.

Зазначено, що адміністративно-правовий статус Служби безпеки України щодо захисту об'єктів критичної інфраструктури – це системна сукупність визначених законодавством України юридичних елементів, які встановлюють місце, роль і призначення Служби безпеки України в суспільно-правових відносинах, що виникають з метою реалізації діяльності, спрямованої на забезпечення безпеки і стійкості функціонування об'єктів критичної інфраструктури. Виокремлено елементи відповідного статусу та надано їм характеристику.

З'ясовано, що адміністративно-правовий механізм захисту об'єктів критичної інфраструктури Службою безпеки України – це юридична конструкція, яку становлять адміністративно-правові інструменти, що реалізуються уповноваженими органами, підрозділами, окремими посадовими особами Служби з метою впливу на сферу критичної інфраструктури, а також забезпечення стійкості, безпеки функціонування зарахованих до неї об'єктів.

Визначено глибоку інтегрованість Служби безпеки України в роботу системи органів забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури. Водночас реалізація інструментарію відповідного механізму відбувається із суворим дотриманням принципу дотримання державної таємниці та не допускає публічного розголошення операційного порядку діяльності СБУ.

Доведено, що адміністративно-правові інструменти захисту об'єктів критичної інфраструктури Службою безпеки України – це передбачені

законодавством України форми, засоби, способи й заходи, які використовуються органами та підрозділами СБУ для формування необхідного стану безпеки об’єктів критичної інфраструктури, підтримання стійкості їх функціонування, а також безпосереднього захисту від будь-яких загроз і посягань.

Встановлено, що взаємодія Служби безпеки України з державними та громадськими інституціями в процесі запобігання несанкціонованому втручанню у функціонування об’єктів критичної інфраструктури – це врегульована нормами чинного законодавства система узгоджених дій, заходів, інформаційного обміну тощо між Службою безпеки України та іншими уповноваженими органами державної влади, органами місцевого самоврядування, суб’єктами управління критичною інфраструктурою та інститутами громадянського суспільства, спрямована на виявлення, запобігання і нейтралізацію загроз незаконного втручання, а також на забезпечення безперервності та стійкості функціонування об’єктів критичної інфраструктури.

З’ясовано, що стратегічне планування забезпечення безпеки та стійкості функціонування об’єктів критичної інфраструктури – це довгостроковий, системний та комплексний процес формування цілей, принципів, пріоритетів і механізмів, спрямованих на попередження, мінімізацію та нейтралізацію загроз, що можуть порушити безперервність роботи життєво важливих інфраструктурних систем держави. Таке планування має комплексний характер, адже передбачає узгодження дій між різними державними органами, операторами критичної інфраструктури, силовими структурами, науковими установами та громадськими інституціями, що забезпечує всебічне бачення ризиків і подальшого опрацювання шляхів їх подолання.

Окреслено недоліки Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури, а саме: по-перше, План

видається досить загальним і містить відносно розмиті адміністративно-правові механізми для практичного виконання; по-друге, у ньому немає чітких показників оцінки ефективності, через що складно оцінити, чи досягнуто поставлені цілі; по-третє, недостатньо визначено питання ресурсів, зокрема фінансових, технічних і кадрових, які описані поверхово; по-четверте, механізми взаємодії з приватним сектором та громадськістю практично не деталізовані, хоча ці суб'єкти відіграють важливу роль у забезпечення безпеки критичної інфраструктури; по-п'яте, процедура обміну інформацією залишається нечіткою, що може впливати на швидкість і якість реагування на загрози.

Узагальнено, що стратегічне планування забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури є ключовим елементом національної політики у сфері безпеки, оскільки воно визначає довгострокові підходи до захисту систем, від яких залежить життєдіяльність держави та суспільства. Таке планування спрямоване не лише на забезпечення безперервного функціонування об'єктів критичної інфраструктури, а й на підвищення її здатності протистояти комплексним, гібридним і технологічно складним загрозам, характерним для сучасного безпекового середовища.

Встановлено, що вдосконалення адміністративно-правового регулювання діяльності Служби безпеки України в умовах режиму воєнного стану щодо захисту об'єктів критичної інфраструктури має передбачати: по-перше, забезпечення гармонізації законів України «Про Службу безпеки України» та «Про критичну інфраструктуру» в частині: а) визначення місця СБУ в системі суб'єктів захисту критичної інфраструктури; б) закріплення та деталізація повноважень Служби в межах захисту об'єктів критичної інфраструктури.

Зауважено, що оцінювання діяльності Служби безпеки України в умовах режиму воєнного стану щодо захисту об'єктів критичної

інфраструктури – це системний, цілеспрямований та науково і методично обґрунтований процес ретроспективного та поточного аналізу змісту, результатів і наслідків адміністративно-управлінських, контррозвідувальних й координаційних заходів, що здійснюються Службою безпеки України з метою забезпечення стійкого функціонування, захищеності та безпеки об’єктів критичної інфраструктури в умовах дії воєнного стану, шляхом визначення їхньої ефективності, результативності, законності та відповідності характеру воєнних і гібридних загроз, з подальшим використанням отриманих висновків для підзвітності, удосконалення управлінських рішень і формування науково обґрунтованої бази для розвитку системи національної безпеки.

Ключові слова: критична інфраструктура, об’єкт, захист адміністративно-правове регулювання, завдання, принципи, нормативно-правові засади, адміністративно-правовий статус, Служба безпеки України, адміністративно-правовий механізм, адміністративно-правові інструменти, взаємодія, стратегічне планування, удосконалення, адміністративне законодавство.

SUMMARY

Monastyretskyi V. L. Administrative and legal basis for the activities of the Security Service of Ukraine regarding the protection of critical infrastructure facilities. – *Professional scientific paper as manuscript.*

Thesis for obtaining a scientific degree of Candidate of Legal Sciences, specialty 12.00.07 «Administrative Law and Procedure; Financial Law; Information Law». – Scientific Institute of Public Law, Scientific Institute of Public Law, Kyiv, 2025.

The Thesis provides a theoretical generalization and a new solution to the scientific problem, which lies in establishing the essence and revealing the peculiarities of the administrative and legal foundations of the Security Service of Ukraine's activities regarding the protection of critical infrastructure facilities, on the basis of which to provide substantiated proposals and recommendations aimed at improving administrative legislation in this area, taking into account the challenges and threats caused by military aggression.

It has been proven that the protection of critical infrastructure is a complex, systematic, multi-vector activity carried out in the process of creating and managing a critical infrastructure facility and aimed at preventing, warning, detecting, and eliminating threats to the security of the functioning and very existence of such a facility, compensating for damage, and remediation of negative consequences in cases of implementation of threats.

It has been established that State policy in the field of critical infrastructure protection is the strategic and tactical vectors of activity of State authorities and other authorized public administration entities regarding the organization and effective implementation of activities aimed at protecting critical infrastructure in Ukraine, which are determined by objective conditions of socio-political and economic development, the security situation, etc.

It has been argued that entities at the national level responsible for ensuring the security and stability of critical infrastructure facilities perform broad functions

and are responsible for the implementation of global objectives related to: the formation and implementation of State policy in the field of critical infrastructure; identifying facilities that are part of the critical infrastructure system; coordinating and managing other protection entities, as well as organizing their interaction; developing and approving strategic documents related to the implementation of protection measures, etc.

It has been concluded that the Security Service of Ukraine has a rather narrow focus in the field of ensuring the security and stability of critical infrastructure facilities. Therefore, the SSU is a specialized law enforcement agency authorized to counter threats that pose a high level of public danger and are capable of causing damage not only to individual critical infrastructure facilities, but also to the vital interests of society and the State as a whole.

It has been proven that the principles of ensuring the security and stability of critical infrastructure facilities by the Security Service of Ukraine are basic legal principles normatively established and grounded on universally recognized values and the purpose of law that determine the content, organization, and procedure of the SSU's activities to prevent threats, protect, and maintain the stable functioning of critical infrastructure facilities.

In general, the state of regulatory and legal support for the security and stability of critical infrastructure facilities in the activities of the Security Service of Ukraine can be assessed as generally established, but still not fully systematized and focused primarily on security and counterintelligence aspects. Regulatory framework provides the SSU with the necessary powers to identify and neutralize threats to critical infrastructure facilities, but it focuses primarily on responding to threats rather than on comprehensively ensuring the stability and continuity of their functioning. At the same time, there is insufficient detail regarding the mechanisms for coordination with other critical infrastructure protection entities and limited regulation of preventive measures, which reduces the effectiveness of the practical implementation of the relevant powers.

It has been established that the administrative and legal status of the Security Service of Ukraine regarding the protection of critical infrastructure facilities is a systematic set of legal elements defined by Ukrainian legislation establishing the place, role, and purpose of the SSU in socio-legal relations arising from the implementation of activities aimed at ensuring the security and stability of critical infrastructure facilities. The elements of the relevant status have been identified and characterized.

It has been substantiated that the administrative and legal mechanism for the protection of critical infrastructure facilities by the Security Service of Ukraine is a legal construct consisting of administrative and legal instruments implemented by authorized bodies, subdivisions, individual officials of the Service with the aim of influencing the critical infrastructure sector and ensuring the stability and security of the functioning of the facilities included in it.

The deep integration of the SSU into the work of the system of bodies ensuring the security and stability of critical infrastructure facilities has been noted. At the same time, the implementation of the instruments of the relevant mechanism is carried out in strict compliance with the principle of State secrecy and does not allow public disclosure of the SSU operational procedures.

It has been proven that the administrative and legal instruments for protecting critical infrastructure facilities by the Security Service of Ukraine are the forms, means, methods, and measures provided for by Ukrainian legislation, which are used by the SSU bodies and units to establish the necessary security conditions for critical infrastructure facilities, maintain the stability of their functioning, and provide direct protection against any threats and encroachments.

It has been established that the interaction between the Security Service of Ukraine and State and public institutions in the process of preventing unauthorized interference in the functioning of critical infrastructure facilities is a system of coordinated actions, measures, and information exchange, etc., between the SSU and other authorized State authorities, local self-government bodies, critical

infrastructure management entities, and civil society institutions, which is regulated by the norms of current legislation and aimed at identifying, preventing, and countering unauthorized interference in the functioning of critical infrastructure facilities.

It has been established that strategic planning for ensuring the security and resilience of critical infrastructure facilities is a long-term, systematic, and comprehensive process of forming goals, principles, priorities, and mechanisms aimed at preventing, minimizing, and neutralizing threats that could disrupt the continuity of the functioning of the State's vital infrastructure systems. Such planning is comprehensive in nature, as it involves coordination between various State bodies, critical infrastructure operators, law enforcement agencies, scientific institutions, and public institutions, which ensures a comprehensive view of risks and further development of ways to overcome them.

The shortcomings of the National Plan for the Protection and Security of Critical Infrastructure have been identified, including: firstly, the Plan appears to be rather general and contains relatively vague administrative and legal mechanisms for practical implementation; secondly, it lacks clear performance indicators, making it difficult to assess whether the objectives have been achieved; thirdly, the issue of resources, in particular financial, technical, and human resources, is not sufficiently defined and is described in a superficial manner; fourthly, the mechanisms for interaction with the private sector and the public are practically not detailed, although these entities play an important role in ensuring the security of critical infrastructure; fifthly, the procedure for information exchange remains unclear, which may affect the speed and quality of response to threats.

In summary, strategic planning for the security and resilience of critical infrastructure is a key element of national security policy, as it defines long-term approaches to protecting the systems on which the functioning of the State and society depend. Such planning is aimed not only at ensuring the continuous

functioning of critical infrastructure facilities, but also at enhancing their ability to withstand complex, hybrid, and technologically sophisticated threats characteristic of the modern security environment.

It has been established that improving the administrative and legal regulation of the activities of the Security Service of Ukraine under the legal regime of martial law regarding the protection of critical infrastructure facilities should provide for the harmonization of the Laws of Ukraine "On the Security Service of Ukraine" and «On Critical Infrastructure» in terms of: a) defining the place of the SSU in the system of critical infrastructure protection entities; b) consolidating and detailing the powers of the Service in the protection of critical infrastructure facilities.

It should be noted that the assessment of the activities of the Security Service of Ukraine under martial law in relation to the protection of critical infrastructure facilities is a systematic, targeted, and scientifically and methodologically sound process of retrospective and ongoing analysis of the content, results, and consequences of administrative, counterintelligence, and coordination measures carried out by the Security Service of Ukraine to ensure the stable functioning, protection, and security of critical infrastructure facilities under martial law by determining their effectiveness, efficiency, legality, and relevance to the nature of military and hybrid threats, with the further use of the conclusions obtained for accountability, improvement of management decisions, and formation of a scientifically sound basis for the development of the national security system.

Keywords: critical infrastructure, facility, protection, administrative and legal regulation, tasks, principles, regulatory and legal framework, administrative and legal status, Security Service of Ukraine, administrative and legal mechanism, administrative and legal instruments, interaction, strategic planning, improvement, administrative legislation.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Монастирецький В. Л. Поняття адміністративно-правового механізму захисту об’єктів критичної інфраструктури Службою безпеки України. *Право та державне управління*. 2022. № 3. С. 505–510.

2. Монастирецький В. Л. Місце служби безпеки України в системі суб’єктів забезпечення безпеки та стійкості функціонування об’єктів критичної інфраструктури. *KELM*. 2023. № 7 (59). С. 477–480 (Республіка Польща).

3. Монастирецький В. Л. Адміністративно-правові інструменти захисту об’єктів критичної інфраструктури службою безпеки України. *Право і суспільство*. 2024. № 4. С. 865–870.

4. Monastyretskyi V. Definition of the administrative and legal status of the security service of Ukraine with regard to the protection of critical infrastructure facilities. *Entrepreneurship, Economy and Law*. 2024. № 4. P. 33–37.

5. Монастирецький В. Л. До проблеми визначення поняття критичної інфраструктури та її захисту. *Науковий вісник публічного та приватного права*. 2025. Вип. 4. С. 246–250.

які засвідчують апробацію матеріалів дисертації:

6. Монастирецький В. Л. Принципи забезпечення безпеки та стійкості функціонування об’єктів критичної інфраструктури Службою безпеки України. *Виклики сучасності та наукові підходи до їх вирішення*: матеріали Міжнар. наук.-практ. конф. (Київ, 12–13 серп. 2020 р.). Київ: Наук.-дослід. ін-т публіч. права, 2020. С. 132–134.

7. Монастирецький В. Л. Структура адміністративно-правового статусу Служби безпеки України щодо захисту об’єктів критичної інфраструктури. *Інноваційні підходи до реформування сучасного законодавства*: матеріали Міжнар. наук.-практ. конф. (Київ, 20–21 квіт. 2023 р.). Київ: Наук.-дослід. ін-т публіч. права, 2023. С. 144–146.

8. Монастирецький В. Л. Завдання забезпечення безпеки та стійкості функціонування об’єктів критичної інфраструктури Службою безпеки України. *Актуальні проблеми імплементації наукових досягнень у практичну діяльність*: матеріали Міжнар. наук.-практ. конф. (Київ, 4–5 черв. 2024 р.). Київ: Наук.-дослід. ін-т публіч. права, 2024. С. 98–100.

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дослідження. Наявна безпекова ситуація в Україні засвідчує, що критична інфраструктура в сучасних цивілізованих державах перетворилася з допоміжного елементу забезпечення життєдіяльності суспільства на системоутворюючий та базовий чинник національної безпеки, від стійкості якого безпосередньо залежить функціонування публічної влади, економіки, обороноздатності й основних соціальних процесів. Енергетичні, транспортні, інформаційно-комунікаційні, фінансові та інші життєво важливі об'єкти формують складну взаємопов'язану мережу, порушення якої здатне спричинити негативні наслідки загальнодержавного масштабу. В умовах постійних атак на критичну інфраструктуру України питання її захисту набуває не лише технічного чи організаційного, а й передусім військового характеру. Зазначене забезпечує низка суб'єктів, у системі яких самостійне місце належить Службі безпеки України.

Діяльність вказаного органу в цій сфері має специфічний характер з огляду на особливості правового статусу Служби, а також властивості власне критичної інфраструктури. Зазначене своєю чергою зумовлює підвищені вимоги до правової визначеності, легітимності й ефективності застосовуваних повноважень. Водночас динамічний розвиток законодавства про критичну інфраструктуру, поява нових форм загроз і трансформація моделі державного управління спонукають до ґрунтовного наукового осмислення адміністративно-правових засад діяльності Служби безпеки України в цій сфері.

Зв'язок теми дисертації із сучасними дослідженнями. Варто зауважити, що в останні роки багато проблемних аспектів, пов'язаних із діяльністю служби безпеки України, у своїх наукових працях розглядали: О. В. Антонюк, І. Р. Байрак, О. М. Бандурка, М. В. Барандій,

В. М. Бесчастний, В. М. Біліченко, С. В. Бунін, М. М. Бурбика, З. М. Бурик, А. В. Гайдук, Ю. В. Гаруст, Є. А. Гетьман, О. О. Гречко, Н. В. Гришина, Р. З. Дарміць, О. Ю. Дахно, О. В. Джафарова, Є. В. Дуліба, Д. Г. Заброда, В. О. Зозуля, А. М. Клочко, Є. В. Кобко, Ю. І. Коваленко, А. Т. Комзюк, І. В. Кременовська, В. В. Крижна, В. І. Курило, К. М. Куркова, Л. В. Лазоренко, А. О. Левчук, В. І. Литвиненко, Л. І. Луценко-Миськів, А. А. Манжула, О. Ю. Мішин, В. Ю. Оксінь, В. В. Полюхович, І. С. Процик, Я. Ф. Радиш, О. М. Рєзнік, К. В. Ростовська, О. Ю. Салманова, М. О. Саракуца, Є. Ю. Соболь, С. В. Сокирко, О. А. Сокуренко, Л. В. Сорока, О. В. Стасів, Т. О. Цимбалістий, О. І. Червяков, Р. В. Шаповал, С. О. Шатрава, О. О. Шевчук, К. В. Шкарупа, О. С. Юнін.

Водночас, попри значний теоретичний доробок, у науковій літературі фактично неопрацьованим є питання дослідження адміністративно-правових засад діяльності Служби безпеки України щодо захисту об’єктів критичної інфраструктури.

Таким чином, наявність низки прогалин та недоліків правового й організаційного характеру, складна безпекова ситуація, а також відсутність комплексних монографічних досліджень обумовлюють актуальність і своєчасність дисертаційного дослідження, присвяченого адміністративно-правовим засадам діяльності Служби безпеки України щодо захисту об’єктів критичної інфраструктури.

Зв’язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження виконано відповідно до Цілей сталого розвитку України на період до 2030 року, затверджених Указом Президента України від 30 вересня 2019 року № 722/2019; Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки, схваленого Указом Президента України від 11 травня 2023 року № 273/2023; Стратегії національної безпеки України, затвердженої Указом Президента України від 14 вересня 2020 року

№ 392/2020; Антикорупційної стратегії на 2021–2025 роки, затвердженої Законом України від 20 червня 2022 року № 2322-IX; Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури, затвердженого розпорядженням Кабінету Міністрів України від 19 вересня 2023 року № 825-р. Тема роботи узгоджується з темою науково-дослідної роботи Науково-дослідного інституту публічного права «Правове забезпечення прав, свобод та законних інтересів суб'єктів публічно-правових відносин» (номер державної реєстрації 0120U105390).

Мета та завдання дослідження. *Мета* дисертаційного дослідження полягає в тому, щоб встановити сутність і розкрити особливості адміністративно-правових засад діяльності Служби безпеки України щодо захисту об'єктів критичної інфраструктури, а також на основі узагальнення правозастосовної практики надати обґрунтовані пропозиції та рекомендації, спрямовані на вдосконалення адміністративного законодавства в цій сфері, з урахуванням викликів і загроз, обумовлених військовою агресією.

Досягнення поставленої мети зумовлює потребу у вирішенні таких *завдань*:

– розкрити захист об'єктів критичної інфраструктури як об'єкт адміністративного-правового регулювання та предмет діяльності Служби безпеки України;

– встановити місце Служби безпеки України в системі суб'єктів забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури;

– розкрити завдання, принципи й нормативні засади забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури Службою безпеки України;

– з'ясувати сутність та окреслити структуру адміністративно-правового статусу Служби безпеки України щодо захисту об'єктів критичної інфраструктури;

– визначити поняття й узагальнити особливості адміністративно-правового механізму захисту об’єктів критичної інфраструктури Службою безпеки України;

– виокремити адміністративно-правові інструменти захисту об’єктів критичної інфраструктури Службою безпеки України;

– розкрити взаємодію Служби безпеки України з державними та громадськими інституціями в процесі запобігання несанкціонованого втручання у функціонування об’єктів критичної інфраструктури;

– окреслити специфіку стратегічного планування забезпечення безпеки та стійкості функціонування об’єктів критичної інфраструктури, виокремити місце в ньому Служби безпеки України;

– запропонувати напрями вдосконалення адміністративно-правового регулювання діяльності Служби безпеки України в умовах режиму воєнного стану щодо захисту об’єктів критичної інфраструктури.

Об’єктом дослідження є правові відносини, які виникають у процесі діяльності Служби безпеки України щодо захисту об’єктів критичної інфраструктури.

Предмет дослідження – адміністративно-правові засади діяльності Служби безпеки України щодо захисту об’єктів критичної інфраструктури.

Методи дисертаційного дослідження. Методологічну основу дисертації становлять різноманітні методи наукового пізнання. Так, використання методу *документального аналізу* та *аналітичного* методу дало змогу розкрити захист об’єктів критичної інфраструктури як об’єкт адміністративного-правового регулювання та предмет діяльності Служби безпеки України (підрозділ 1.1); встановити місце Служби безпеки України в системі суб’єктів забезпечення безпеки та стійкості функціонування об’єктів критичної інфраструктури (підрозділ 1.2). *Структурно-логічний* та *системно-функціональний* методи застосовано з метою розкриття завдань, принципів і нормативних засад забезпечення безпеки та стійкості

функціонування об’єктів критичної інфраструктури Службою безпеки України (підрозділ 1.3); з’ясування сутності й окреслення структури адміністративно-правового статусу Служби безпеки України щодо захисту об’єктів критичної інфраструктури (підрозділ 1.4). Визначити поняття та узагальнити особливості адміністративно-правового механізму захисту об’єктів критичної інфраструктури Службою безпеки України дав змогу *логіко-семантичний метод* (підрозділ 2.1). *Формально-юридичний* метод використано для того, що визначити адміністративно-правові інструменти захисту об’єктів критичної інфраструктури Службою безпеки України (підрозділ 2.2). Застосування *функціонального методу* уможливило надання характеристики взаємодії Служби безпеки України з державними та громадськими інституціями в процесі запобігання несанкціонованого втручання у функціонування об’єктів критичної інфраструктури (підрозділ 2.3), а також з’ясування особливостей стратегічного планування забезпечення безпеки та стійкості функціонування об’єктів критичної інфраструктури, визначення місця в ньому Служби безпеки України (підрозділ 3.1). Запропонувати напрями вдосконалення адміністративно-правового регулювання діяльності Служби безпеки України в умовах режиму воєнного стану щодо захисту об’єктів критичної інфраструктури (підрозділ 3.2) вдалося за допомогою методів *моделювання* та *прогнозування*.

Науково-теоретичне підґрунтя дисертаційної роботи становлять праці фахівців з галузі конституційного, адміністративного права, а також інших наукових дисциплін, зокрема теорії держави та права, теорії управління, соціології, філософії. *Нормативно-правову основу* праці ставить Конституція України, а також низка законодавчих, підзаконних і відомчих нормативно-правових актів Служби безпеки України. *Інформаційною та емпіричною* базою дисертаційної роботи є науково-періодичні видання, статистичні дані

діяльності Служби безпеки України, наукова публіцистика, аналітичні матеріали тощо.

Наукова новизна отриманих результатів полягає в тому, що дисертація є першої спробою встановити сутність і розкрити особливості адміністративно-правових засад діяльності Служби безпеки України щодо захисту об'єктів критичної інфраструктури, а також надати обґрунтовані пропозиції та рекомендації, спрямовані на вдосконалення адміністративного законодавства в цій сфері з урахуванням сучасних викликів і загроз. У результаті проведеного дослідження сформульовано низку нових наукових положень та висновків, зокрема:

вперше:

– визначено характерні особливості взаємодії Служби безпеки України з державними та громадськими інституціями в процесі запобігання несанкціонованого втручання у функціонування об'єктів критичної інфраструктури: 1) у відповідних правовідносинах Служба безпеки України переважно відіграє роль координатора, а отже, вона є обов'язковим учасником процесу погодження стратегічно важливих рішень, пов'язаних із захистом об'єктів критичної інфраструктури; 2) така спільна діяльність передбачає узгодження рішень і дій Служби безпеки України з одним або декількома органами влади, а також операторами критичної інфраструктури, що необхідно через високий рівень взаємозалежності систем; 3) до взаємодії активно залучається громадський сектор, представники якого беруть участь у моніторингу, аналізі ризиків, обговоренні політик безпеки та формуванні культури кібер- та фізичної стійкості; 4) специфіка взаємодії полягає в тому, що Служба безпеки України передає іншим інституціям релевантні, а іноді й засекречені дані про загрози, що дозволяє прискорити реагування на ризики, а також покладає на інші сторони взаємодії додаткову відповідальність; 5) у межах практичної реалізації відповідної спільної діяльності увагу зосереджено переважно на профілактиці, що охоплює раннє виявлення та

блокування загроз, включно з попередженням диверсій, кібератак, інсайдерських дій; 6) спрямована на синхронізацію стандартів і вимог безпеки між різними секторами; 7) взаємодія передбачає об'єднання кібербезпеки, фізичного захисту, антикризового управління, антитерористичної діяльності й розвідки, що відповідає сучасним реаліям; 8) інклюзивність взаємодії, адже Служба безпеки України залучає та обговорює ключові питання безпеки з професійними об'єднаннями, галузевими асоціаціями та профільними експертами; 9) ключовою метою взаємодії є створення такої системи захисту критичної інфраструктури, яка здатна витримати тривалі й комбіновані впливи, характерні для сучасних воєнних і кібервикликів;

– запропоновано авторське визначення поняття «адміністративно-правовий механізм захисту об'єктів критичної інфраструктури Службою безпеки України», зміст якого запропоновано розглядати крізь призму таких елементів: 1) адміністративно-правові інструменти захисту об'єктів критичної інфраструктури; 2) інституційна основа реалізації відповідних інструментів; 3) нормативні акти, що визначають порядок і специфіку реалізації останніх;

– окреслено особливості стратегічного планування забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури, до яких віднесено такі: 1) орієнтація на довгостроковий прогноз ризиків і сценаріїв загроз, які можуть бути скореговані залежно від безпекової, економічної та інших ситуацій; 2) має комплексний характер, адже має враховувати й поєднувати фізичну, технологічну, інформаційну, організаційну складові та кібербезпеку; 3) передбачає узгодження та координацію дій різними державними органами, операторами інфраструктури та суспільними інституціями; 4) має не лише превентивний характер, спрямований на запобігання інцидентам, а й реактивний; 5) враховує критичні залежності між різними секторами інфраструктури, зокрема критичної; 6) потребує чіткого

розподілу ресурсів і компетенції спеціально уповноважених суб'єктів; 7) передбачає регулярне оновлення планів на основі аналізу інцидентів і результатів моніторингу;

удосконалено:

– визначення поняття критичної інфраструктури, яким запропоновано вважати сукупність матеріальних і нематеріальних об'єктів, що мають критичне значення для нормального функціонування всієї держави, її економіки, національної безпеки, оборони, соціального сектору, порушення яких потенційно становить загрозу або має ризик спричинення реальної шкоди національним інтересам, функціонуванню державного апарату, життю, здоров'ю та добробуту населення;

– твердження про те, що Служба безпеки України як правоохоронний орган виконує правоохоронну, правозастосовну та інші публічні функції, які безпосередньо пов'язані із захистом прав, свобод, законних інтересів суспільства та кожної окремої людини від протиправних посягань, зокрема на об'єктах критичної інфраструктури; встановленням осіб, які вчинили правопорушення, збором доказів їх вини та притягненням до юридичної відповідальності;

– теоретичний підхід щодо тлумачення адміністративно-правових інструментів захисту об'єктів критичної інфраструктури Службою безпеки України, якими запропоновано розуміти передбачені чинним законодавством форми, засоби, способи й заходи, що використовуються органами та підрозділами СБУ для формування необхідного стану безпеки об'єктів критичної інфраструктури, підтримання стійкості їх функціонування, а також безпосереднього захисту від будь-яких загроз і посягань;

– наукове бачення критеріїв оцінювання ефективності діяльності Служби безпеки України в умовах режиму воєнного стану щодо захисту об'єктів критичної інфраструктури, які запропоновано поділити на дві групи: 1) якісні,

а саме: законність та обґрунтованість управлінських рішень і заходів; відповідність діяльності СБУ характеру та рівню воєнних і гібридних загроз; рівень превентивності у виявленні та нейтралізації загроз об’єктам критичної інфраструктури; ефективність міжвідомчої координації та взаємодії з операторами критичної інфраструктури; адаптивність управлінських рішень до динаміки воєнної обстановки; дотримання принципу пропорційності й балансу між безпекою та правами людини; якість організаційно-правового забезпечення захисту об’єктів критичної інфраструктури; рівень підзвітності й контрольованості діяльності; 2) кількісні, зокрема: кількість виявлених і нейтралізованих загроз об’єктам критичної інфраструктури; кількість попереджених диверсійних, терористичних загроз та кібератак; частка об’єктів критичної інфраструктури, охоплених превентивними заходами безпеки; середній час реагування на загрози й інциденти; кількість проведених координаційних заходів, спільних операцій і нарад; кількість обов’язкових приписів, рекомендацій або заходів реагування, реалізованих операторами критичної інфраструктури; рівень безперервності функціонування об’єктів критичної інфраструктури під час воєнних загроз; динаміка зниження інцидентів безпеки порівняно з попередніми періодами;

дістало подальшого розвитку:

– узагальнення кола принципів забезпечення безпеки та стійкості функціонування об’єктів критичної інфраструктури Службою безпеки України, до яких віднесено засади: законності та верховенства права; забезпечення й дотримання прав та свобод людини і громадянина; координованості та взаємодії; гнучкості й адаптивності до змін; конфіденційності та захисту таємної інформації;

– поняття взаємодії Служби безпеки України з державними та громадськими інституціями в процесі запобігання несанкціонованому втручанню у функціонування об’єктів критичної інфраструктури, якою запропоновано розуміти врегульовану нормами чинного законодавства

систему узгоджених дій, заходів, інформаційного обміну тощо між Службою безпеки України та іншими уповноваженими органами державної влади, органами місцевого самоврядування, суб'єктами управління критичною інфраструктурою та інститутами громадянського суспільства, що спрямована на виявлення, запобігання і нейтралізацію загроз незаконного втручання, а також на забезпечення безперервності та стійкості функціонування об'єктів критичної інфраструктури;

– обґрунтування наукової думки про те, що суб'єкти загальнодержавного рівня забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури виконують широкі функції та відповідають за реалізацію глобальних цілей, пов'язаних із формуванням і провадженням державної політики у сфері критичної інфраструктури; визначенням об'єктів, які належать до системи останньої; здійсненням координації та управління іншими суб'єктами захисту, а також організацією їх взаємодії; розробленням і затвердженням стратегічних документів, пов'язаних із проведенням заходів захисту;

– теза про те, що реалізація Службою безпеки України адміністративно-правових інструментів захисту критичної інфраструктури переважно відбувається в співпраці з іншими уповноваженими в цій сфері діяльності суб'єктами, що пояснюється декількома моментами: по-перше, превалюванням принципу координованості та взаємодії забезпечення Службою безпеки України безпеки і стійкості функціонування об'єктів критичної інфраструктури; по-друге, тим фактом, що Служба безпеки України не здійснює безпосереднє управління щодо останніх та має спільно працювати з операторами, секторальними органами тощо;

– твердження про те, що участь Служби безпеки України в міжвідомчих робочих групах забезпечує безперервний обмін оперативною інформацією, яка є критично важливою для раннього виявлення загроз, адже втручання у функціонування об'єктів критичної інфраструктури часто має багатоетапний

характер і може виявлятися паралельно в різних сферах, а інші інституції, залучені до робочої групи, отримують доступ до аналітичних можливостей Служби безпеки України та її здатності реагувати на загрози державного рівня, що посилює їхню спроможність діяти у сфері захисту критичної інфраструктури.

Практичне значення отриманих результатів полягає в тому, що викладені в дисертації висновки та пропозиції використовуються і можуть бути використані в:

– *науково-дослідній сфері* – як основа для проведення подальших досліджень, присвячених адміністративно-правовим засадам діяльності Служби безпеки України щодо захисту об'єктів критичної інфраструктури (акт впровадження Науково-дослідного інституту публічного права);

– *правотворчій діяльності* – у процесі вдосконалення та розробки нових нормативно-правових актів різної юридичної сили, у нормах яких закріплено адміністративно-правові засади діяльності Служби безпеки України щодо захисту об'єктів критичної інфраструктури;

– *правозастосовній діяльності* – з метою підвищення ефективності діяльності Служби безпеки України щодо захисту об'єктів критичної інфраструктури;

– *освітньому процесі* – під час підготовки підручників, навчальних посібників, а також лекцій і навчальних матеріалів з дисциплін «Адміністративне право», «Правоохоронна діяльність», «Національна безпека та оборона» тощо.

Апробація матеріалів дисертації. Підсумки розроблення проблематики та відповідні висновки оприлюднено на міжнародних науково-практичних конференціях: «Виклики сучасності та наукові підходи до їх вирішення» (м. Київ, 12–13 серпня 2020 р.), «Інноваційні підходи до реформування сучасного законодавства» (м. Київ, 20–21 квітня 2023 р.), «Актуальні

проблеми імплементації наукових досягнень у практичну діяльність» (м. Київ, 4–5 червня 2024 р.).

Структура та обсяг дисертації. Дисертація складається зі вступу, трьох розділів, які містять дев’ять підрозділів, загальних висновків, списку використаних джерел, додатків. Загальний обсяг дисертації становить 213 сторінок. Список використаних джерел містить 180 найменувань на 21 сторінці.

РОЗДІЛ 1
ЗАГАЛЬНІ ЗАСАДИ ДІЯЛЬНОСТІ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ ЩОДО ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1. Захист об'єктів критичної інфраструктури як об'єкт адміністративно-правового регулювання та предмет діяльності Служби безпеки України

В умовах повномасштабної агресії вкрай важливо, щоб держава, а також усі її функціональні складові працювали належним чином та були захищені від зовнішнього протиправного впливу. Адже стабільність країни в складні часи – це запорука добробуту суспільства загалом та кожного окремого громадянина зокрема. Одним з ключових чинників цього є безпека критичної інфраструктури. Її захист становить предмет роботи державних органів, передусім Служби безпеки України (далі – СБУ), а також об'єкт адміністративно-правового регулювання.

Фундаментом критичної інфраструктури слугує більш широке поняття – «інфраструктура». Термін має латинське походження та утворений одночасно від двох слів: «infra» – нижче, під; «structura» – будова, розміщення [167, с. 62]. В енциклопедичній літературі інфраструктуру розкрито як сукупність специфічних форм, методів і процесів, а також різноманітних споруд і комунікацій, що забезпечують загальні умови й нормальне функціонування економічної, соціальної, екологічної та інших галузей життєдіяльності суспільства, його відтворення й розвиток. Ці умови створюються комплексом галузей економіки, системою технологічних, організаційних, соціальних, комунікаційних взаємозв'язків усіх елементів інфраструктури. На думку укладачів енциклопедії, до інфраструктури належать галузі та види діяльності, що обслуговують як виробничі, так і

невиробничі сфери економіки (транспорт, зв'язок, енергетика, комунальне господарство, водопостачання, торгівля, освіта, охорона здоров'я, кредитно-банківська система тощо), а також допомагають прискорити обіг товарів, капіталів, усіх цінностей, збільшити обсяги виробництва завдяки ефективному використанню наукових досягнень, людського та природно-ресурсного потенціалів [50].

Досліджуючи у своїй дисертації зміст категорії «інфраструктура», А. М. Балашов стверджує, що в загальному значенні це – сукупність об'єктів і форм діяльності, що відіграють допоміжну роль щодо матеріального виробництва й забезпечують загальні умови нормальної життєдіяльності суспільства. В економічній царині, продовжує автор, інфраструктуру визначено як сукупність матеріальних і організаційно-правових умов, що забезпечують сталий економічний розвиток. До матеріальних умов належать наявність розвиненої мережі шляхів сполучення, засобів зв'язку, мереж електро- і водопостачання, а до організаційно-правових – наявність розвинених державних і приватних інститутів, а також стійкої законодавчої бази [7, с. 154].

Визначення критичної інфраструктури та її захисту запропоновано на офіційному рівні. Відповідно до Закону України «Про критичну інфраструктуру», захист критичної інфраструктури – всі види діяльності, що виконуються перед або під час створення, функціонування, відновлення та реорганізації об'єкта критичної інфраструктури, спрямовані на своєчасне виявлення, запобігання і нейтралізацію загроз безпеці об'єктів критичної інфраструктури, а також мінімізацію та ліквідацію наслідків у разі їх реалізації. Досить детально документом описано зміст і значення об'єктів критичної інфраструктури. Згідно з п. 13 ч. 1 ст. 1 Закону, останні становлять об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки й оборони, порушення

функціонування яких може завдати шкоди життєво важливим національним інтересам [123].

Не можна залишити поза увагою в процесі оцінки змісту критичної інфраструктури та діяльності із її захисту індивідуальні висновки науковців, які досліджували ці питання. Аналізуючи процес становлення явища критичної інфраструктури, Л. А. Арсенович зауважує, що вперше цю категорію як політичну концепцію було використано в США. Саме в цій країні вперше офіційно визнано предикат «критична інфраструктура» та остаточно його затверджено 2001 року законом USA «Patriot Act». Так, законодавством США поняття «критична інфраструктура» трактується як «система життєво важливих для країни фізичних чи віртуальних активів і засобів, повне знищення або навіть часткова недієздатність яких можуть призвести до негативного впливу на національну безпеку, економіку, здоров'я та безпеку населення, або будь-яку комбінацію з переліченого». У США до критичної інфраструктури також віднесли національні символи та пам'ятки, а також комерційні об'єкти (музеї, виставки та інші місця, що становлять національну цінність) [6, с. 19].

Сучасні науковці, наприклад, І. В. Уряднікова та В. М. Заплатинський, доходять висновку, що критична інфраструктура – це фізичні та віртуальні системи, об'єкти й ресурси – руйнування, знищення або зниження дієздатності яких призведе до суттєвих загроз країні (регіону або міста), її національній безпеці, життєдіяльності та здоров'ю населення [160, с. 189]. На переконання С. С. Теленика, критична інфраструктура є системним комплексом стратегічних матеріальних та інформаційних об'єктів виробничої, невиробничої, соціальної сфери, а також окремими складовими цього комплексу, зокрема ключовими ресурсними, покликаними забезпечувати повноцінний життєвий цикл, безпеку, охорону здоров'я, добробут людини, сталий розвиток суспільства й економіки держави, підтримання її суверенітету, з огляду на те, що зловмисне втручання у

функціонування, а також пошкодження, руйнація або виведення з ладу системи або її елементів внаслідок диверсій, техногенних чи природних катастроф спроможне призвести до тяжких наслідків: жертв чи поневірянь, шкоди національним інтересам, знецінення надбань людини та держави [154, с. 37]. Водночас О. М. Герасименко критичну інфраструктуру визначає як систему взаємопов'язаних або окремих об'єктів інфраструктури, які становлять та/або забезпечують основу для виконання завдань економіки, оборони, національної безпеки України, руйнація або пошкодження яких призведе до заподіяння шкоди національним інтересам [25, с. 48].

Визначаючи зміст і значення критичної інфраструктури, а також специфіку її захисту, Б. В. Богдан виокремлює ключові ознаки цієї категорії, а саме: 1) системність – виявляється у вертикальній і горизонтальній координації між суб'єктами; 2) міжгалузевий характер – передбачає, що інститут критичної інфраструктури функціонує на стику кількох галузей права, адже регулюється нормами адміністративного, інформаційного, кримінального, фінансового права; 3) публічно-правова природа – полягає в тому, що захист критичної інфраструктури становить публічний інтерес, що обумовлює переважання норм публічного права, імперативного методу правового регулювання; 4) пріоритетність забезпечення національної безпеки України, а не задоволення приватних інтересів окремих суб'єктів; 5) стратегічність – життєво важливими функціями держави та суспільства є забезпечення належної охорони здоров'я населення, функціонування енергопостачання, транспорту, цифрових мереж, оскільки системне порушення функціонування критичної інфраструктури може призвести до негативних наслідків у масштабах держави або адміністративно-територіальної одиниці; 5) динамічність і технологічна чутливість – інститут критичної інфраструктури постійно адаптується до змін безпекової ситуації на національному й міжнародному рівнях, до появи нових непередбачуваних ризиків і загроз, до технологічних викликів (цифрові системи управління),

що потребує постійного оновлення нормативно-правової бази та процедур ризик-менеджменту; 6) превентивний характер – передбачає запобігання виникнення надзвичайних подій через ідентифікацію об'єктів критичної інфраструктури, оцінку ризиків і вразливостей, планування; 7) тісна взаємодія між державою та приватними суб'єктами – запровадження державою вимог до захисту об'єктів критичної інфраструктури, державного аудиту; 8) міжнародна інтегрованість – інститут критичної інфраструктури гармонізується зі змістом директив Європейського Союзу, міжнародною термінологією [13, с. 669].

Як доводять В. І. Франчук, П. Я. Пригунов та С. І. Мельник, критична інфраструктура – це системи й ресурси, фізичні чи віртуальні, що забезпечують функції та послуги, порушення яких призведе до найсерйозніших негативних наслідків для життєдіяльності суспільства, соціально-економічного розвитку країни та забезпечення національної безпеки. На їх думку, основна ідея формування і функціонування об'єктів критичної інфраструктури в країні полягає в тому, щоб створити необхідні умови для реалізації, зокрема: 1) базових потреб людини; 2) життєво важливих функцій держави в мирний час, в умовах надзвичайного, воєнного стану та стану війни. Учені переконують, що захист об'єктів критичної інфраструктури – це діяльність, спрямована на забезпечення високого рівня безпеки відповідного об'єкта, у межах якого забезпечується його функціонування, цілісність, самодостатність і стійкість та діяльність, спрямована на попередження, виявлення, ліквідацію загроз чи небезпеки критичній інфраструктурі, а в разі їх реалізації – відновлення чи відшкодування за завдані збитки [163].

У своєму монографічному дослідженні О. П. Єрменчук доходить висновку, що критична інфраструктура – це система надзвичайно важливих матеріальних і нематеріальних об'єктів національної інфраструктури, що забезпечують її стале функціонування, руйнація або пошкодження яких

(наявними загрозами) може призвести до людських жертв і значних матеріальних збитків з найсерйознішими негативними наслідками для життєдіяльності суспільства, соціально-економічного розвитку країни та національної безпеки. За цих умов захист критичної інфраструктури поєднує три основні напрями: 1) захист від загроз у сфері державної безпеки; вони можуть включати внутрішні загрози та фізичне знищення критичної інфраструктури; 2) захист від кіберзагроз; 3) захист від надзвичайних ситуацій [22; 44, с. 14].

Аналіз наукових підходів засвідчує досить суттєву відмінність між законодавчим і доктринальним розумінням критичної інфраструктури. Вважаємо, що тлумачення вчених відрізняються більшою комплексністю, відображають специфічні характеристики категорії та її вплив на соціум і середовище його життєдіяльності. Ураховуючи зазначене, можна сформулювати власний уточнений висновок щодо сутності критичної інфраструктури та діяльності з її захисту: сукупність матеріальних і нематеріальних об’єктів, які мають критичне значення для нормального функціонування всієї держави, її економіки, національної безпеки, оборони, соціального сектору, порушення яких потенційно становить або має ризик спричинення реальної шкоди національним інтересам, роботі державного апарату, життю, здоров’ю та добробуту населення [82].

Своєю чергою захист критичної інфраструктури – це комплексна, систематична, багатовекторна діяльність, яка провадиться в процесі створення й управління об’єктом критичної інфраструктури та спрямовується на профілактику, попередження, виявлення та припинення загроз безпеці функціонування та власне факту існування такого об’єкта, відшкодування шкоди та виправлення негативних наслідків у разі реалізації загроз [82].

Відповідь на питання про сутність критичної інфраструктури як об’єкта адміністративно-правового регулювання полягає в специфіці правовідносин, на які спрямовано її вплив. Зазначене галузеве регулювання упорядковує

адміністративно-правові відносини, тобто суспільні відносини, які виникають, змінюються та припиняються у сфері публічного управління та реалізації публічних функцій. Найбільш влучні тлумачення цих відносин запропонували співавтори посібника «Адміністративне право України» Л. С. Гулак, С. С. Єсімов, М. В. Ковалів, Г. Ю. Лук'янова та інші, на думку яких зазначені відносини становлять урегульовані адміністративно-правовими нормами суспільні відносини, що виникають у сфері, безпосередньо пов'язаній з владно-управлінською діяльністю, однією зі сторін яких є суб'єкт, наділений державно-владними повноваженнями з метою задоволення публічних або індивідуальних інтересів суб'єктів таких правовідносин. Як різновид правових відносин загалом, продовжують науковці, адміністративно-правові мають усі основні ознаки. Водночас їм притаманні низка особливостей, обумовлених специфікою виконавчої та розпорядчої діяльності: 1) сторонами (суб'єктами) адміністративно-правових відносин є суб'єкти адміністративного права, тобто носії передбачених адміністративно-правовими нормами прав і обов'язків, які здатні ці права реалізовувати, а покладені обов'язки виконувати; 2) те, що однією зі сторін завжди є носій юридично-владних повноважень щодо інших суб'єктів, якими його наділяють адміністративно-правові норми; 3) адміністративно-правові відносини формуються зазвичай в особливій сфері суспільного життя – публічному (державному та самоврядному) управлінні, передусім у зв'язку із здійсненням органами виконавчої влади своїх владно-розпорядчих функцій. Ця особливість адміністративних правовідносин прямо випливає зі змісту предмета адміністративно-правового регулювання; 4) адміністративні правовідносини можуть виникати за ініціативою будь-якої із сторін. Проте згода або бажання другої сторони не є обов'язковою умовою їх виникнення. Адміністративні правовідносини можуть виникати всупереч бажанню другої сторони; 5) суперечки, що виникають між сторонами адміністративних правовідносин, вирішуються зазвичай у позасудовому порядку, тобто

шляхом прямого розпорядження правомочного органу (в адміністративному порядку); 6) в окремих випадках передбачено судовий порядок вирішення адміністративно-правових спорів; 7) порушення однією зі сторін адміністративно-правового відношення вимог адміністративно-правової норми тягне за собою юридичну відповідальність, зокрема перед державою (адміністративна чи дисциплінарна відповідальність); 8) адміністративно-правові відносини завжди мають публічно-владний характер, оскільки один з їх суб'єктів обов'язково має юридично-владні повноваження щодо інших учасників цих відносин [1, с. 99–100].

Суспільно-правові відносини цього типу також притаманні сфері захисту критичної інфраструктури. Подібна діяльність фактично слугує їх детермінантом і вираженням, що підтверджується декількома моментами. Так, згідно з Конституцією України від 28 червня 1996 року № 254к/96-ВР (далі – Конституція, Основний Закон), людина, її життя та здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю. Права та свободи людини, їх гарантії визначають зміст і спрямованість діяльності держави. Держава відповідає перед людиною за свою діяльність. Утвердження та забезпечення прав і свобод людини є головним обов'язком держави. Крім того, відповідно до ст. 17, захист суверенітету й територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу. Оборона України, захист її суверенітету, територіальної цілісності й недоторканності покладаються на Збройні Сили України. Забезпечення державної безпеки й захист державного кордону України покладаються на відповідні військові формування та правоохоронні органи держави, організація і порядок діяльності яких визначаються законом [64].

Згідно з Основним Законом, ключовий обов'язок і напрям державної діяльності полягає в забезпеченні добробуту населення країни, створенні

умов для реалізації всіма його представниками своїх суб'єктивних прав, а також досягнення відповідних інтересів у будь-яких сферах. Критична інфраструктура прямо пов'язана з цими питаннями, адже порушення безпеки її об'єктів створює загрозу для громадян України, обсягів їх правових можливостей, життя та здоров'я. У зв'язку з цим, захист критичної інфраструктури кореспондується із загальним функціоналом держави в особі повноважних суб'єктів із забезпечення прав, свобод й інтересів людини та громадянина, а отже, перебуває в межах предметної орієнтації адміністративного права.

Наступне, на що варто звернути увагу під час вивчення характеристики захисту критичної інфраструктури як об'єкта адміністративно-правового регулювання, – це наявність окремої ланки державної політики, пов'язаної з організацією та здійсненням вказаної комплексної діяльності. У «Великій Українській енциклопедії» зазначено, що «політика» (з грецького «πολιτική» – самоуправління в полісі, державні та суспільні справи, мистецтво управління державою) – це одна зі сфер людської діяльності, спрямована на реалізацію цілей та інтересів задля регулювання різнорівневих взаємин між суспільними групами, державами й народами. Термін «політика» сформулювали давньогрецькі мислителі для означення міста-держави – поліса. У трактаті «Політика» Аристотель тлумачив це поняття як діяльність держави, спрямовану на забезпечення її могутності. Політику розуміли як узагальнення проблем розвитку давньогрецьких правлінь і урядів, а також як одну зі сфер діяльності, що визначає статус індивіда в державі. У сучасній науковій думці політика – це стратегічна діяльність органів державної влади стосовно внутрішніх і зовнішніх взаємодій у формі дипломатії, торгівлі, міграційної політики, міжнародної співпраці, наукових та освітніх проєктів, силової конкуренції, економічних і військово-політичних союзів. Політика є сферою програмної діяльності академічних і релігійних інституцій, політичних партій та громадських

організацій у конкретному соціальному середовищі. Вона спрямована на збереження чи зміну наявного порядку, підтримання миру чи ведення війни, розподіл ресурсів, влади та власності в державно організованому суспільстві [63; 102; 180].

Натомість державна політика, як пише канадський філософ М. Пол-Браун, – це обраний особою, державними органами, урядом напрям дій, завдяки якому вони задовольняють певні свої потреби чи використовують свої можливості, що відображаються в досягнутих результатах і в реальному впливові на життя суспільства [15, с. 65]. Українські науковці, зокрема А. В. Перепелиця, зазначають, що державна політика – це оптимальний синтез об'єктивних тенденцій суспільного розвитку і переважаючих суб'єктивних суджень про свої інтереси в ньому [95, с. 35]. Згідно з тлумаченням В. Є. Романова, О. М. Рудіка та Т. М. Бруса, остання є відносно стабільною, організованою та цілеспрямованою діяльністю уряду стосовно певної проблеми, яка здійснюється ним безпосередньо чи опосередковано і впливає на життя суспільства [137, с. 14]. О. В. Рябічко вважає, що державна політика – це пропонований курс діяльності уряду для задоволення потреб чи використання можливостей, сформульований із зазначенням очікуваних результатів та їх впливу на наявний стан справ і конкретне розв'язання проблем [141]. Одне з найбільш розгорнутих визначень запропонував І. І. Петренко: «Державна політика – це діяльність органів державної влади з управління та керівництва суспільством на основі єдиних цілей, принципів і методів, яка передбачає розробку, законодавче закріплення та впровадження державних цільових програм у різних сферах суспільного життя з метою розв'язання нагальних проблем, задоволення потреб суспільства» [96]. Натомість, згідно з баченням А. І. Лиги, державна політика є системою діяльності держави з виявлення суспільного інтересу та забезпечення досягнення суспільно-політичної згоди в приватних і публічних складових інтересу, який визначає принципи, цілі та пріоритетні завдання для реалізації

соціально-справедливого, системного, цілеспрямованого, взаємопов'язаного, циклічного та безперервного процесу, що у взаємодії та синтезі діяльності державних і суспільних інституцій на всіх етапах формування та реалізації політики, досягає суспільно потрібного результату [71, с. 195].

Таким чином, державна політика у сфері захисту критичної інфраструктури – це стратегічні й тактичні вектори роботи органів державної влади та інших уповноважених суб'єктів публічного управління щодо організації та ефективного провадження діяльності стосовно захисту критичної інфраструктури в України, обумовлені об'єктивними умовами суспільно-політичного, економічного розвитку, безпекової ситуації тощо. Попри те, що державна політика поширюється на всю територію України та стосується не лише публічного, а й приватного сектору, її розробка, нормативне оформлення, а також безпосередня реалізація – це предмет роботи органів державної влади різних рівнів, які володіють відповідним колом повноважень і необхідною компетенцією. Тобто йдеться про вираження їх публічної-владної діяльності, пов'язані з якою відносини регламентовані адміністративно-правовими нормами.

Наступним моментом, який виражає адміністративно-правовий характер захисту критичної інфраструктури, слугує монополія державного сектору у формуванні критичної інфраструктури шляхом визначення об'єктів, які до неї належать. Згідно з розділом ІІІ Закону України «Про критичну інфраструктуру» від 16 листопада 2021 року № 1882-IX, віднесення об'єктів до критичної інфраструктури здійснюється в порядку, встановленому Кабінетом Міністрів України (далі – КМУ), а в окремих випадках – Національним банком України та іншими уповноваженими органами державної влади. Віднесення здійснюється за сукупністю критеріїв, що визначають соціальну, політичну, економічну, екологічну значущість таких об'єктів для забезпечення оборони країни, безпеки громадян, суспільства, держави та правопорядку, зокрема для реалізації життєво

важливих функцій і надання життєво важливих послуг, свідчать про існування загроз для них, можливість виникнення кризових ситуацій через несанкціоноване втручання в їх функціонування, припинення функціонування, людський фактор чи природні лиха, тривалість робіт для усунення таких наслідків до повного відновлення штатного режиму [123].

Відповідно до ст. 8 зазначеного Закону, до таких критеріїв належать: 1) виконання об'єктом функцій із забезпечення життєво важливих національних інтересів; 2) існування викликів і загроз, що можуть виникати щодо об'єктів критичної інфраструктури; 3) імовірність завдання значної шкоди нормальним умовам життєдіяльності населення; 4) уразливість таких об'єктів, тяжкість можливих негативних наслідків, внаслідок чого буде заподіяна значна шкода здоров'ю населення (визначається кількістю постраждалих, загиблих та осіб, які отримали значні травми, а також чисельністю евакуйованого населення); соціальній сфері (руйнація систем соціального захисту населення і надання соціальних послуг, втрата спроможності держави задовольнити критичні потреби суспільства); державному суверенітету (зниження обороноздатності, дискредитація іміджу країни, дестабілізація системи державного управління та унеможливлення виконання державою своїх функцій); економіці (вплив на внутрішній валовий продукт, розмір економічних втрат, як прямих, так і непрямих); природним ресурсам загальнодержавного та місцевого значення; 5) масштабність негативних наслідків для держави, які впливають на діяльність стратегічно важливих об'єктів для кількох секторів життєзабезпечення чи призводять до втрати унікальних національно значущих активів, систем і ресурсів, матимуть тривалі наслідки для держави і позначаться на діяльності ряду інших секторів; 6) тривалість ліквідації таких наслідків та дія подальшого негативного впливу на інші сектори держави; 7) вплив на функціонування суміжних секторів критичної інфраструктури [123].

Згідно зі ст. 10 Закону, об’єкти критичної інфраструктури підлягають категоризації. З огляду на це, відбувається визначення рівня вимог щодо забезпечення їх захисту. На сьогодні встановлено такі категорії:

– I категорія критичності – особливо важливі об’єкти, які мають загальнодержавне значення, значний вплив на інші об’єкти критичної інфраструктури та порушення функціонування яких призведе до виникнення кризової ситуації державного значення;

– II категорія критичності – життєво важливі об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації регіонального значення;

– III категорія критичності – важливі об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації місцевого значення;

– IV категорія критичності – необхідні об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації локального значення [123].

Урегульованість діяльності із захисту критичної інфраструктури саме положеннями адміністративного права зумовлює належність останньої до предмета роботи органів державної влади, які власне забезпечують її фактичне провадження. Вони становлять досить значну групу, окрема складова якої – правоохоронні відомства.

Правоохоронні органи поряд з іншими публічно-владними суб’єктами створюють систему захисту критичної інфраструктури, описану та затверджену у своєму складі Законом України «Про критичну інфраструктуру» від 16 листопада 2021 року № 1882-IX. Одним з її ключових учасників є Служба безпеки України (далі – СБУ, СБ України, Служба), яка поряд з іншими відомствами правоохоронного змісту виконує найбільш важливі завдання з боротьби та припинення протиправних дій осіб та груп, що загрожують безпеці об’єктів критичної інфраструктури. Специфіка

діяльності СБУ окреслюється не лише Законом, а й відомчими нормативними документами, такими як Закон України «Про Службу безпеки України» від 25 березня 1992 року № 2229-XII, та низкою інших актів. Про це йдеться в ст. 18 Закону від 16 листопада 2021 року № 1882-IX: «Діяльність Національного банку України, уповноваженого органу у сфері захисту критичної інфраструктури України, центрального органу виконавчої влади, що забезпечує формування державної політики у сфері цивільного захисту, центрального органу виконавчої влади, що реалізує державну політику у сфері цивільного захисту, Служби безпеки України, Національної гвардії України, Національної поліції України, Збройних Сил України, Державної спеціальної служби транспорту та Державної служби спеціального зв'язку та захисту інформації України з питань формування та/або реалізації державної політики у сфері захисту критичної інфраструктури здійснюється в межах, визначених цим Законом, та в порядку, встановленому законами України, що регламентують правові засади організації та діяльності зазначених у цій статті органів» [123; 131].

Підбиваючи підсумки, слід зауважити, що захист об'єктів критичної інфраструктури як об'єкта адміністративно-правового регулювання означений тим, що ця діяльність: по-перше, детермінована обов'язком держави забезпечувати права, свободи, законні інтереси людини та громадянина, а також створювати безпечні для життя та здоров'я нації умови існування; по-друге, організовується та здійснюється у форматі окремої ланки державної політики; по-третє, проводиться щодо об'єктів, віднесення яких до критичної інфраструктури відбувається за волею уповноважених органів державної влади в нормативно встановленому порядку. Крім того, захист критичної інфраструктури належить до предмета діяльності Служби безпеки України, яка покликана протидіяти правопорушенням у цій сфері та слугує одним з правоохоронних органів, що входять до складу системи суб'єктів забезпечення захисту цієї сфери.

1.2. Місце Служби безпеки України в системі суб'єктів забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури

Встановлення ролі та значення Служби безпеки України в процесі реалізації захисту критичної інфраструктури неможливо зробити ізольовано від інших суб'єктів, що забезпечують безпеку і стійкість об'єктів, які до такої інфраструктури належать. Вони становлять розгалужену систему, де кожен має власний набір прав та обов'язків. Крім того, особливості внутрішньої організації останньої мають чітке нормативне закріплення та визначення, що забезпечує комплексність, результативність захисту, а також попереджає проблеми перетинання публічно-владної компетенції.

Так, Закон України «Про критичну інфраструктуру» закріплює таке поняття, як «національна система захисту критичної інфраструктури», що розкрито в такий спосіб: сукупність органів управління, сил і засобів центральних та місцевих органів виконавчої влади (військово-цивільних адміністрацій – у разі утворення), органів місцевого самоврядування, операторів критичної інфраструктури, на які покладається формування та/або реалізація державної політики у сфері захисту критичної інфраструктури. Склад даної системи уточнено в ст. 14 Закону: 1) Кабінет Міністрів України; 2) Апарат Ради національної безпеки і оборони України; 3) Центральна виборча комісія; 4) Національний банк України; 5) Національна комісія з цінних паперів та фондового ринку, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг; 6) Адміністрація Державної служби спеціального зв'язку та захисту інформації України; 7) Фонд державного майна України, інші центральні органи виконавчої влади із спеціальним статусом; 8) уповноважений орган у сфері захисту критичної інфраструктури України;

9) центральний орган виконавчої влади, що забезпечує формування державної політики у сфері цивільного захисту; 9-1) центральний орган виконавчої влади, що реалізує державну політику у сфері цивільного захисту; 10) секторальні та функціональні органи, інші міністерства й центральні органи виконавчої влади; 11) Служба безпеки України; 12) правоохоронні та розвідувальні органи, суб'єкти оперативно-розшукової та контррозвідувальної діяльності; 13) Збройні Сили України, інші військові формування, утворені відповідно до законів України; 14) місцеві органи виконавчої влади (військово-цивільні адміністрації – у разі утворення); 15) органи місцевого самоврядування; 16) оператори критичної інфраструктури; 17) підприємства, установи та організації незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки та стійкості критичної інфраструктури [123].

Отже, СБУ слугує однією з частин об'ємної системи суб'єктів, які відповідають за забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури і володіють відповідним набором повноважень у зазначеній сфері. Причому діяльність Служби поряд з іншими уповноваженими учасниками організовано за чітким переліком рівнів. Цьому питанню присвячено ст. 7 Закону України «Про критичну інфраструктуру», якою установлено та затверджено: 1) загальнодержавний рівень, управління на якому здійснюється Кабінетом Міністрів України, уповноваженим органом у сфері захисту критичної інфраструктури України, органами державної влади відповідно до розподілу повноважень, іншими центральними органами виконавчої влади та державними органами, Національним банком України; 2) регіональний і галузевий рівні, управління на яких здійснюється центральними та місцевими органами виконавчої влади, визначеними в установленому законом порядку відповідальними за забезпечення формування та реалізацію державної політики у сфері захисту критичної інфраструктури в окремому секторі критичної інфраструктури та

відповідальними за функціонування окремих державних систем захисту й реагування; 3) місцевий рівень, управління на якому здійснюється місцевими органами виконавчої влади (військово-цивільними адміністраціями – у разі створення), органами місцевого самоврядування в межах повноважень, покладених на них законодавством; 4) об'єктовий рівень, управління на якому здійснюється оператором критичної інфраструктури на підставі нормативно-правових та регуляторних актів у сфері захисту критичної інфраструктури [123].

Розглянемо більш детально суб'єктів кожного рівня для встановлення місця та ролі серед них Служби безпеки України. Найпершим та найбільш впливовим органом загальнодержавної ланки є КМУ. Згідно з Конституцією та цільовим Законом України «Про Кабінет Міністрів України» від 27 вересня 2014 року № 794-VII, Уряд – це вищий орган виконавчої влади в державі, яку він реалізує безпосередньо, а також через міністерства, інші центральні та місцеві органи виконавчої влади. У своїй діяльності КМУ відповідальний перед Президентом України та парламентом; підконтрольним і підзвітний виключно Верховній Раді України (далі – ВРУ). Уряд становить Прем'єр-міністр України, Перший віцепрем'єр-міністр, віцепрем'єр-міністри, міністри [64; 121].

КМУ виконує широкий спектр завдань, передусім у сфері національної безпеки й оборони, а саме: здійснює заходи щодо забезпечення обороноздатності і національної безпеки України, громадського порядку, боротьби зі злочинністю; забезпечує державний суверенітет і економічну самостійність України, здійснення внутрішньої та зовнішньої політики держави, виконання Конституції і законів України, актів Президента України. Крім того, Уряд: 1) забезпечує реалізацію стратегічного курсу держави на набуття повноправного членства України в Європейському Союзі та в Організації Північноатлантичного договору; 2) вживає заходів щодо забезпечення прав і свобод людини та громадянина; 3) забезпечує

проведення фінансової, цінової, інвестиційної та податкової політики; політики у сферах праці й зайнятості населення, соціального захисту, освіти, науки й культури, охорони природи, екологічної безпеки і природокористування; 4) розробляє та здійснює загальнодержавні програми економічного, науково-технічного, соціального і культурного розвитку України; 5) забезпечує рівні умови розвитку всіх форм власності; здійснює управління об'єктами державної власності відповідно до закону; 6) розробляє проєкт закону про Державний бюджет України і забезпечує виконання затвердженого Верховною Радою України Державного бюджету України, подає Верховній Раді України звіт про його виконання; 7) організовує і забезпечує здійснення зовнішньоекономічної діяльності України, митної справи; 8) спрямовує та координує роботу міністерств, інших органів виконавчої влади; 9) утворює, реорганізовує та ліквідовує відповідно до закону міністерства та інші центральні органи виконавчої влади, діючи в межах коштів, передбачених на утримання органів виконавчої влади; 10) призначає на посади та звільняє з посад за поданням Прем'єр-міністра України керівників центральних органів виконавчої влади, які не входять до складу Кабінету Міністрів України [64; 121].

Безпосередньо як ключовий елемент національної системи захисту критичної інфраструктури КМУ: забезпечує проведення державної політики у сфері захисту критичної інфраструктури України; організовує та забезпечує необхідними силами, засобами й ресурсами функціонування національної системи захисту критичної інфраструктури; визначає уповноважений орган з питань захисту критичної інфраструктури України; забезпечує обмін інформацією та взаємодію інших суб'єктів національної системи захисту; організовує віднесення об'єктів до переліку критичної інфраструктури; забезпечує здійснення заходів із запобігання загрозам безпеці критичної інфраструктури та забезпечення безпеки критичної інфраструктури; забезпечує планування відновлення функціонування критичної

інфраструктури у випадках надзвичайних ситуацій, яким не можна запобігти; забезпечує стійкість критичної інфраструктури до ідентифікованих загроз і небезпек тощо [121; 123].

Крім зазначеного, КМУ спрямовує, координує та контролює роботу наступного суб'єкта досліджуваного рівня – уповноваженого органу у сфері захисту критичної інфраструктури, яким є Державна служба спеціального зв'язку та захисту інформації України (далі – Держспецзв'язку). Її правовий статус затверджено спеціальним Законом України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23 лютого 2006 року № 3475-IV.

Відповідно до ст. 2 Закону, Держспецзв'язку є державним органом, який призначений для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, активної протидії агресії у кіберпросторі, а також інших завдань відповідно до закону. Водночас до переліку основних завдань органу належать: а) участь у формуванні та реалізації державної політики у сферах електронного документообігу в інформаційно-комунікаційних системах, у яких обробляються службова інформація та державна таємниця (у частині захисту інформації державних органів та органів місцевого самоврядування), захисту критичної інформаційної інфраструктури; б) реалізація державної політики щодо захисту критичної технологічної інформації, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснення державного контролю в цих сферах; в) визначення вимог до захисту критичної технологічної інформації, формування загальних вимог до кіберзахисту об'єктів критичної інфраструктури, ведення переліку об'єктів критичної інформаційної інфраструктури, здійснення заходів щодо його оновлення та актуалізації;

г) здійснення контролю за дотриманням вимог законодавства у сферах електронної ідентифікації, електронних довірчих послуг, захисту критичної інформаційної інфраструктури [108].

Більш точну характеристику діяльності Держспецзв'язку як уповноваженого органу у сфері захисту критичної інфраструктури України наведено в ст. 16 Закону України «Про критичну інфраструктуру» від 16 листопада 2021 року № 1882-IX. Так, цей орган забезпечує формування та реалізує державну політику у сфері захисту критичної інфраструктури, здійснює функціональне управління національною системою захисту критичної інфраструктури, забезпечує координацію діяльності міністерств та операторів критичної інфраструктури з питань забезпечення стійкості й захисту об'єктів критичної інфраструктури. Відповідно до покладених законодавством завдань, Держспецзв'язку: 1) координує діяльність міністерств, інших центральних і місцевих органів виконавчої влади (військово-цивільних адміністрацій – у разі утворення) у сфері захисту критичної інфраструктури; 2) узагальнює пропозиції суб'єктів національної системи захисту критичної інфраструктури, формує та веде Реєстр об'єктів критичної інфраструктури (далі – Реєстр); 3) взаємодіє з секторальними, функціональними органами у сфері захисту критичної інфраструктури й операторами критичної інфраструктури з питань забезпечення захисту об'єктів, включених до Реєстру; 4) організовує здійснення оцінки захищеності об'єктів критичної інфраструктури, внесених до Реєстру, аналізує та оцінює загальний стан їх захищеності; 5) проводить оцінку загроз критичній інфраструктурі на національному рівні й оцінку загроз національній безпеці внаслідок реалізації загроз критичній інфраструктурі із залученням секторальних і функціональних органів у сфері захисту критичної інфраструктури; 6) готує щорічну оцінку ризиків та загроз критичній інфраструктурі національного рівня; 7) погоджує проєктні ризики й загрози критичній інфраструктурі секторального рівня; 8) готує

рекомендації щодо визначення вимог до забезпечення захисту та стійкості секторів критичної інфраструктури відповідно до категорій об’єктів критичної інфраструктури; 9) надає пропозиції Кабінету Міністрів України щодо Національного плану захисту та забезпечення стійкості критичної інфраструктури; порядку розроблення, форми та змісту паспорта безпеки об’єкта критичної інфраструктури; порядку розроблення, форми та змісту планів заходів щодо захисту критичної інфраструктури, які приймаються на національному рівні; 10) розробляє та затверджує Проєктні загрози критичній інфраструктурі національного рівня, що становлять інформацію з обмеженим доступом; 11) готує висновки та рекомендації власнику/оператору критичної інфраструктури щодо зміни права власності, цільового призначення чи режиму функціонування об’єкта критичної інфраструктури; 12) забезпечує функціонування системи обміну інформацією між суб’єктами національної системи захисту критичної інфраструктури; 13) створює бази даних щодо загроз і вразливостей критичній інфраструктурі; 14) забезпечує координацію секторальних органів, підготовку пропозицій до проєктів стратегічних документів щодо забезпечення безпеки та стійкості, здійснення захисту критичної інфраструктури – Стратегії національної безпеки України, Стратегії кібербезпеки України та Стратегії громадської безпеки та цивільного захисту України; 15) бере участь у розробленні нової галузі знань, програм навчання, підвищення кваліфікації, робочих і навчальних програм з питань забезпечення стійкості та захисту критичної інфраструктури; 16) здійснює міжнародне співробітництво, забезпечує дотримання та виконання зобов’язань, взятих відповідно до міжнародних договорів України з питань захисту критичної інфраструктури, налагоджує та підтримує зв’язки з міжнародними організаціями, іноземними державами, їх правоохоронними органами і спеціальними службами тощо [123].

На відміну від КМУ та Держспецзв'язку, наступні два суб'єкти загальнодержавного рівня організації захисту критичної інфраструктури не належать до органів виконавчої влади та не знаходяться у взаємному зв'язку чи підпорядкуванні. Наприклад, Національний банк України, відповідно до Закону України «Про Національний банк України», є центральним банком України, особливим центральним органом державного управління, юридичний статус, завдання, функції, повноваження і принципи організації якого визначаються Конституцією України та законодавством. Відповідно до Конституції, основною функцією Національного банку є забезпечення стабільності грошової одиниці України. Паралельно з викладеним Національний банк України: а) забезпечує формування та ведення переліку об'єктів критичної інфраструктури, а також реєстру об'єктів критичної інформаційної інфраструктури в банківській системі України та на ринках небанківських фінансових послуг, державне регулювання і нагляд за діяльністю на яких здійснює Національний банк, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг, визначає критерії та порядок віднесення об'єктів у банківській системі України та на ринках небанківських фінансових послуг, державне регулювання та нагляд за діяльністю на яких здійснює Національний банк, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг до об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури, встановлює вимоги до проведення аудиту інформаційної безпеки в банківській системі України та на ринках небанківських фінансових послуг, державне регулювання та нагляд за діяльністю на яких здійснює Національний банк, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг; б) забезпечує формування та реалізацію державної політики у сфері захисту критичної інфраструктури щодо банків, інших осіб, що здійснюють діяльність на

ринках небанківських фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг відповідно до закону, що визначає правові та організаційні засади функціонування і захисту критичної інфраструктури [125].

Наступним органом є Апарат Ради національної безпеки і оборони України (далі – РНБО). Згідно з цільовим Законом України «Про Раду національної безпеки і оборони України» від 5 березня 1998 року № 183/98-ВР, РНБО – це координаційний орган з питань національної безпеки і оборони при Президентові України. Функціями Ради національної безпеки і оборони України є: 1) внесення пропозицій Президентові України щодо реалізації засад внутрішньої і зовнішньої політики у сфері національної безпеки і оборони; 2) координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони в мирний час; 3) координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони в умовах воєнного або надзвичайного стану та в разі виникнення кризових ситуацій, що загрожують національній безпеці України [130].

Своєю чергою Апарат Ради національної безпеки і оборони України – це державний орган, який здійснює поточне інформаційно-аналітичне та організаційне забезпечення діяльності РНБО (Указ Президента України «Питання Апарату Ради національної безпеки і оборони України» від 14 жовтня 2005 року № 1446/2005). У межах своєї діяльності Апарат: 1) готує матеріали для розгляду на засіданнях Ради, проєкти рішень Ради, указів Президента України про введення в дію відповідних рішень Ради, інших актів Президента України з питань національної безпеки і оборони, доручень Голови Ради національної безпеки і оборони України членам Ради, пов’язані з виконанням покладених на неї функцій; 2) забезпечує здійснення контролю за станом виконання рішень Ради, актів та доручень Президента України,

контроль за виконанням яких покладено на Секретаря Ради національної безпеки і оборони України; 3) готує для розгляду Радою питання щодо організації роботи з виявлення загроз національним інтересам і національній безпеці, визначення шляхів та засобів їх відвернення та нейтралізації, щодо пріоритетів державної політики у сфері національної безпеки і оборони; 4) бере участь у розробленні проєктів нормативно-правових актів, міжнародних договорів та інших документів з питань національної безпеки і оборони; 5) готує в установленому порядку висновки щодо проєктів нормативно-правових актів з питань національної безпеки і оборони; 6) вивчає та аналізує діяльність Збройних Сил України та інших військових формувань, утворених відповідно до законів України, їх готовність до виконання покладених на них завдань, здійснення правоохоронними органами заходів щодо профілактики і боротьби зі злочинністю; 7) аналізує стан забезпечення національної безпеки, зокрема щодо матеріальних, фінансових, кадрових, організаційних аспектів, готує відповідні пропозиції; 8) опрацьовує пропозиції щодо вдосконалення системи забезпечення національної безпеки та організації оборони, утворення, реорганізації та ліквідації органів виконавчої влади у цій сфері; 9) аналізує стан виконання законодавства з питань національної безпеки і оборони, готує пропозиції щодо його вдосконалення; 10) готує пропозиції щодо утворення тимчасових міжвідомчих комісій, робочих та консультативних органів Ради і таке інше [98].

Аналіз загальнодержавного рівня забезпечення безпеки та стійкості функціонування об’єктів критичної інфраструктури засвідчує, що суб’єкти цієї ланки виконують широкі функції та відповідають за реалізацію глобальних цілей, пов’язаних із формуванням і проведенням державної політики у сфері критичної інфраструктури; визначенням об’єктів, які належать до системи останньої; здійсненням координації та управління іншими суб’єктами захисту, а також організацією їх взаємодії; розробленням

та затвердженням стратегічних документів, пов’язаних із проведенням заходів захисту тощо.

Регіональний та галузевий рівні є цариною діяльності секторальних і функціональних органів державної влади, задіяних до захисту критичної інфраструктури. Для того, щоб зрозуміти принцип роботи цих ланок, доречно звернутися до ст. 9 Закону України «Про критичну інфраструктуру», відповідно до якої для організації ефективного забезпечення безпеки та стійкості критичної інфраструктури з урахуванням специфіки забезпечення окремих життєво важливих функцій та/або послуг визначаються сектори критичної інфраструктури. Формування та реалізацію державної політики у відповідних секторах здійснюють секторальні органи у сфері захисту критичної інфраструктури [123].

Відповідно до п. 22 ч. 1 ст. 1 Закону України «Про критичну інфраструктуру», секторальний орган у сфері захисту критичної інфраструктури – це державний орган, визначений законодавством відповідальним за забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури в окремому секторі критичної інфраструктури. Згідно зі ст. 19 Закону, у своїй діяльності останні: 1) створюють у межах штатної чисельності у своєму складі структурні підрозділи з питань захисту критичної інфраструктури; 2) збирають, узагальнюють і здійснюють попередній аналіз даних щодо критичної інфраструктури та її функціонування; 3) спільно з операторами критичної інфраструктури здійснюють категоризацію об’єктів критичної інфраструктури своїх секторів критичної інфраструктури, формують секторальні переліки об’єктів критичної інфраструктури, подають інформацію до Реєстру; 4) розробляють і затверджують: а) вимоги до захисту об’єктів критичної інфраструктури відповідно до їх категорій; б) проєктні загрози критичній інфраструктурі секторального рівня; в) плани взаємодії функціональних органів у сфері захисту критичної інфраструктури у

відповідних секторах для всіх режимів функціонування критичної інфраструктури; плани взаємодії та підтримання життєво важливих функцій на випадок порушення функціонування об'єктів критичної інфраструктури; 5) розробляють і впроваджують норми та регламенти захисту критичної інфраструктури у відповідних секторах критичної інфраструктури; 6) затверджують проєктні загрози критичній інфраструктурі об'єктового рівня у відповідних секторах; 7) погоджують паспорти безпеки об'єктів критичної інфраструктури, надані операторами у відповідних секторах; 8) здійснюють: а) перевірку й оцінку захищеності об'єктів критичної інфраструктури; б) підготовку пропозицій до проєктних ризиків і загроз критичній інфраструктурі національного рівня та щорічної оцінки ризиків і загроз критичній інфраструктурі національного рівня; в) організацію системи підготовки персоналу, навчання та тренувань щодо забезпечення стійкості та захисту секторів критичної інфраструктури; г) підготовку щорічного звіту щодо забезпечення захисту критичної інфраструктури у відповідному секторі; д) участь у встановленому законодавством порядку в реагуванні на кризові ситуації, пов'язані з безпекою, захистом і стійкістю об'єктів критичної інфраструктури, а також у створенні умов для належного виконання правоохоронними, розвідувальними та контррозвідувальними органами своїх завдань щодо захисту критичної інфраструктури тощо [123].

Закріплення державних органів за секторами врегульовано постановою КМУ «Деякі питання об'єктів критичної інфраструктури» від 9 жовтня 2020 року № 1109. Документ визначає 23 сектори критичної інфраструктури та закріплює за кожним із них відповідальний орган державної влади. Наприклад, захист критичної інфраструктури в секторі громадської безпеки здійснюється Міністерством внутрішніх справ (далі – МВС), яке проводить охорону публічного (громадського) порядку, охорону об'єктів критичної інфраструктури на договірних засадах; оперативне цілодобове невідкладне реагування на екстрені комунікації, їх оброблення, зберігання та передачу

інформації про такі комунікації для надання екстреної допомоги населенню. У межах впливу МВС також знаходиться сектор цивільного захисту й територій, що передбачає реагування на надзвичайні ситуації, проведення аварійно-рятувальних та інших невідкладних робіт з ліквідації наслідків надзвичайних ситуацій, надання допомоги постраждалим. Іншим прикладом слугує Міністерство оборони України, яке забезпечує захист критичної інфраструктури в секторі оборони [32].

Своєю чергою, функціональні органи у сфері захисту критичної інфраструктури – це державні органи, визначені відповідальними за функціонування окремих державних систем захисту й реагування. Зазначені органи наділені такими повноваженнями: 1) беруть участь у встановленому законодавством порядку в реагуванні на кризові ситуації, пов'язані із забезпеченням безпеки та стійкості критичної інфраструктури; 2) готують пропозиції щодо включення об'єктів інфраструктури до Реєстру; 3) формують перелік об'єктів критичної інфраструктури, що належать до сфери їх управління; 4) надають власникам та операторам інфраструктури консультації щодо ризиків і загроз критичній інфраструктурі та заходів щодо їх нейтралізації; 5) здійснюють іншу діяльність для забезпечення стійкості та захисту критичної інфраструктури в межах повноважень, що регулюють діяльність суб'єктів захисту критичної інфраструктури, зокрема: організовують проведення оцінки загроз та ризиків критичній інфраструктурі у відповідних сферах; беруть участь у проведенні оцінки загроз і ризиків критичній інфраструктурі на загальнодержавному рівні; формують пропозиції щодо національних та секторальних проєктних ризиків і загроз; забезпечують організацію взаємодії та обміну інформацією з іншими суб'єктами національної системи захисту критичної інфраструктури; здійснюють моніторинг рівня безпеки об'єктів критичної інфраструктури у відповідних сферах (Закон України «Про критичну інфраструктуру» від 16 листопада 2021 року № 1882-IX) [123].

Законодавство у сфері критичної інфраструктури не надає перелік функціональних органів, однак частково зазначений момент освітлено в проєкті наказу Міністерства розвитку громад та територій України від 2025 року, яким визначено план взаємодії функціональних органів у сфері захисту критичної інфраструктури. Статусом «функціональний» проєкт наділяє Державну прикордонну службу, Національну гвардію України, Державну службу України з надзвичайних ситуацій та, що вкрай важливо для нашого дослідження, Службу безпеки України [101]. Аналогічно СБУ описано в положеннях постанови КМУ «Деякі питання паспортизації об'єктів критичної інфраструктури» від 4 серпня 2023 року № 818 [33]. Як відомство публічної влади та функціональний суб'єкт забезпечення безпеки і стійкості роботи об'єктів критичної інфраструктури СБУ, згідно із Законом України «Про Службу безпеки України» від 25 березня 1992 року № 2229-XII, – це державний орган спеціального призначення з правоохоронними функціями, який забезпечує державну безпеку України [131].

Систему Служби безпеки України становлять Центральне управління Служби безпеки України, підпорядковані йому регіональні органи, органи військової контррозвідки, військові формування, а також навчальні, науково-дослідні та інші заклади Служби безпеки України. Центральне управління СБУ, інші органи й установи, що входять у систему Служби, є юридичними особами, мають печатку із зображенням державного герба України та своїм найменуванням, інші печатки і штампи, рахунки в банках, зокрема валютні [131].

Для виконання покладених завдань Служба безпеки України може встановлювати контакти з органами безпеки іноземних держав і взаємодіяти з ними на підставі норм міжнародного права, відповідних договорів та угод. Крім того, СБУ взаємодіє з Управлінням охорони вищих посадових осіб України, правоохоронними та митними органами у порядку і на засадах, визначених законами, указами Президента України та прийнятими на їх

основі актами Служби безпеки України і відповідного відомства [131]. На СБУ покладають значний спектр повноважень, однак безпосередньо в галузі захисту критичної інфраструктури Служба здійснює попередження, виявлення, припинення та розкриття злочинів технологічного тероризму, запобігання вчиненню терористичних актів з використанням небезпечних хімічних речовин, диверсій у суб'єктів господарювання хімічної промисловості та на об'єктах критичної інфраструктури [131].

Таким чином, суб'єкти забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури другого, регіонально-галузевого, рівня – це основний масив публічних відомств, які реалізують заходи й інструменти спрямовані на: а) забезпечення роботи об'єктів критичної інфраструктури за встановленими законодавством секторами; б) прогнозування та виявлення потенційно наявних загроз їх безпеці, а також реагування на порушення та протиправні дії відносно вказаних об'єктів. У цій групі СБУ – це спеціальний функціональний, правоохоронний орган, предметом діяльності якого є боротьба із суспільно небезпечними діями окремих осіб та/або їх груп, вчинюваних на об'єктах критичної інфраструктури та відносно них, що становить ризики національній безпеці [84].

Останні два рівні, місцевий та об'єктовий, виражено в діяльності державних адміністрацій як місцевих органів виконавчої влади, органів місцевого самоврядування та операторів критичної інфраструктури. Так, суб'єкти місцевого значення, відповідно до Закон України «Про критичну інфраструктуру» від 16 листопада 2021 року № 1882-IX, а саме місцеві органи виконавчої влади (військово-цивільні адміністрації – у разі утворення) у сфері захисту критичної інфраструктури забезпечують: 1) розроблення та затвердження місцевих програм забезпечення безпеки і стійкості критичної інфраструктури, програм підвищення стійкості територіальних громад до кризових ситуацій, викликаних припиненням або

погіршенням надання важливих для їх життєдіяльності послуг чи для здійснення життєво важливих функцій; 2) розроблення, затвердження та погодження із заінтересованими органами: а) місцевих планів взаємодії залучених суб'єктів у кризовій ситуації з метою підтримання життєво важливих функцій та надання життєво важливих послуг, планів відновлення функціонування критичної інфраструктури; б) програм навчання населення для забезпечення захисту в разі виникнення режиму реагування на виникнення кризової ситуації та режиму відновлення штатного функціонування [123].

Своєю чергою органи місцевого самоврядування, згідно із Законом України «Про місцеве самоврядування», вживають необхідних заходів щодо захисту критичної інфраструктури, відновлення функціонування важливих державних об'єктів національної економіки, об'єктів критичної інфраструктури та об'єктів, які забезпечують життєдіяльність населення, підвищення стійкості громад до кризових ситуацій, викликаних припиненням або погіршенням надання важливих для їх життєдіяльності послуг чи припиненням здійснення життєво важливих функцій [124].

Що стосується об'єктового рівня, то його представленого операторами критичної інфраструктури, яких Закон України «Про критичну інфраструктуру» визначає таким чином: «Юридична особа будь-якої форми власності та/або фізична особа – підприємець, що на правах власності, оренди або на інших законних підставах здійснює управління об'єктом критичної інфраструктури та відповідає за його поточне функціонування». Відповідно до ст. 21 Закону, основними завданнями операторів критичної інфраструктури є: 1) забезпечення захисту об'єктів критичної інфраструктури, зокрема створення, налагодження та підтримання функціонування ефективної системи фізичної безпеки, безпеки операційних систем і кібербезпеки; 2) розроблення, оновлення та забезпечення виконання об'єктових планів заходів щодо забезпечення безпеки і стійкості критичної

інфраструктури, правил управління ризиками безпеки, планів локалізації та ліквідації наслідків аварій, а також заходів кіберзахисту; 3) проведення оцінки ризиків на об'єктах критичної інфраструктури й обмін інформацією про ризики та загрози з іншими суб'єктами національної системи захисту критичної інфраструктури, а також створення умов для належного виконання правоохоронними, розвідувальними та контррозвідувальними органами своїх завдань щодо захисту критичної інфраструктури; 4) створення окремого структурного підрозділу або визначення відповідальної особи за організацію захисту критичної інфраструктури та забезпечення постійного зв'язку з відповідними суб'єктами національної системи захисту критичної інфраструктури; 5) оперативне реагування на протиправні дії, фізичні атаки, спрямовані на відключення або пошкодження роботи операційних систем чи систем забезпечення фізичної безпеки об'єкта критичної інфраструктури тощо [123].

Таким чином, Служба безпеки України має досить вузьке спрямування діяльності у сфері забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури. СБУ є спеціалізованим правоохоронним органом, уповноваженим протидіяти загрозам, що мають підвищений рівень публічної небезпеки та здатні завдати шкоди не лише окремим об'єктам критичної інфраструктури, а й життєво важливим інтересам суспільства й держави загалом. Саме комплексний характер цих загроз, які можуть зачіпати безпеку населення, суверенітет і конституційний лад, зумовлює унікальне місце СБУ в системі суб'єктів забезпечення безпеки та стійкості функціонування досліджуваної сфери, а її повноваження дозволяють не лише реагувати на посягання та різноманітні загрози, а й здійснювати превентивний вплив, формуючи ключову ланку державного механізму захисту критично важливих об'єктів [84].

1.3. Завдання, принципи й нормативні засади забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури Службою безпеки України

Забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури Службою безпеки України є складним процесом, реалізація якого передбачає вирішення нею низки завдань і виконання низку функцій. Етимологічно термін «завдання» – це: а) наперед визначений, запланований для виконання обсяг роботи, справа і таке інше; б) мета, до якої прагнуть; те, що хочуть здійснити; в) наказ виконати що-небудь в умовах воєнних дій; г) настанова, розпорядження виконати певне доручення тощо [147]. З огляду на це, завдання забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури Службою безпеки України – це сукупність мікроцілей діяльності СБУ, її органів і підрозділів у сфері захисту об'єктів критичної інфраструктури від злочинних посягань окремих осіб та груп, що становлять небезпеку національним інтересам і суспільству.

Законом України «Про Службу безпеки України» на СБУ покладається захист державного суверенітету, конституційного ладу, територіальної цілісності, науково-технічного й оборонного потенціалу України, законних інтересів держави та прав громадян від розвідувально-підривної діяльності іноземних спеціальних служб, посягань з боку окремих організацій, груп та осіб, а також забезпечення охорони державної таємниці. До завдань Служби безпеки України також входить попередження, виявлення, припинення та розкриття кримінальних правопорушень проти миру й безпеки людства, тероризму та інших протиправних дій, які безпосередньо створюють загрозу життєво важливим інтересам України [131].

Безпосередньо завдання щодо захисту критичної інфраструктури Законом України «Про критичну інфраструктуру» не визначаються як для СБУ, так і інших публічних органів. Водночас документ описує мету й цілі

державної політики у вказаній сфері, на що варто звернути увагу. Згідно зі ст. 5 Закону, мета останньої полягає в забезпеченні безпеки об'єктів критичної інфраструктури, запобіганні виявам несанкціонованого втручання в їх функціонування, прогнозуванні та запобіганні кризовим ситуаціям на об'єктах критичної інфраструктури. Своєю чергою до завдань державної політики Законом віднесено такі: 1) запобігання виявам несанкціонованого втручання в її функціонування, прогнозування та запобігання кризовим ситуаціям на об'єктах критичної інфраструктури; 2) попередження кризових ситуацій, що порушують безпеку критичної інфраструктури; 3) створення, впровадження, розвиток та забезпечення функціонування національної системи захисту критичної інфраструктури, зокрема шляхом визначення уповноваженого органу у сфері захисту критичної інфраструктури України, а також визначення повноважень у сфері захисту критичної інфраструктури інших суб'єктів національної системи захисту критичної інфраструктури; 4) розроблення нормативно-правової та нормативно-технічної бази з питань забезпечення безпеки об'єктів критичної інфраструктури; 5) розроблення та реалізація державних цільових програм із захисту критичної інфраструктури; 6) розроблення комплексу заходів з контролю за ризиками безпеки, виявлення, запобігання та ліквідації наслідків інцидентів безпеки на об'єктах критичної інфраструктури; 7) встановлення обов'язкових вимог із забезпечення безпеки об'єктів критичної інфраструктури, їх захищеності на всіх етапах життєвого циклу, зокрема під час створення, прийняття в експлуатацію, модернізації; 8) аналіз викликів та загроз, що впливають на стійкість критичної інфраструктури, оцінка стану її захищеності; 9) розроблення методології аналізу результативності державної політики у сфері захисту критичної інфраструктури; 10) підготовка, перепідготовка, підвищення кваліфікації, тренування працівників національної системи захисту критичної інфраструктури; 11) забезпечення взаємодії національної

системи захисту критичної інфраструктури з відповідними міжнародними системами, насамперед європейськими та євроатлантичними [123].

Звернутися також варто до цілей, викладених у розпорядженні КМУ «Про схвалення Концепції створення державної системи захисту критичної інфраструктури» від 6 грудня 2017 року № 1009-р. Так, Концепцією передбачено, що створення державної системи захисту критичної інфраструктури спрямоване на забезпечення стійкості критичної інфраструктури до загроз усіх видів, включаючи загрози природного й техногенного характеру, загрози, спричинені протиправними діями, та інші загрози. Поставлена мета передбачає розв'язання уповноваженими суб'єктами таких проблем: 1) унормування технічних вимог щодо будівництва та експлуатації об'єктів критичної інфраструктури із забезпеченням їх стійкого функціонування у різних режимах функціонування критичної інфраструктури; 2) розбудова державно-приватного партнерства у сфері захисту критичної інфраструктури для підвищення безпеки та забезпечення стійкості критичної інфраструктури з визначенням зобов'язань держави та власників (розпорядників) об'єктів критичної інфраструктури; 3) налагодження обміну інформацією між суб'єктами державної системи захисту критичної інфраструктури про загрози критичній інфраструктурі, характеристики систем захисту об'єктів критичної інфраструктури, механізми і процедури реагування на загрози; 4) розроблення і затвердження єдиної методології проведення оцінки загроз критичній інфраструктурі; розроблення переліку об'єктів критичної інфраструктури; 5) збір, аналіз та узагальнення даних щодо об'єктів критичної інфраструктури та їх функціонування; 6) обмін інформацією, а також постійний моніторинг стану безпеки об'єктів критичної інфраструктури; 7) участь в установленому законодавством порядку в реагуванні на кризові ситуації, пов'язані з виникненням загроз критичній інфраструктурі, та забезпеченні захисту і стійкості критичної інфраструктури; 8) здійснення завчасного інформування

(попередження про загрози) власників (розпорядників) об’єктів критичної інфраструктури та надання інформаційної, консультативної, експертної, технологічної допомоги власникам (розпорядникам) об’єктів критичної інфраструктури, користувачам їх послуг (населенню) з метою запобігання виникненню, реагування, мінімізації можливого впливу загроз тощо [132].

За відсутності окремого конкретизованого підходу вважаємо, що завдання забезпечення безпеки та стійкості функціонування об’єктів критичної інфраструктури Службою безпеки України – це комбінація цілей, які виконуються цим органом особливого призначення в його поточній діяльності та безпосередньо як суб’єктом національної системи захисту критичної інфраструктури. З огляду на закони України «Про Службу безпеки України», «Про критичну інфраструктуру», а також інші нормативні документи, можна виокремити такі завдання [83]:

– участь у реалізації в межах визначеної Законом України «Про Службу безпеки України» та іншими відомчими документами компетенції мети та завдань державної політики у сфері захисту об’єктів критичної інфраструктури;

– здійснення у встановленому законодавством порядку попередження, профілактики, виявлення, розкриття та розслідування злочинів, які належать до підслідності органів СБУ та вчинені на об’єктах критичної інфраструктури або стосовно них;

– організація та проведення заходів, спрямованих на боротьбу з тероризмом, диверсіями, зокрема з використанням інформаційних і цифрових технологій на об’єктах критичної інфраструктури;

– виявлення осіб, організованих злочинних груп та злочинних організацій, діяльність яких спрямована на порушення безпеки об’єктів критичної інфраструктури, перешкоджання їх нормальній роботі, а також забезпечення притягнення цих осіб до встановленої законом міри юридичної відповідальності;

– організаційне, матеріально-технічне, кадрове, фінансово-господарське та інше забезпечення діяльності органів і підрозділів СБУ, задіяних у забезпеченні безпеки та захисті об’єктів критичної інфраструктури від злочинів, віднесених до її підслідності [83];

– систематична оцінка ризиків, моніторинг наявних загроз критичній інфраструктури держави з огляду на умови об’єктивної дійсності політичного, економічного, військового та іншого змісту, а також планування заходів протидії таким загрозам, мінімізації їх негативного впливу;

– організація та забезпечення системної взаємодії між органами, підрозділами Служби безпеки України та іншими суб’єктами національної системи захисту критичної інфраструктури з питань обміну інформацією, планування спільних профілактичних заходів, реагування на загрози безпеки функціонування об’єктів критичної інфраструктури [83];

– забезпечення захисту відомостей, що становлять державну таємницю у сфері роботи об’єктів критичної інфраструктури, а саме нерозголошення інформації про організацію, стан, планування та здійснення заходів із захисту та забезпечення безпеки та стійкості об’єктів критичної інфраструктури з І та ІІ категорій критичності, включаючи створення резервів необхідних ресурсів для реагування на кризові ситуації та ліквідації їх наслідків на об’єктах критичної інфраструктури (Закон України «Про державну таємницю» від 21 січня 1994 року № 3855-XII) [83; 109].

Практична реалізація завдань СБУ в галузі забезпечення безпеки та стійкості функціонування об’єктів критичної інфраструктури відбувається з обов’язковим урахуванням і дотриманням певних принципів. Слово «принцип» (від лат. «principium» – першооснова, джерело) в українській мові тлумачать так: 1) вихідне положення теорії, системи, наукового напряму; 2) засада, основний закон, правило точної науки; 3) особливість, що слугує основою створення чого-небудь, спосіб створення певного об’єкта; 4) спосіб реалізації завдання; 5) основа діяльності установи, підприємства, організації

тощо; 6) переконання, канон, норма; 7) керівна ідея будь-якої діяльності чи процесу, першоджерело та основне правило функції [92]. У своєму монографічному дослідженні В. В. Чумак зауважує, що принципами є головні положення науки чи будь-якої практичної діяльності, а також правила оцінювання її результатів. Автор стверджує: «Принципи пов'язують між собою сукупність категорій, які знаходяться у взаємозв'язках між собою. Принцип є ланцюгом, який пов'язує закономірності й діяльність» [169, с. 32].

У теорії державного управління В. Д. Бакуменко принципи характеризує як вияви закономірностей у державному управлінні, що відображені у вигляді певних положень, які застосовуються в теоретичній і практичній діяльності людей у сфері державного управління. Дослідник зауважує, що зазвичай це – фундаментальні, науково обґрунтовані, а в певних випадках і законодавчо закріплені положення, відповідно до яких будується та функціонує система державного управління [43, с. 564]. Своєю чергою Н. Р. Нижник вважає, що принципи державного управління – це об'єктивні закономірності й відносини суспільно-політичної природи, що визначають зміст, організаційну структуру та життєдіяльність компонентів державного управління. Вони сформульовані у вигляді певних наукових положень, що закріплені правом і застосовуються в теоретичній і практичній державно-управлінській діяльності [90, с. 162].

У правовій галузі питання сутності принципів має дискусійний характер. На думку авторів «Юридичної енциклопедії», ідеться про основні засади, вихідні ідеї, що характеризуються універсальністю, загальною значущістю, вищою імперативністю та відображають суттєві положення теорії, вчення, науки, системи внутрішнього й міжнародного права, політичної, державної чи громадської організації (гуманізм, законність, справедливість, рівність громадян перед законом тощо) [175, с. 110–111]. Водночас В. Ф. Погорілко та В. Л. Федоренко пропонують розкривати принципи як керівні засади, ідеї, ідеали, що визначають сутність, зміст,

спрямованість і форми правового регулювання, та виокремлюють загальні, тобто керівні засади, ідеї, а іноді й завдання права [5; 103, с. 16–17]. У дисертаційній роботі О. М. Руднєвої йдеться про те, що принципи – це головні чинники, що визначають найважливіші структурні зв'язки у предметі, методі, механізмі правового регулювання всередині правової системи й поза нею (зв'язки із соціальним середовищем), які отримують офіційне та навіть неофіційне відображення в праві. «Як регулятори суспільних відносин, вони мають також і загальну цілеспрямованість, адже здебільшого визначають перспективи розвитку не лише права, а й суспільства, держави і тим самим сприяють усуненню прогалин або ж інших недоліків чинного законодавства», – зауважує авторка, спираючись на дослідження розуміння принципів у юридичних джерелах [139, с. 75]. Натомість Т. І. Фулей зводить зміст принципів до двох ключових концепцій: 1) принципи права – це основоположні ідеї; 2) це – нормативні засади права, що визначають сутність і спрямованість правового регулювання [164, с. 9].

Одне з найбільш комплексних досліджень правових принципів провів А. М. Колодій, який у своїй монографії визначив не лише поняття, а й основний масив ознак, притаманний цій категорії. Науковець обґрунтовує такий висновок: принципи права – це такі вихідні ідеї існування права, які виражають найважливіші закономірності й підвалини вказаного типу держави та права, є однопорядковими із сутністю права і становлять його головні риси, вирізняються універсальністю, вищою імперативністю та загальнозначущістю, відповідають об'єктивній необхідності побудови і зміцнення певного суспільного ладу. Учений вважає, що саме принципи права спрямовують і надають синхронності всьому механізму правового регулювання суспільних відносин, найбільш досконало, порівняно з іншими, розкривають місце права в суспільному житті та його розвитку. Вони є критерієм законності й правомірності дій громадян і посадових осіб, адміністративного апарату та органів юстиції і за певних умов мають

важливе значення для зростання правосвідомості населення, його культури й освіти. Отже, принципи підлягають системному аналізу в їх динаміці та статиці. Становлячи головний зміст права, юридичні принципи отримують усі його властивості і функції, а це означає, що: а) вони нормативно-регулятивні, загальні, обов'язкові, об'єктивно обумовлені, історичні та ідейно-політичні категорії; б) їх соціальною функцією є регулювання та охорона суспільних відносин; в) вони є самостійною юридичною категорією, тобто мають ознаки, відокремлюючи їх від усіх інших категорій [60, с. 27].

Таким чином, зазначене вище дає змогу дійти висновку, що принципи забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури Службою безпеки України – це нормативно закріплені та засновані на загальновизнаних цінностях і призначенні права, базові юридичні засади, які визначають зміст, організацію та порядок діяльності Служби безпеки України щодо запобігання загрозам, охорони й підтримання стабільного функціонування об'єктів критичної інфраструктури. Як і у випадку із завданнями, принципи діяльності СБУ як частини національної системи захисту критичної інфраструктури не віднайшли класифікації в законодавстві. У своїй поточній роботі органи та підрозділи СБ України, відповідно до Закону України «Про Службу безпеки України» від 25 березня 1992 року № 2229-XII, керуються принципами законності, поваги до прав і гідності особи, позапартійності, відповідальності перед народом України, поєднання єдиноначальності й колегіальності, гласності і конспірації [131].

Закон України «Про критичну інфраструктуру» від 16 листопада 2021 року № 1882-IX визначає перелік основних принципів державної політики в зазначеній сфері, який охоплює: 1) визнання необхідності забезпечення безпеки та стійкості критичної інфраструктури; 2) визначення законодавчих вимог до принципів, пріоритетів, стратегічних завдань, підходів щодо захисту критичної інфраструктури; 3) визначення суб'єктів національної системи захисту критичної інфраструктури, їх повноважень і

засад відповідальності, порядку взаємодії; 4) створення умов та впровадження заходів, спрямованих на ефективне зниження і контроль за ризиками безпеки, на зниження ризику реалізації можливих загроз, ліквідацію та/або мінімізацію наслідків реалізованих загроз, кризових ситуацій та інших їх видів; 5) створення системи раннього виявлення загроз критичній інфраструктурі; 6) запровадження державно-приватного партнерства, взаємодії суб'єктів господарювання та населення з питань забезпечення захисту та стійкості критичної інфраструктури; 7) забезпечення міжнародного співробітництва у сфері захисту критичної інфраструктури; 8) створення умов швидкого відновлення надання життєво важливих функцій та послуг у разі реалізації загроз і порушення функціонування критичної інфраструктури [123].

На нашу думку, систему принципів діяльності Служби безпеки України як суб'єкта забезпечення безпеки і стійкості функціонування об'єктів критичної інфраструктури становлять такі вихідні ідеї [86]:

– принципи законності та верховенства права. Згідно зі ст. 8 Конституції, «в Україні визнається і діє принцип верховенства права. Конституція України має найвищу юридичну силу. Закони та інші нормативно-правові акти приймаються на основі Конституції України і повинні відповідати їй. Норми Конституції України є нормами прямої дії. Звернення до суду для захисту конституційних прав і свобод людини і громадянина безпосередньо на підставі Конституції України гарантується» [64]. У контексті нашого дослідження принцип верховенства права та законності закріплює вимоги щодо обов'язковості відповідності діяльності органів і підрозділів Служби безпеки України стосовно захисту критичної інфраструктури наявним юридичним положенням, а також використання лише тих адміністративних, кримінально-процесуальних та інших інструментів роботи, які відповідають компетенції і повноваженням останніх;

– принцип забезпечення та дотримання прав та свобод людини і громадянина. Досить детально зміст цієї вихідної засади окреслено в ст. 5 Закону України «Про Службу безпеки України» від 25 березня 1992 року № 2229-XII. У документі закріплено положення про те, що діяльність СБУ здійснюється на основі дотримання прав і свобод людини. Органи та співробітники Служби безпеки України мають поважати гідність людини, виявляти до неї гуманне ставлення, не допускати розголошення відомостей про особисте життя людини. У виняткових випадках з метою припинення та розкриття державних злочинів окремі права та свободи особи можуть бути тимчасово обмежені в порядку й межах, визначених Конституцією та законами України. Неправомірне обмеження законних прав і свобод людини є неприпустимим та тягне за собою відповідальність згідно із законодавством. Орган Служби безпеки України в разі порушення його співробітниками під час виконання службових обов'язків прав чи свобод людини повинен вжити заходів щодо поновлення цих прав і свобод, відшкодування заподіяної моральної та матеріальної шкоди, притягнення винних до відповідальності [131]. Таким чином, відповідно до вимог наведеного принципу, діяльність органів, підрозділів і кожного окремого працівника Служби безпеки України, навіть в аспекті протидії таким негативним явищам, як тероризм, та іншим злочинам на особливо важливих для суспільства й держави об'єктах критичної інфраструктури, не може відбувається з порушенням прав, свобод і законних інтересів людини та громадянина. СБУ має право обмежувати права та свободи, але виключно у встановлених законодавством випадках для досягнення поставлених цілей, дотримуючись вимог формалізованої процедури. Будь-які інші дії поза дотримання цього правила матимуть протиправний і караний характер [86];

– принцип координованості та взаємодії. Зазначена вихідна засада пов'язана з належністю СБУ до загальнонаціональної системи захисту об'єктів критичної інфраструктури. Відповідно до цього, реалізація Службою

своїх завдань і функцій повинно органічно поєднуватись із цілями державної політики, а також враховувати настанови координаційних органів вищого, загальнонаціонального рівня управління сектором критичної інфраструктури. Крім того, у процесі забезпечення безпеки і стійкості роботи об'єктів останньої СБУ діє у співпраці з іншими публічними органами, поєднуючи сили й засоби, обмінюючись інформацією та відомостями, здійснюючи спільний моніторинг загроз тощо. Про це власне йдеться в ст. 8 Закону України «Про Службу безпеки України»: «Служба безпеки України взаємодіє з державними органами, підприємствами, установами, організаціями та посадовими особами, які сприяють виконанню покладених на неї завдань. Громадяни України та їх об'єднання, інші особи сприяють законній діяльності Служби безпеки України на добровільних засадах» [131];

– принцип гнучкості й адаптивності до змін. Бурхливий технологічний розвиток людства суттєво позначається на загрозах об'єктам критичної інфраструктури, які набувають нових моделей реалізації, передусім за допомогою використання інформаційно-телекомунікаційних, ШІ-технологій тощо. Щоб ефективно протидіяти цим негативним факторам Служба безпеки України має постійно вдосконалювати методи, матеріально-технічну основу своєї діяльності, підвищувати обізнаність кадрового складу, досліджувати іноземний досвід боротьби із злочинністю, активно розвивати сектор протидії кіберзлочинам і кібертероризму. Пристосування до актуальних загроз забезпечить досконаліть та безперервність захисту критичної інфраструктури, готовність СБУ до виконання завдань [86];

– принцип конфіденційності та захисту таємної інформації. СБУ як орган національної безпеки провадить більшу частину своєї діяльності секретно, працюючи із чутливими відомостями, які становлять державну таємницю, охоронювану законодавством. Виток подібної інформації в суспільство може зумовити її протиправне використання особами та групами для вчинення суспільно небезпечних діянь. З метою попередження цього

СБУ, попри цілком прозорий характер роботи національної системи захисту об’єктів критичної інфраструктури, реалізує свої повноваження із суворим дотриманням правил і вимог режиму секретності [86].

Крім завдань та принципів, виключно важливим аспектом діяльності СБУ як суб’єкта забезпечення безпеки та стійкості об’єктів критичної інфраструктури, є система нормативних засад, що регламентують роботу органу в зазначеному напрямі, а також закріплюють вище визначені цілі та ідейні основи. Ключове місце серед нормативних засад належить Конституції України. Вона є основним документом національної системи права, яка: закріплює принципи побудови й роботи державної влади; декларує основоположні права, свободи та обов’язки людини та громадянина; визначає основи адміністративно-територіального устрою країни; регламентує правовий статус місцевого самоврядування; окреслює основні обов’язки держави із забезпечення прав та інтересів людини і громадянина тощо. Положення Конституції прямо не стосуються захисту критичної інфраструктури, але декларують окремі принципи захисту останньої, врегульовують статус деяких суб’єктів національної системи забезпечення безпеки її об’єктів, порядок формування керівної ланки Служби безпеки України тощо [64].

Крім Конституції України, у цьому контексті варті уваги законодавчі акти, які представлено багатьма документами, що стосуються діяльності СБУ, зокрема, як суб’єкта захисту критичної інфраструктури, а саме:

– Закон України «Про критичну інфраструктуру» від 16 листопада 2021 року № 1882-IX – визначає правові й організаційні засади створення та функціонування національної системи захисту критичної інфраструктури і є складовою законодавства у сфері національної безпеки;

– Закон України «Про Службу безпеки України» від 25 березня 1992 року № 2229-XII – регулює питання організації, забезпечення та реалізації органами й підрозділами СБУ діяльності, спрямованої на протидію

злочинності, тероризму; забезпечення державної таємниці в роботі підприємств, установ та організацій; протидії розвідувальній діяльності іноземних держав та країни-агресора тощо;

– Закон України «Про боротьбу з тероризмом» від 20 березня 2003 року № 638-IV – має на меті захист особи, держави та суспільства від тероризму, виявлення та усунення причин і умов, які його породжують, визначає правові та організаційні основи боротьби з цим небезпечним явищем, повноваження та обов'язки органів виконавчої влади, об'єднань громадян і організацій, посадових осіб та окремих громадян у цій сфері, порядок координації їх діяльності, гарантії правового й соціального захисту громадян у зв'язку з участю в боротьбі з тероризмом;

– Закон України «Про контррозвідувальну діяльність» від 26 грудня 2002 року № 374-IV – визначає поняття, правові основи організації та здійснення контррозвідувальної діяльності;

– Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII – визначає правові й організаційні основи забезпечення захисту життєво важливих інтересів людини та громадянина, суспільства й держави, національних інтересів України в кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб і громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки тощо [106; 122; 123; 128; 131].

Операційні моменти захисту критичної інфраструктури органами та підрозділами СБУ уточнено в підзаконних нормативних документах загальнодержавного значення, поширених на всіх суб'єктів національної системи захисту, а також відомчими актами, які стосуються безпосередньо СБ України.

До першої підгрупи підзаконних документів належать постанови КМУ від 9 жовтня 2020 року № 1109 «Деякі питання об’єктів критичної інфраструктури», від 19 серпня 2023 року № 825-р «Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури», від 22 липня 2022 року № 821 «Про затвердження Порядку проведення моніторингу рівня безпеки об’єктів критичної інфраструктури», від 29 грудня 2021 року № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту», від 26 листопада 2025 року № 1533 «Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози» тощо [32; 34; 112; 116; 118].

Серед документів другої групи можна виокремити спільний наказ СБУ та Адміністрації Держспецзв’язку від 19 грудня 2024 року № 627/772 «Деякі питання розробки, затвердження та погодження планів захисту об’єктів критичної інфраструктури за проєктною загрозою національного рівня “кібератака/кіберінцидент”», яким урегульовано питання взаємодії СБУ та Держспецзв’язку з планування захисту об’єктів критичної інфраструктури, передусім від кіберзагроз [35]. Варто зауважити, що більшість підзаконних актів, які стосуються внутрішньої діяльності СБУ, містять державну таємницю, через що їх детальний розгляд у межах нашої дисертації є ускладненим.

Таким чином, стан нормативних засад забезпечення безпеки та стійкості функціонування об’єктів критичної інфраструктури в діяльності Служби безпеки України можна оцінити як загалом сформований, але такий, що залишається недостатньо систематизованим та орієнтованим передусім на безпекові й контррозвідувальні аспекти. Нормативне регулювання наділяє СБУ необхідними повноваженнями для виявлення та нейтралізації загроз об’єктам критичної інфраструктури, однак воно переважно зосереджене на реагуванні на загрози, а не на комплексному забезпеченні стійкості та безперервності їх функціонування. Водночас спостерігається недостатня

деталізація механізмів координації з іншими суб'єктами захисту критичної інфраструктури та обмежена регламентація превентивних заходів, що знижує ефективність практичної реалізації відповідних повноважень.

1.4. Сутність і структура адміністративно-правового статусу Служби безпеки України щодо захисту об'єктів критичної інфраструктури

Особлива роль Служби безпеки України в системі суб'єктів захисту критичної інфраструктури пояснюється специфікою її адміністративно-правового статусу. Вказана категорія притаманна всім без винятку органам влади, проте залежно від нормативних основ діяльності та сфери публічного інтересу конкретного відомства може відрізнятись за сутністю та структурою. Поняття «статус» виражає положення, становище, місце або роль когось-, чогось. Зазначене слово походить з латинської мови, де «status» означає стан певного об'єкта [176]. Вбачається певна єдність етимологічних і філософських трактувань наведеного терміна, адже в останній науковій галузі йому відповідають категорії «стан», «становище», що розкриваються таким чином: єдність буття і небуття, неперервний процес змін, що повинен привести до виникнення чогось, до перетворення можливості в дійсність, до наявного буття. Загалом у філософію категорію статусу ввів Аристотель, який розглядав її в тісному зв'язку з категоріями «сутність» і «відношення» [97, с. 157; 162, с. 607]. Отже, з огляду на положення етимології та філософії, можна констатувати: статус – це термін-характеристика, який описує місце, роль, положення, стан певного суб'єкта або об'єкта в межах певних зовнішніх ознак. Суттєво на зміст поняття «статус» вплинула соціологія, де воно набуло значення однієї з ключових категорій.

Згідно з документами та офіційними джерелами міжнародної організації ЮНЕСКО, соціальний статус – це позиція людини в суспільстві та суспільних відносинах [178]. У підручнику із соціології В. Н. Городяненко соціальний статус визначає як позицію особистості в соціальній системі, пов'язану з належністю до певної соціальної групи чи спільноти, сукупність її соціальних ролей та якість і ступінь їх виконання. Він (статус) охоплює узагальнюючу характеристику становища індивіда в суспільстві: професію, кваліфікацію, освіту, характер виконуваної праці, посаду, матеріальне становище, наявність влади, партійну і профспілкову належність, ділові відносини, належність до демографічних або етнічних груп (національність, релігійність, вік, сімейне становище, родинні зв'язки). Крім того, соціальні статуси, зауважує автор, поділяються на привласнені, або одержані незалежно від суб'єкта, найчастіше від народження (раса, стать, вік, національність) і досягнуті, або надбані власними зусиллями індивіда (сімейне становище, професійно-кваліфікаційний рівень тощо). Серед статусів вирізняють інтегральний та допоміжні. Іноді їх взаємодія може спричиняти внутрішньоособистісні конфлікти [26]. У дослідженні О. В. Белькової соціальний статус схарактеризовано як положення особи в суспільстві. «Поняття "положення" також застосовують у різних значеннях: певне становище, зумовлене відповідними обставинами; місце і роль у суспільстві, у соціальному чи професійному середовищі. За вживанням понять "роль" та "місце" у суспільному житті можна сказати, що воно (положення) особи в певних обставинах визначає, які дії може людина виконувати в ньому та виконання яких дій від особи можна вимагати, обумовлює спосіб, у який виконуються відповідні дії. Положення (статус) характеризує дещо незалежне від волі особи, яка його займає, та може визначатися як встановлене коло можливостей, за межі якого особа не може вийти. Такі можливості встановлюються не власне особою, а соціальними нормами, які прийняті в певному суспільстві, певній суспільній групі та

обумовлені наявністю в особи певних ознак, що дають змогу займати це положення», – пише авторка [11, с. 52].

У юриспруденції існує декілька різновидів статусу: загальний правовий та галузеві, зокрема адміністративний, кожен з яких переймає значний масив ознак соціального. Наприклад, С. Я. Бурда зазначає: «Правовий статус – це теоретична конструкція, що з'єднує нормативні характеристики, теоретичні уявлення і та реальну практику реалізації правових установлень. Особливості правового статусу як категорії полягають у тому, що він дозволяє комплексно, з урахуванням різних точок зору, свого нормативного режиму, правових форм соціальних можливостей та обтяжень підійти до моделювання юридичного стану різних осіб та організацій і в такий спосіб подолати недоліки однобічного підходу до вивчення якого-небудь суб'єкта як носія лише прав або юридичних обов'язків» [18, с. 18–19]. Натомість І. Й. Снігур стверджує, що правовий статус – це юридично закріплене положення особи в суспільстві. Основою правового статусу слугує фактичний соціальний статус, тобто реальне становище людини в цій системі суспільних відносин. Соціальний і правовий статуси співвідносяться як зміст та форма. З огляду на зазначене, автор доходить такого висновку: «Правовий статус – комплексна, інтеграційна категорія, що відображає взаємовідносини особистості та суспільства, громадянина й держави, індивіда та колективу, інші соціальні зв'язки» [148, с. 16]. Водночас Т. П. Попович пропонує ширшу характеристику вказаної категорії. На думку науковця, правовий статус дозволяє визначити місце, становище особи у відносинах з державою та суспільством загалом. Такі відносини відображаються у формі взаємних прав та обов'язків, що й становлять основу правового статусу. На підставі цього вчений виокремлює широку та вузьку дефініції категорії. Згідно із широким підходом, правовий статус – це суб'єктивні права, свободи, юридичні обов'язки з поєднанням їх із правосуб'єктністю та юридичною відповідальністю. З позиції вузького підходу, правовий статус – це юридично

закріплене становище особи в суспільстві, що відображене в сукупності його прав та обов'язків, які визначені та гарантовані Конституцією й законами України, іншими нормативно-правовими актами, міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України [105, с. 715–716].

Щодо адміністративно-правового статусу, то він слугує галузевим відгалуженням класичного, правового та врегульовує положення фізичної або юридичної особи в координатах публічно-владних правовідносин. Т. О. Коломоєць визначає категорію як сукупність суб'єктивних прав та обов'язків, закріплених нормами адміністративного права. Водночас обов'язковою ознакою набуття суб'єктом адміністративно-правового статусу є наявність у нього конкретних суб'єктивних прав та обов'язків, що реалізуються в межах як адміністративних правовідносин, так і поза ними [11; 61, с. 64].

Слід зауважити, що наукові підходи до тлумачення адміністративно-правового статусу зазвичай орієнтовані на конкретний суб'єкт. Наприклад, адміністративно-правовий статус фізичної особи І. П. Голосніченко визначає як комплекс її прав та обов'язків, закріплених нормами адміністративного права, реалізація яких забезпечується певними гарантіями. Основою цього статусу слугує адміністративна правоздатність, тобто здатність мати права та виконувати обов'язки адміністративно-правового характеру [2, с. 198]. Адміністративно-правовим статусом органів внутрішніх справ (сучасна поліція) та місцевих органів влади як суб'єктів взаємодії С. Л. Курило вважає їхнє положення (становище) в системі суспільних відносин і механізмі державного управління, що визначається державою шляхом закріплення в нормах адміністративного законодавства їхніх завдань, функцій, повноважень і відповідальності, які реалізуються зазначеними суб'єктами через відповідні адміністративно-правові (управлінські відносини), зокрема ті, що складаються безпосередньо під час їхньої взаємодії з питань

забезпечення громадської безпеки та громадського порядку [70, с. 525–526]. О. В. Литвин обстоює таке тлумачення адміністративно-правового статусу державних службовців: визначений чинним законодавством перелік суб'єктивних прав, юридичних обов'язків, гарантій їх реалізації, а також обмежень, що в сукупності забезпечують реалізацію державним службовцем повноважень у межах функцій і завдань державної служби. Керуючись таким баченням, автор у якості частин (елементів) адміністративно-правового статусу пропонує виокремлювати: права; обов'язки; гарантії реалізації прав та обов'язків; обмеження державних службовців [72, с. 74]. О. Ю. Дрозд, Л. В. Сорока та Л. І. Миськів схарактеризували адміністративно-правовий статус органів виконавчої влади як різновид правового статусу, який визначає права, обов'язки, повноваження та відповідальність конкретного суб'єкта цієї системи (міністерство, служба, агентство, інспекція, центральний орган виконавчої влади зі спеціальним статусом, колегіальний орган, інший центральний орган виконавчої влади, місцевий орган влади) у сфері публічного адміністрування та конкретних адміністративних відносин. На їх думку, такий статус встановлюється законами або іншими нормативно-правовими актами, однак здебільшого – положеннями про засади та організацію їхньої діяльності [38, с. 507].

Д. О. Іщук розкриває адміністративно-правовий статус Національного агентства з питань запобігання корупції як сукупність закріплених нормами адміністративного права елементів, що визначають спрямованість діяльності агентства, а також призначення цього органу в системі відповідних суб'єктів. До відповідних елементів такого статусу, на думку вченого, належать: структура агентства, завдання, функції, повноваження, гарантії та відповідальність. Автор виокремлює такі особливості адміністративно-правового статусу НАЗК: 1) мета існування цього відомства полягає в тому, щоб запобігти вчиненню корупційного правопорушення, а також створити всі необхідні умови для того, щоб мінімізувати або ж ліквідувати корупційні

ризики в діяльності підприємств, установ, організацій у подальшому; 2) використовує у своїй діяльності специфічні форми й методи протидії корупції (наприклад, електронне декларування); 3) має особливу ієрархічну будову, що впливає на специфіку прийняття управлінських рішень; 4) наділене специфічним переліком повноважень та юридичних гарантій діяльності; 5) основною формою безпосередньої роботи Національного агентства є засідання, які мають регулярний характер [52].

Проведений аналіз дає змогу констатувати багатоманітність наукових концепцій з приводу змісту й значення адміністративно-правового статусу. Їх розгляд і зіставлення надають можливість сформулювати авторську інтерпретацію категорії з огляду на порушену в цій статті проблему. Отже, на нашу думку, адміністративно-правовий статус Служби безпеки України щодо захисту об'єктів критичної інфраструктури – це системна сукупність визначених законодавством України юридичних елементів, які встановлюють місце, роль і призначення СБУ в суспільно-правових відносинах, що виникають з реалізації діяльності направленої на забезпечення безпеки і стійкості функціонування об'єктів критичної інфраструктури. Сутність цього статусу визначають декілька головних особливостей, які принципово вирізняють СБУ з-поміж інших суб'єктів національної системи захисту об'єктів критичної інфраструктури. Так, СБ України є передусім правоохоронним органом, що власне визначає перелік виконуваних ним функцій [177].

Відповідно до Закону України «Про державний захист працівників суду і правоохоронних органів», правоохоронними визначаються органи прокуратури, Національної поліції, служби безпеки, Військової служби правопорядку в Збройних Силах України, а також Національне антикорупційне бюро України, органи охорони державного кордону, Бюро економічної безпеки України, органи й установи виконання покарань, слідчі ізолятори, органи державного фінансового контролю, рибоохорони,

державної лісової охорони, інші органи, які здійснюють правозастосовні або правоохоронні функції [107].

До змісту правоохоронних органів неодноразово зверталися дослідники юридичної галузі. Так, В. Т. Маляренко правоохоронним органом вважає державну установу (або державну юридичну особу), яка діє в системі органів влади та виконує на основі закону державні функції (владні, організаційно-розпорядчі, контрольно-перевірочні тощо) в різних сферах внутрішньої та зовнішньої діяльності Української держави [151]. М. І. Мельник наголошує на тому, що правоохоронний орган – це державний, зазвичай озброєний, орган, який виконує правоохоронні функції та у зв'язку з цим потребує специфічного матеріального та іншого забезпечення. З метою ефективного виконання своїх обов'язків працівники наділяються різноманітними специфічними правами, мають відповідні пільги, зовнішні ознаки належності до правоохоронних органів, користуються підвищеним правовим захистом [77, с. 43–44]. Крім того, О. В. Тюріна, В. І. Осадчий, В. М. Скрипнюк та О. М. Дуфенюк стверджують, що в широкому значенні правоохоронні органи – це всі державні органи, наділені певними повноваженнями в галузі контролю за додержанням законності й правопорядку. У вузькому значенні до правоохоронних органів належать державні органи, які спеціально створені для забезпечення законності та правопорядку, боротьби зі злочинністю і з цією метою їм надані повноваження застосовувати передбачені законом заходи примусу та перевиховання правопорушників [94, с. 71; 145, с. 11–10; 158, с. 79]. У зазначеному контексті В. Г. Лукашевич акцентує на тому, що правоохоронні органи – це сукупність державних органів, основною функцією котрих є охорона законності, боротьба зі злочинністю та іншими правопорушеннями, а саме: суд, прокуратура, органи юстиції, органи внутрішніх справ, органи державної безпеки, органи державного арбітражу [73, с. 23–34]. Отже, СБУ як правоохоронний орган виконує правоохоронну, правозастосовну та інші публічні функції,

безпосередньо пов’язані із захистом прав, свобод, законних інтересів суспільства та кожної окремої людини від протиправних посягань, зокрема на об’єктах критичної інфраструктури; встановленням осіб, які вчинили правопорушення, збором доказів їх вини та притягненням до юридичної відповідальності. Відмінність такого функціоналу від інших органів влади полягає в тому, що СБ України активно застосовує державний примус для досягнення поставлених перед відомством цілей, який виражено в широкому переліку адміністративних та інших інструментів обмеження прав і свобод фізичних осіб, зокрема за використанням фізичного впливу, спеціальних засобів та навіть вогнепальної зброї.

Друга особливість адміністративно-правового статусу СБУ полягає в тому, що цей орган є головним суб’єктом боротьби з тероризмом. Згідно із Законом України «Про боротьбу з тероризмом» від 20 березня 2003 року № 638-IV, тероризм – це суспільно небезпечна діяльність, яка полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, тортур, залякування населення та органів влади або вчинення інших посягань на життя чи здоров’я ні в чому не винних людей або погрози вчинення злочинних дій з метою досягнення злочинних цілей. Також у документі виокремлено технологічний тероризм, про який часто йдеться саме в контексті роботи об’єктів критичної інфраструктури та який становить: «кримінальні правопорушення, що вчиняються з терористичною метою із застосуванням ядерної, хімічної, бактеріологічної (біологічної) та іншої зброї масового ураження або її компонентів, інших шкідливих для здоров’я людей речовин, засобів електромагнітної дії, комп’ютерних систем та комунікаційних мереж, включаючи захоплення, виведення з ладу і руйнування потенційно небезпечних об’єктів, які прямо чи опосередковано створили або загрожують виникненням загрози надзвичайної ситуації внаслідок цих дій та становлять небезпеку для персоналу, населення чи довкілля; створюють умови для аварій і катастроф техногенного

характеру». Боротьба з наведеним негативним явищем покладає на СБУ особливі обов'язки та закріплює за ним спеціальні права, що дають змогу користуватись специфічними адміністративними інструментами, що недоступні для інших носіїв владних повноважень [106].

Третє, на що варто звернути увагу характеризуючи адміністративно-правове положення Служби безпеки України як суб'єкта захисту об'єктів критичної інфраструктури, – це визначений Законом України «Про державну таємницю» від 21 січня 1994 року № 3855-XII статус спеціально уповноваженого органу з питань забезпечення охорони державної таємниці. Остання, відповідно до ст. 1 Закону, – це вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані в установленому законом порядку, державною таємницею і підлягають охороні державою. Окремі з таких відомостей прямо стосуються роботи об'єктів критичної інфраструктури, що потребує контролю процесу їх використання, а також відслідковування осіб, які мають доступ до цих відомостей, попередження витоку останніх або розголошення представникам іноземних спецслужб, терористам тощо [109].

Останнім специфічним моментом адміністративно-правового статусу СБУ як суб'єкта захисту критичної інфраструктури є особлива управлінська підпорядкованість цього органу. На відміну від інших учасників відповідних відносин, які найчастіше входять у систему органів виконавчої влади, СБ України характеризується самостійністю. Наприклад, у межах відання такого секторального органу, як Міністерство внутрішніх справ України, знаходяться два суб'єкти забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури, а саме Державна служба з надзвичайних ситуацій (далі – ДСНС) та Національна поліція (далі – НПУ) [115].

Так, ДСНС, відповідно до відомчого нормативного акта, є центральним органом виконавчої влади, діяльність якого спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ і який реалізує державну політику у сфері цивільного захисту, захисту населення і територій від надзвичайних ситуацій та запобігання їх виникненню, ліквідації наслідків надзвичайних ситуацій, рятувальної справи, гасіння пожеж, пожежної та техногенної безпеки, діяльності аварійно-рятувальних служб, а також гідрометеорологічної діяльності. Основними завданнями ДСНС є: 1) реалізація державної політики у сфері цивільного захисту, захисту населення і територій від надзвичайних ситуацій, запобігання їх виникненню, ліквідації наслідків надзвичайних ситуацій, рятувальної справи, гасіння пожеж, пожежної та техногенної безпеки, діяльності аварійно-рятувальних служб, а також гідрометеорологічної діяльності; 2) здійснення державного нагляду (контролю) за додержанням і виконанням вимог законодавства у сфері пожежної та техногенної безпеки, діяльності аварійно-рятувальних служб; 3) внесення на розгляд Міністра внутрішніх справ пропозицій щодо забезпечення формування державної політики у зазначених сферах; 4) виконання функцій компетентного органу у сфері діяльності, пов’язаної з об’єктами підвищеної небезпеки [114].

Щодо поліції, то згідно із Законом України «Про Національну поліцію» від 2 липня 2015 року № 580-VIII, остання є центральний органом виконавчої влади, який служить суспільству шляхом забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки та порядку. Як і у випадку з ДСНС, діяльність поліції спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України. Своєю чергою завданнями НПУ є надання поліцейських послуг у сферах: 1) забезпечення публічної безпеки та порядку; 2) охорони прав і свобод людини, а також інтересів суспільства й держави; 3) протидії злочинності; 4) надання в межах, визначених законом, послуг з допомоги особам, які з

особистих, економічних, соціальних причин або внаслідок надзвичайних ситуацій потребують такої допомоги [126].

Своєю чергою Служба безпеки України, відповідно до Закону України «Про Службу безпеки України» від 25 березня 1992 року № 2229-XII, не входить до жодної із систем державної влади. Основною демократичною інституцією, якій прямо підпорядковано роботу СБУ, є Президент України. Його актами затверджено загальну структуру СБУ, а також засади роботи Антитерористичного центру, що створено для організації і проведення антитерористичних операцій та координації діяльності суб'єктів, які ведуть боротьбу з тероризмом чи залучаються до антитерористичних операцій. Президент призначає та звільняє з посади Голову СБУ, а Центральне управління органу вносить гаранту конституції пропозиції про видання актів з питань збереження державної таємниці, обов'язкових для виконання органами державного управління, підприємствами, установами, організаціями і громадянами [131]. Крім визначеного, саме Президент України та уповноважений ним орган здійснюють контроль за діяльністю Служби безпеки України, а саме за дотриманням конституційних прав громадян і законодавства в оперативно-розшуковій діяльності та діяльності у сфері охорони державної таємниці органів і підрозділів СБУ, а також контроль за відповідністю виданих Службою положень, наказів, розпоряджень, інструкцій і вказівок Конституції і законам України [131].

Переходячи до огляду структурних елементів адміністративно-правового статусу Служби безпеки України щодо захисту об'єктів критичної інфраструктури, наголосимо, що в наукових джерелах цей аспект вчені розкривають по-різному. Зазвичай до статусу кожного окремого учасника публічно-владних відносин включають різні складові, визначені передусім сферою його діяльності та нормативно-правовими особливостями закріплення юридичного положення. У контексті нашого дослідження вважаємо за доцільне використати чотириелементну структуру, яка за

змістом відповідає більшості наявних концепцій. Таким чином, адміністративно-правовий статус Служби безпеки України як суб'єкта забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури становлять [87]:

– нормативно визначена компетенція. Як стверджує у своїй дисертаційній роботі Л. П. Москович, термін «компетенція» («competentia») латинського походження і буквально означає: узгодженість частин, домірність, симетрію; знання справи; рівень освіти, досвід роботи за спеціальністю, стаж роботи на посаді; коло питань, щодо яких хтось добре обізнаний, тощо [89, с. 83]. У складі адміністративно-правового статусу СБУ компетенція – це нормативно визначене коло ключових питань і проблем, на вирішення яких спрямовано роботу органів та підрозділів Служби під час забезпечення безпеки об'єктів критичної інфраструктури. Кара за подібні діяння передбачена Кримінальним кодексом України від 5 квітня 2001 року № 2341-III (далі – ККУ), а їх перелік охоплює такі тяжкі кримінальні правопорушення, як шпигунство, диверсія, державна зрада, терористичний акт, втягнення у вчинення терористичного акту, створення терористичної групи чи організації, сприяння вчиненню терористичного акту тощо [67];

– повноваження Служби безпеки України у сфері захисту об'єктів критичної інфраструктури. Повноваження є комплексною категорією, яка охоплює нормативно закріплені права та обов'язки органів і підрозділів СБУ за напрямом забезпечення безпеки, стійкості функціонування системи критичної інфраструктури. Фактично цей елемент визначає, яким саме чином органи та підрозділи Служби виконують покладені на відомства завдання і функції, тобто реалізують його компетенцію. Загальний масив повноважень урегульовано передусім основними документами, де відображено статус СБУ як частини національної системи захисту критичної інфраструктури, а саме законами «Про Службу безпеки України» від 25 березня 1992 року № 2229-XII, «Про критичну інфраструктуру» від 16 листопада 2021 року № 1882-IX

[123; 131]. Більш специфічні права та обов'язки, в контексті окремих різновидів діяльності Служби визначено законами України «Про боротьбу з тероризмом» від 20 березня 2003 року № 638-IV, «Про контррозвідувальну діяльність» від 26 грудня 2002 року № 374-IV тощо [106; 122; 127];

– гарантії діяльності Служби безпеки України в процесі забезпечення захисту критичної інфраструктури. Юридичними гарантіями слугують закріплені законодавством про діяльність СБУ умови, засоби та способи, якими забезпечено повне та якісне виконання органами, підрозділами та персоналом СБ України своїх прав та обов'язків із підтримання безпеки і стійкості функціонування об'єктів критичної інфраструктури. Основний перелік гарантій роботи Служби визначено Законом України «Про Службу безпеки України» від 25 березня 1992 року № 2229-XII. Наприклад, документ встановлює, що регіональні органи СБУ у своїй оперативно-службовій діяльності є незалежними від органів місцевої державної адміністрації та місцевого самоврядування, посадових осіб, партій і рухів. Причому в інтересах державної безпеки органи та підрозділи Служби безпеки України можуть створюватися на окремих державних стратегічних об'єктах і територіях, у військових формуваннях. Так, органи військової контррозвідки створюються для контррозвідувального забезпечення Збройних Сил України і Державної прикордонної служби України та інших військових формувань, дислокованих на території України [131]. Крім того, органи місцевої державної адміністрації та місцевого самоврядування зобов'язані сприяти Службі безпеки України, її органам і підрозділам у вирішенні житлових та інших соціально-побутових проблем, забезпеченні транспортом і зв'язком. СБУ гарантується право мати адміністративні приміщення та інші споруди, об'єкти охорони здоров'я, навчального, науково-дослідного, господарського та соціально-культурного призначення, відомчий житловий фонд [131]. Відповідне коло гарантій безпосередньо стосується персоналу СБУ. Так, стаття 28 Закону декларує, що військовослужбовці Служби безпеки України

під час виконання покладених на них обов'язків є представниками влади, діють від імені держави і перебувають під її захистом. Недоторканність їх особи, їх честь і гідність охороняються законодавством [131];

– відповідальність СБУ за ефективність і результативність роботи із захисту критичної інфраструктури. Це – система засобів впливу на посадових осіб служби й орган загалом за допущені порушення прав, законних інтересів громадян, неналежну реалізацію заходів забезпечення безпеки об'єктів критичної інфраструктури, недбалість, яка призвела до порушення їх функціонування або повного припинення, вчинення інших негативних дій, що впливають на якість діяльності органу. Так, згідно зі ст. 35 Закону України «Про Службу безпеки України» від 25 березня 1992 року № 2229-XII, співробітники Служби безпеки України самостійно приймають рішення в межах своїх повноважень. Вони мають відмовлятися від виконання будь-яких наказів, розпоряджень або вказівок, які суперечать чинному законодавству. За протиправні дії та бездіяльність вони несуть дисциплінарну, адміністративну та кримінальну відповідальність. Працівники Служби безпеки України (крім військовослужбовців), яких притягнуто до відповідальності за вчинення адміністративного правопорушення, пов'язаного з корупцією, або кримінального правопорушення, звільняються із служби в триденний строк з дня одержання відповідним органом Служби безпеки України копії відповідного судового рішення. Військовослужбовці Служби безпеки України, яких притягнуто до відповідальності за вчинення адміністративного правопорушення, пов'язаного з корупцією, або кримінального правопорушення, підлягають звільненню із служби [131]. Крім зазначеного, об'єктивній оцінці суб'єктами контролю піддається діяльність всього органу загалом за різними напрямами, зокрема із захисту критичної інфраструктури. Наслідками цього може стати зміна керівної ланки СБУ, ліквідація її структурних підрозділів та інші подібні заходи з метою підвищення рівня ефективності роботи [87].

Підбиваючи підсумки, слід констатувати, що адміністративно-правовий статус СБУ характеризується багатьма відмінними аспектами, які зумовлюють унікальність органу та його впливовість, а саме: статус правоохоронного та спеціально уповноваженого органу з питань забезпечення охорони державної таємниці, центральне місце з-поміж суб'єктів боротьби з тероризмом, а також високий рівень управлінської незалежності. Безпосередньо структура цього статусу охоплює компетенцію, повноваження, гарантії діяльності із захисту критичної інфраструктури та відповідальність за ефективність провадження останньої. Належне закріплення елементів на законодавчому рівні має вкрай важливе значення, адже забезпечить більш ефективне та якісне виконання Службою своїх завдань та функцій у досліджуваній сфері суспільного життя [87].

Висновки до розділу 1

Здійснено аналіз наукових підходів, який засвідчив суттєву відмінність між законодавчим і доктринальним розумінням критичної інфраструктури. Зауважено, що тлумачення вчених відрізняються більшою комплексністю, відображають специфічні характеристики категорії, її вплив на соціум і середовище його життєдіяльності. Сформульовано висновок про те, що критична інфраструктура – це сукупність матеріальних і нематеріальних об'єктів, що мають критичне значення для нормального функціонування всієї держави, її економіки, національної безпеки, оборони, соціального сектору, порушення яких потенційно становить загрозу або має ризик спричинення реальної шкоди національним інтересам, функціонуванню державного апарату, життю, здоров'ю та добробуту населення.

Доведено, що захист критичної інфраструктури – це комплексна, систематична, багатовекторна діяльність, яка реалізується в процесі

створення та управління об’єктом критичної інфраструктури та спрямовується на профілактику, попередження, виявлення та припинення загроз безпеці функціонування та власне факту існування такого об’єкта, відшкодування шкоди та виправлення негативних наслідків у разі реалізації загроз.

Зауважено, що згідно з Основним Законом ключовий обов’язок та напрям державної діяльності полягає в забезпеченні добробуту населення країни, створення умов для реалізації усіма його представниками своїх суб’єктивних прав, а також досягнення відповідних інтересів у будь-яких сферах. Критична інфраструктура прямо пов’язана з цими питаннями, адже порушення безпеки її об’єктів створює загрозу для громадян України, обсягів їх правових можливостей, життя та здоров’я. Через це, захист критичної інфраструктури кореспондується із загальним функціоналом держави в особі повноважних суб’єктів із забезпечення прав, свобод та інтересів людини і громадянина, у зв’язку з чим перебуває в межах предметної орієнтації адміністративного права.

З’ясовано, що державна політика у сфері захисту критичної інфраструктури – це стратегічні й тактичні вектори діяльності органів державної влади та інших уповноважених суб’єктів публічного управління щодо організації та ефективної реалізації діяльності у сфері захисту критичної інфраструктури в Україні, які обумовлені об’єктивними умовами суспільно-політичного, економічного розвитку, безпекової ситуації тощо.

Констатовано, що захист об’єктів критичної інфраструктури як об’єкта адміністративно-правового регулювання характеризується тим, що ця діяльність: по-перше, детермінована обов’язком держави забезпечувати права, свободи, законні інтереси людини та громадянина, а також створювати безпечні для життя та здоров’я нації умови існування; по-друге, організовується та здійснюється у форматі окремої ланки державної політики; по-третє, проводиться щодо об’єктів, віднесення яких до критичної

інфраструктури відбувається за волею уповноважених органів державної влади в нормативно встановленому порядку. Крім того, захист критичної інфраструктури належить до предмета діяльності Служби безпеки України, яка протидіє правопорушенням у цій сфері та є одним з правоохоронних органів, що входять до складу системи відповідних суб'єктів захисту.

Аргументовано положення про те, що суб'єкти загальнодержавного рівня забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури виконують широкі функції та відповідають за реалізацію глобальних цілей, пов'язаних із формуванням і провадженням державної політики у сфері критичної інфраструктури; визначенням об'єктів, які належать до системи останньої; здійсненням координації та управління іншими суб'єктами захисту, а також організацією їх взаємодії; розробленням і затвердженням стратегічних документів, пов'язаних із проведенням заходів захисту.

Обґрунтовано, що суб'єкти забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури другого, регіонально-галузевого, рівня – це основний масив державних органів, які реалізують заходи та інструменти, спрямовані на: а) забезпечення функціонування об'єктів критичної інфраструктури за встановленими законодавством секторами; б) прогнозування та виявлення потенційно наявних загроз їх безпеці, а також реагування на порушення і протиправні дії стосовно вказаних об'єктів. У вказаній групі Служба безпеки України – це спеціальний функціональний, правоохоронний орган, предметом діяльності якого є боротьба із суспільно небезпечними діями окремих осіб та/або їх груп, вчинюваних на об'єктах критичної інфраструктури та щодо них, що становить ризики національній безпеці.

Сформульовано висновок про те, що Служба безпеки України має досить вузьке спрямування діяльності у сфері забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури. Служба є

спеціалізованим правоохоронним органом, уповноваженим протидіяти загрозам, що мають підвищений рівень публічної небезпеки та які здатні завдати шкоди не лише окремим об'єктам критичної інфраструктури, а й життєво важливим інтересам суспільства та держави загалом. Наголошено, що саме комплексний характер цих загроз, які можуть зачіпати безпеку населення, суверенітет і конституційний лад, зумовлює унікальне місце Служби безпеки України в системі суб'єктів забезпечення безпеки та стійкості функціонування досліджуваної сфери, а її повноваження дозволяють не лише реагувати на посягання та різноманітні загрози, а й здійснювати превентивний вплив, формуючи ключову ланку державного механізму захисту критично важливих об'єктів.

Зауважено, що завдання забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури Службою безпеки України – це сукупність мікроцілей діяльності СБУ, її органів та підрозділів у сфері захисту об'єктів критичної інфраструктури від злочинних посягань окремих осіб та груп, що несуть небезпеку національним інтересам та суспільству.

З'ясовано, завданнями забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури Службою безпеки України є такі: 1) участь у реалізації (у межах визначеної Законом України «Про Службу безпеки України» та відповідними відомчими нормативно-правовими актами компетенції, мети й завдань) державної політики у сфері захисту об'єктів критичної інфраструктури; 2) здійснення у встановленому законодавством порядку попередження, профілактики, виявлення, розкриття та розслідування злочинів, які належать до підслідності органів Служби безпеки України та вчинені на об'єктах критичної інфраструктури або стосовно них; 3) організація та реалізація заходів, спрямованих на боротьбу з тероризмом, диверсіями, зокрема з використанням інформаційних і цифрових технологій, на об'єктах критичної інфраструктури; 4) виявлення

осіб, організованих злочинних груп та злочинних організацій, діяльність яких спрямована на порушення безпеки об’єктів критичної інфраструктури, перешкоджання їх нормальній роботі, а також забезпечення притягнення цих осіб до встановленої законом відповідальності; 5) організаційне, матеріально-технічне, кадрове, фінансово-господарське та інше забезпечення діяльності органів і підрозділів Служби безпеки України, залучених до забезпечення безпеки й захисту об’єктів критичної інфраструктури від злочинів, що належать до її підслідності; 6) систематична оцінка ризиків, моніторинг наявних загроз критичній інфраструктурі держави з огляду на умови об’єктивної дійсності політичного, економічного, військового та іншого змісту, а також планування заходів протидії таким загрозам, мінімізації їх негативного впливу; 7) особлива процедура організації та забезпечення системної взаємодії між органами, підрозділами Служби безпеки України та іншими суб’єктами національної системи захисту критичної інфраструктури з питань обміну інформацією, планування спільних профілактичних заходів, реагування на загрози безпеки функціонування об’єктів критичної інфраструктури; 8) забезпечення захисту відомостей, що становлять державну таємницю, у сфері роботи об’єктів критичної інфраструктури.

Доведено, що принципи забезпечення безпеки та стійкості функціонування об’єктів критичної інфраструктури Службою безпеки України – це нормативно закріплені та засновані на загальновизнаних цінностях і призначенні права, базові юридичні засади, які визначають зміст, організацію та порядок діяльності Служби безпеки України щодо запобігання загрозам, охорони й підтримання стабільного функціонування об’єктів критичної інфраструктури. До таких принципів віднесено: законність та верховенство права; принцип забезпечення та дотримання прав та свобод людини і громадянина; координованості та взаємодії; гнучкості та адаптивності до змін; конфіденційності та захисту таємної інформації.

Зазначено, що принцип забезпечення та дотримання прав і свобод людини та громадянина полягає в тому, що діяльність органів, підрозділів і кожного окремого працівника Служби безпеки України, навіть в аспекті протидії таким негативним явищам, як тероризм, та іншим злочинам на особливо важливих для суспільства й держави об'єктах критичної інфраструктури, не може відбуватися з порушенням прав, свобод і законних інтересів людини та громадянина. СБУ має право обмежувати права та свободи, але виключно у встановлених законодавством випадках для досягнення поставлених цілей, дотримуючись вимог формалізованої процедури.

Акцентовано увагу на тому, що бурхливий технологічний розвиток людства суттєво позначається на загрозах об'єктам критичної інфраструктури, які набувають нових моделей реалізації, передусім завдяки використанню інформаційно-телекомунікаційних, ШІ-технологій тощо. Щоб ефективно протидіяти цим негативним факторам, Служба безпеки України має постійно вдосконалювати методи, матеріально-технічну основу своєї діяльності, підвищувати обізнаність кадрового складу, досліджувати іноземний досвід боротьби зі злочинністю, активно розвивати сектор протидії кіберзлочинам і кібертероризму. Пристосування до актуальних загроз забезпечить досконаліть та безперервність захисту критичної інфраструктури, готовність СБУ до випробувань.

Встановлено, що стан нормативних засад забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури в діяльності Служби безпеки України можна оцінити як загалом сформований, але такий, що залишається недостатньо систематизованим і орієнтованим передусім на безпекові та контррозвідувальні аспекти. Досліджуване нормативне регулювання забезпечує Службу безпеки України необхідними повноваженнями для виявлення та нейтралізації загроз об'єктам критичної інфраструктури, однак воно переважно зосереджене на реагуванні на загрози,

а не на комплексному забезпеченні стійкості та безперервності їх функціонування. Водночас спостерігається недостатня деталізація механізмів координації з іншими суб'єктами захисту критичної інфраструктури й обмежена регламентація превентивних заходів, що знижує ефективність практичної реалізації відповідних повноважень.

Доведено, що адміністративно-правовий статус Служби безпеки України щодо захисту об'єктів критичної інфраструктури – це системна сукупність визначених законодавством України юридичних елементів, які встановлюють місце, роль і призначення Служби безпеки України в суспільно-правових відносинах, що виникають з метою реалізації діяльності, спрямованої на забезпечення безпеки і стійкості функціонування об'єктів критичної інфраструктури.

Обґрунтовано, що Служба безпеки України як правоохоронний орган виконує правоохоронну, правозастосовну та інші публічні функції, які безпосередньо пов'язані із захистом прав, свобод, законних інтересів суспільства та кожної окремої людини від протиправних посягань, зокрема на об'єктах критичної інфраструктури; встановленням осіб, які вчинили правопорушення, збором доказів їх вини та притягненням до юридичної відповідальності. Відмінність такого функціоналу від інших органів влади полягає в тому, що СБУ активно застосовує державний примус для досягнення поставлених перед відомством цілей, який виражено в широкому переліку адміністративних та інших інструментів обмеження прав і свобод фізичних осіб, зокрема за використанням фізичного впливу, спеціальних засобів та, навіть, вогнепальної зброї.

Наголошено, що адміністративно-правовий статус Служби безпеки України характеризується багатьма відмінними аспектами, які визначають унікальність органу та його впливовість, що передбачає статус правоохоронного та спеціально уповноваженого органу з питань забезпечення охорони державної таємниці, ключове місце серед суб'єктів

боротьби з тероризмом, а також високий рівень управлінської незалежності. Встановлено, що належне закріплення наведених елементів адміністративно-правового статусу Служби безпеки України на законодавчому рівні має вкрай важливе значення, що забезпечить більш ефективне та якісне виконання Службою своїх завдань і функцій у досліджуваній сфері суспільного життя.

Зауважено, що в складі адміністративно-правового статусу СБУ компетенція – це нормативно визначене коло ключових питань і проблем, на вирішення яких спрямовано роботу органів та підрозділів Служби під час забезпечення безпеки об’єктів критичної інфраструктури, а саме боротьба зі злочинами, які вчиняються стосовно об’єктів критичної інфраструктури або на них безпосередньо. Своєю чергою повноваження є комплексною категорією, яка включає в себе нормативно закріплені права та обов’язки органів і підрозділів СБУ за напрямом забезпечення безпеки, стійкості функціонування системи критичної інфраструктури. Фактично цей елемент визначає, яким саме чином органи та підрозділи Служби виконують покладені на відомства завдання і функції, тобто реалізують його компетенцію.

РОЗДІЛ 2
ХАРАКТЕРИСТИКА АДМІНІСТРАТИВНО-ПРАВОВОГО МЕХАНІЗМУ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ СЛУЖБОЮ БЕЗПЕКИ УКРАЇНИ

2.1. Поняття та особливості адміністративно-правового механізму захисту об'єктів критичної інфраструктури Службою безпеки України

З практичним виконанням Службою безпеки України своїх завдань і функцій у контексті захисту об'єктів критичної інфраструктури пов'язана така категорія, як «адміністративно-правовий механізм». Слово «механізм», як зазначає у своїй дисертації П. С. Лютіков, означає внутрішній устрій (система ланок) машини, пристрою, апарата, що приводить їх у дію; система, устрій, що визначає порядок якого-небудь виду діяльності; послідовність станів, процесів, які визначають собою яку-небудь дію, явище [24, с.71; 74, с. 354]. «Структура механізму, як і будь-якого комплексного явища, складна і містить певні елементи. Елемент – це складова будь-якого цілого. Коли йдеться про соціальні явища, елементи становлять також соціальні явища або відносини, однак не ізольовані, а підпорядковані меті того явища, складовою якого вони є», – пише М. В. Романов [138, с. 54].

У контексті управління такі дослідники, як Н. Р. Нижник, С. П. Мосов, Г. І. Леліков, а також Н. С. Зелінська, яка активно використовує їх напрацювання, зазначають, що механізм становить сукупність дій, які забезпечують здійснення кожного етапу головного процесу. Учені наводять визначення терміна «механізм управління» як частини системи управління, що забезпечує вплив на фактори, від стану яких залежить результат діяльності управлінського об'єкта. Крім того, механізм управління є засобом організації суспільними справами, де взаємопов'язані методи, засоби та

принципи управління, що забезпечує ефективну реалізацію цілей управління [31, с. 235, 254; 47, с. 49].

Своєю чергою С. І. Крук зазначає, що на відміну від технічних наук, звідки й саме походить термін «механізм», науки суспільного та політико-правового блоку визначають його не стільки як фізичне явище, котре може бути виявлено за допомогою органів почуттів чи за допомогою технічних пристроїв, скільки сукупність прав та обов'язків, обґрунтовані ними зміст і характер діяльності індивідів, груп, спільнот, об'єднань. Причому в межах наук цього блоку специфіка механізму визначається в тому, що він спирається на державну владу (орієнтується на її поділ і забезпечення балансу між гілками, на нейтралізацію узурпації одна одної). Ця влада передбачає зіставлення панування і підпорядкування між взаємодіючими сторонами, в основі її знаходяться примус і право, що висвітлюють легітимність державного управління [68].

З огляду на викладе вище, механізм – це система самостійних, не залежних однин від одного елементів, які об'єднано спільною метою, що забезпечує їх функціонування як єдиного цілісного об'єкта. Подібну думку поділяє В. О. Боняк, яка проводить аналіз сутності механізму в правовій галузі. Дослідниця зазначає, що ця категорія використовується для словесного позначення різних загальнотеоретичних категорій у наступних словосполученнях: «механізм правового регулювання», «механізм правотворчості», «механізм формування правомірної поведінки», «загальний механізм дії права». Причому автор наголошує, що «будь-який механізм слугує високоорганізованою системою. Система – це єдність елементів, що перебувають у певних зв'язках і відносинах між собою, характеризують сутність об'єкта, становлять єдине ціле» [14, с. 114].

Водночас варто звернутись до численних наукових підходів, у яких висвітлено сутність правового механізму як самостійної категорії. Наприклад, Т. І. Тарахонич пропонує розуміти останній як певну

конструкцію, яка передбачає дію послідовно організованих юридичних засобів, які дають можливість досягти конкретної юридичної цілі з дотриманням відповідної процедури. «Кожна ланка такого механізму є самостійним комплексом юридичних засобів», – вважає науковець [153, с. 13]. С. І. Бевз зауважує, що правовий механізм – це інструментальна частина правового регулювання, як завжди за допомогою нього реалізується. Він (механізм) покликаний юридично гарантувати досягнення цілей, які ставить законодавець, видаючи або санкціонуючи юридичні норми в межах певних типів (моделей) юридичного впливу. За твердженням вченого, якщо правове регулювання – один з виявів правового впливу за допомогою правових засобів, то механізм – це сукупність цих засобів, які пов'язані між собою та сприяють досягненню правовим регулюванням визначеної мети [8, с. 43–44].

Згідно з позицією О. І. Безпалової, термін «механізм» у межах юриспруденції становить сукупність методів, форм, прийомів, способів, завдяки правильному використанню яких можна буде досягти оптимальної організації всіх елементів системи, їх ефективного функціонування, що в результаті повинно привести до отримання бажаного результату [9]. Ю. А. Ведєрніков та А. В. Папірна зауважують: правовий механізм – це взята в сукупності система правових засобів, за допомогою яких здійснюється правове регулювання суспільних відносин. За допомогою цієї системи правових засобів, способів і форм нормативність права переводиться у впорядкованість суспільних відносин, задовольняються інтереси суб'єктів права, встановлюється і забезпечується правопорядок [21]. А. О. Зубко стверджує, що правові механізми – це певні «комплекти» юридичних засобів, які мають нормативне закріплення та орієнтовані в їх практичному використанні на реалізацію суб'єктами своїх інтересів і досягнення тієї чи іншої цілі як наслідку правового регулювання визначених суспільних відносин. Конкретний правовий механізм як цілісна, взаємопов'язана

структура відображає послідовні стадії юридичної діяльності (громадян, організацій, посадових осіб, органів публічної влади) та різноманітні правові засоби, варіанти їх взаємодії на кожній стадії. За допомогою правових механізмів здійснюється гарантована законодавством реалізація завдань правового регулювання, впливу на суспільні відносини для досягнення конкретної мети [49, с. 297].

Таким чином, правовий механізм – це спеціальна юридична конструкція, яку становлять інструменти, організоване та послідовне використання яких дозволяє реалізувати положення норм чинного законодавства, суб'єктивні права, свободи, законні інтереси, а також отримати будь-який інший юридично значущий результат, який змінює, припиняє чи зумовлює появу нових суспільно-правових відносин. Водночас визначене підтверджує класичний, стандартизований механізм, зміст якого змінюється в аспекті окремих правових галузей, наприклад, адміністративної.

Висвітлюючи загальні особливості категорії «адміністративно-правовий механізм», Ю. О. Коваленко зауважує, що він (механізм) є системою адміністративно-правових засобів і факторів, що виконують низку функцій держави, які покладаються на неї адміністративним законодавством держави (чи конкретизуються нормативно-правовими актами цієї галузі права); передбачені нормами адміністративного законодавства (також і суміжних галузей права); підпорядковані загальній меті, завданням та загальноправовим і галузевим принципам цієї галузі права [59, с. 42]. Водночас І. В. Хміль розглядає адміністративно-правовий механізм міжнародного співробітництва у сфері забезпечення національної безпеки як термінологічно-правову абстракцію, яка позначає сукупність сутнісно відмінних, однак взаємопов'язаних і взаємодоповнюючих, складових адміністративно-правового характеру, синергізм яких уможливлює здійснення державами спільних взаємовигідних заходів щодо охорони й захисту відповідних національних інтересів від реальних і потенційних

загроз [166, с. 42]. Адміністративно-правовий механізм регулювання міграції Н. П. Тиндик розкриває як систему норм та інших правових засобів, що регулюють відносини у сфері діяльності суб'єктів міграції, спрямованих на реалізацію повноважень між учасниками цих відносин, у разі порушення яких застосовуються заходи державного впливу [155, с. 9].

У своїй дисертаційній роботі О. І. Дубенко зазначає: «Категорія "адміністративно-правовий механізм забезпечення безпеки" має функціональне значення для практичної реалізації і є системою комплексних заходів з охорони та відновлення порушених прав людини, створює організаційно-правову базу, що дозволяє органам державної влади та місцевого самоврядування безперешкодно здійснювати свої повноваження» [40, с. 15–16]. Т. А. Кобзєва стверджує, що адміністративно-правовий механізм управління фінансовою системою України становить засновану на нормах адміністративного права динамічну систему, у межах якої у встановлених законодавствам формах і за допомогою визначених методів діяльності суб'єкти управління фінансовою системою України реалізують функції, спрямовані на врегулювання суспільних відносин у цій сфері [58].

Слушні висновки зробила Т. А. Шумейко в процесі аналізу специфіки адміністративно-правового механізму формування та реалізації державної політики у сфері обігу зброї в Україні. На думку авторки, він є юридичною конструкцією, що ґрунтується на нормах чинного законодавства взаємоузгоджена система нормативно-правових, інституційних, правозастосовних й організаційних форм і засобів, які сукупно, цілісно та послідовно впливають на суб'єктів, відносини та процеси у сфері обігу зброї, виконуючи таким чином завдання формування та реалізації державної політики у відповідній сфері. Вказаний механізм поширюється на: 1) суб'єктів державної влади, на яких офіційно (нормами чинного законодавства) покладено права та обов'язки щодо формування та/або

реалізації вказаної державної політики; 2) суб'єктів громадянського суспільства, які можуть бути долучені до формування та/або реалізації державної політики у сфері обігу зброї в державі в законом визначеній мірі; 3) суб'єктів, які набувають статусу суб'єкта дозвільної системи та суб'єкта відносин стосовно зброї (щодо виготовлення, ремонтування, модернізації, зберігання, придбання, реалізації, передавання, охорони, обліку, використання зброї, а також тирів, стрільбищ тощо) [173, с. 173–174].

Не менш цікаву позицію щодо проблеми адміністративно-правового механізму пропонує у своїх працях С. В. Сірко. Науковець тлумачить вказану категорію в контексті волонтерської діяльності: це – процес упорядкування суспільних відносин, що складаються у сфері волонтерської діяльності, і система певних правових засобів, за допомогою яких держава визначає поведінку суб'єктів цих відносин, таким способом виконуючи регулятивну та охоронну функції для гарантування їхніх прав, свобод і законних інтересів. Аналіз сутності цього механізму дав змогу сформулювати такі висновки: 1) механізм адміністративно-правового забезпечення волонтерської діяльності можливо розглядати крізь призму механізму правового регулювання, оскільки він є однією з провідних категорій адміністративного права, за допомогою якої здійснюється ефективний вплив на поведінку суб'єктів права та має суміжні до виконання завдання поряд з категорією правового забезпечення; 2) механізм адміністративно-правового забезпечення волонтерської діяльності регулює всі суспільні відносини, що виникають у сфері волонтерської діяльності, а його основне завдання − упорядкування всіх можливих суспільних відносин у цій сфері; 3) механізм адміністративно-правового забезпечення волонтерської діяльності − це певний процес, тобто спрямований рух задля досягнення визначеної цілі, а його особливостями є коло учасників, на яке розповсюджується його вплив, і спосіб їхньої поведінки; 5) механізм адміністративно-правового забезпечення волонтерської діяльності спочатку встановлює поведінку певних учасників

відносин у ній, прописуючи їх у правових нормах, лише після цього починається їхня дія та безпосередня реалізація; 6) основною його метою є встановлення певних правових засад, які забезпечують законні права й інтереси суб'єктів цих відносин і слугують гарантом публічних суспільних інтересів у цій сфері [144].

Проведений аналіз дає змогу виокремити характерні властивості поняття «адміністративно-правовий механізм»: 1) це – явища, суворо регламентовані нормами адміністративного законодавства й уточнені положеннями підзаконних, відомчих актів тощо; 2) основу цього механізму становлять інструментальні, прикладні елементи, які застосовуються для досягнення юридично значущого результату; 3) їх реалізація відбувається в діяльності спеціального кола уповноважених законодавством носіїв публічної влади, які становлять інституційну складову механізму; 4) результатом втілення в життя такого механізму є ефективне та успішне виконання суб'єктом публічних повноважень покладених на нього завдань і функцій, за рахунок чого відбувається реалізація певних суспільно-правових відносин та поведінки їх учасників [85].

З огляду на викладене вище, адміністративно-правовий механізм захисту об'єктів критичної інфраструктури Службою безпеки України – це юридична конструкція, яку становлять адміністративно-правові інструменти, що реалізуються уповноваженими органами, підрозділами, окремими посадовими особами Служби з метою впливу на сферу критичної інфраструктури, а також забезпечення стійкості, безпеки функціонування віднесених до неї об'єктів. Структура цього адміністративно-правового механізму охоплює такі складові: 1) адміністративно-правові інструменти захисту об'єктів критичної інфраструктури; 2) інституційна основа реалізації відповідних інструментів; 3) нормативні акти, що визначають порядок і специфіку реалізації останніх [85].

Визначений адміністративно-правовий механізм наділений ознаками, що прямо пов’язані зі статусом СБУ. Так, передусім необхідно відмітити той факт, що процеси та процедури захисту критичної інфраструктури органами та підрозділами СБ України вирізняються таємністю. Це виявляється в обмеженні доступу до більшості внутрішньоорганізаційних документів, виданих у межах роботи Служби. Попри потужну законодавчу основу діяльності органу із забезпечення безпеки і стійкості функціонування об’єктів критичної інфраструктури, підзаконні норми, які показують, яким саме чином відомство приводить до дії положення законів, відсутні в публічному просторі.

Зазначений момент також впливає на інституційну складову адміністративно-правового механізму. У цьому контексті варте уваги питання організаційної структури, основи якої визначено на законодавчому рівні та уточнено на підзаконному рівні. Закон України «Про загальну структуру і чисельність Служби безпеки України» від 20 жовтня 2005 року № 3014-IV визначає, що систему органу становлять: Центральне управління Служби безпеки України; підпорядковані йому регіональні органи; органи військової контррозвідки; навчальні, наукові, науково-дослідні та інші заклади, установи, організації і підприємства Служби безпеки України. Для забезпечення виконання покладених на СБУ завдань у Центральному управлінні Служби безпеки України та підпорядкованих йому органах відповідно до закону створюються і діють функціональні підрозділи: контррозвідки; захисту національної державності; контррозвідувального захисту інтересів держави у сфері інформаційної безпеки; здійснення оперативно-бойової діяльності та спеціальних заходів досудового слідства; охорони державної таємниці; оперативно-технічних заходів; оперативного документування; спеціального зв’язку; організаційного, інформаційно-аналітичного, кадрового, правового, господарського, фінансового та інших

видів забезпечення оперативно-службової діяльності СБУ. При Службі функціонує Антитерористичний центр [110].

Загальна чисельність СБУ визначається в кількості 37 000 осіб, з яких чисельність підрозділу Служби безпеки України, що здійснює оперативно-бойову діяльність та спеціальні заходи (Центр спеціальних операцій «А»), становить 10 000 осіб, в особливий період (крім періоду дії воєнного стану) – у кількості 41 000 осіб. На період дії воєнного стану чисельність підрозділу визначається згідно з Мобілізаційним планом України на особливий період [110].

Більш точний концепт структури затверджено Указом Президента України від 27 грудня 2005 року № 1860/2005 «Питання Служби безпеки України». Зокрема, Указ розкриває складові Центрального управління СБУ, до якого входять: Апарат Голови Служби безпеки України, Департамент інформаційно-аналітичного забезпечення, Департамент контррозвідки, Департамент військової контррозвідки, Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, Департамент захисту національної державності, Департамент оперативно-технічних заходів, Департамент оперативного документування, Департамент охорони державної таємниці та ліцензування, Департамент господарського забезпечення, Головне слідче управління, Головне управління внутрішньої безпеки, Центр спеціальних операцій «А», Головна інспекція Управління роботи з особовим складом, Управління правового забезпечення, Управління забезпечення спеціального оперативного обліку, Управління спеціального зв’язку, військово-медичне управління, Служба мобілізації та територіальної оборони, Фінансово-економічне управління, відділ забезпечення досудового слідства, Управління режиму, документального забезпечення і контролю, Управління внутрішнього аудиту, Центр охорони праці і пожежно-технічного нагляду [99].

Регіональні органи представлено головними управління СБУ в Автономній Республіці Крим, місті Києві та Київській області, Донецькій та Луганській областях, а також управліннями у Вінницькій, Волинській, Житомирській, Закарпатській, Запорізькій та всіх інших областях [99].

Крім того, згідно з Указом, структура СБУ включає навчальні та науково-дослідні заклади й установи, як Національна академія Служби безпеки України, Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України, Галузевий державний архів Служби безпеки України тощо [99]. Попри цілком публічний і відкритий перелік структурних елементів Служби безпеки України, зокрема тих, які беруть участь у забезпеченні захисту об'єктів критичної інфраструктури, специфіка їх діяльності та статусу, наприклад, функції, завдання, повноваження та інші подібні моменти, не освітлені для широкого загалу, а будь-які внутрішньоорганізаційні документи з цього приводу обмежені в доступі до них.

Наступна особливість полягає в тому, що реалізація СБУ адміністративно-правових інструментів захисту критичної інфраструктури здебільшого відбувається в співпраці з іншими уповноваженими в цій сфері діяльності суб'єктами, що пояснюється декількома моментами: по-перше, привалюванням принципу координованості та взаємодії забезпечення СБУ безпеки та стійкості функціонування об'єктів критичної інфраструктури; по-друге, тим фактом, що Служба не чинить безпосереднє управління щодо останніх та має спільно працювати з операторами, секторальними органами тощо.

Наприклад, СБУ є учасником Міжвідомчої комісії з питань захисту критичної інфраструктури згідно з постановою КМУ від 15 липня 2025 року № 885 «Про утворення Міжвідомчої комісії з питань захисту критичної інфраструктури», до якої, крім представників служби, належать голова Держспецзв'язку, голова Міжвідомчої комісії, заступник Державного

секретаря Кабінету Міністрів України, заступник голови Міжвідомчої комісії, заступник секретаря Ради національної безпеки і оборони України (за згодою), заступник Міністра енергетики з питань цифрового розвитку, цифрових трансформацій і цифровізації, заступник Міністра цифрової трансформації, заступник Міністра розвитку громад та територій з питань цифрового розвитку, цифрових трансформацій і цифровізації, заступник Міністра економіки, довкілля та сільського господарства, заступник Міністра охорони здоров'я, заступник Міністра фінансів з питань цифрового розвитку, цифрових трансформацій і цифровізації, заступник Міністра внутрішніх справ, заступник Міністра оборони, заступник Міністра юстиції тощо [133].

СБУ також входить до загальнонаціональної системи реагування на порушення кібербезпеки, зокрема кібертероризм. Вказаному питанню присвячено постанову КМУ від 13 листопада 2025 року № 1471 «Про затвердження Порядку взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності», яка визначає механізм взаємодії: а) національної команди реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA) з правоохоронними, розвідувальними та контррозвідувальними органами, суб'єктами оперативно-розшукової діяльності; б) галузевих і регіональних команд реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) з правоохоронними, розвідувальними та контррозвідувальними органами, суб'єктами оперативно-розшукової діяльності, іншими суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози; в) Національної поліції, СБУ з іншими суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози [117].

Відповідно до положення СБУ отримує інформацію від інших суб'єктів про значні кіберінциденти, кібератаки, кіберзагрози, виявлені або потенційні

вразливості інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, у яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, а також об'єктів критичної інформаційної інфраструктури. СБУ в межах повноважень, визначених законодавством, інформує інших суб'єктів національної системи реагування про актуальні кіберзагрози у сфері державної безпеки та взаємодіє з ними під час реагування на кіберінциденти, кібератаки, кіберзагрози з урахуванням особливостей, встановлених законодавством у зазначеній сфері [117].

Таким чином, саме представлена конструкція та особливості притаманні адміністративно-правовому механізму роботи Служби безпеки України у сфері захисту критичної інфраструктури. Аналіз його сутності показав загальну та досить глибоку інтегрованість СБУ в роботу системи органів забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури. Водночас реалізація інструментарію відповідного механізму відбувається із суворим дотриманням принципу дотримання державної таємниці та не допускає публічного розголошення операційного порядку діяльності СБУ. Подібне ускладнює теоретико-правові дослідження, що цілком логічне з міркувань національної безпеки та ризику потрапляння секретів і специфіки роботи СБУ до осіб та груп, які можуть використати вказану інформацію для завдавання шкоди суспільству або державі.

2.2. Адміністративно-правові інструменти захисту об'єктів критичної інфраструктури Службою безпеки України

Як один з ключових елементів адміністративно-правового механізму діяльності Служби безпеки України із захисту критичної інфраструктури, інструменти мають високий ступінь дослідницької цінності. Адже окрім

функціонального призначення, вони характеризуються унікальним переліком та в певній частині не доступні іншим учасникам публічно-владних відносин у цій сфері. За своєю сутністю категорія походить від терміна «інструмент», який у Великому тлумачному словнику сучасної української мови визначається, як: 1) знаряддя для праці; 2) технічний пристрій, призначений для виконання профілактичних, діагностичних, лікувальних, дослідницьких маніпуляцій і процедур; 3) сукупність знарядь праці; 4) засіб, спосіб для досягнення чогось, реалізації якоїсь мети, цілі; 5) фінансові інструменти: цінні папери, валюта, грошові зобов'язання, страхові поліси, кредитні договори та інші види ринкового фінансового продукту тощо [23, с. 507].

Причому наведена категорія має полігалузеве значення. Так, з точки зору теорії управління це – засоби, реалізації цілей, завдань і функцій управлінської діяльності [53, с. 92]. Згідно з науковими розробками сфери державного управління, інструмент визначено як зовнішнє вираження дій органів і посадових осіб, що здійснюють вплив на суб'єктів суспільно-правових відносин [165, с. 48]. У криміналістичній науці інструмент – це засоби та заходи, що використовуються працівниками правоохоронних органів для розслідування злочинів [135, с. 352].

У загальному значенні інструмент – це сукупність способів, засобів, або реальних приладів, знарядь, що використовуються для провадження якоїсь діяльності. Окрема концептуальна позиція з приводу змісту категорії склалась в адміністративному праві. Так, визначаючи адміністративно-правові інструменти поняттям «інструменти публічного адміністрування», К. Чепкова дійшла висновку, що сутнісну характеристику категорії становлять такі особливості: 1) інструменти публічного адміністрування мають правову природу, що забезпечує їхню легітимність і законність. Вони використовуються в межах компетенції адміністративних органів відповідно до чинного законодавства та слугують засобом правового врегулювання суспільних відносин; 2) ці інструменти є зовнішнім вираженням

адміністративної діяльності адміністративних органів. Вони використовуються виключно для досягнення публічних інтересів, забезпечення правопорядку та реалізації державної політики. Інструменти публічного адміністрування безпосередньо впливають на суспільні процеси, сприяючи забезпеченню публічного адміністрування; 3) інструменти публічного адміністрування відзначаються здатністю до адаптації та гнучкості до викликів у сфері суспільних відносин. Вони можуть змінюватися залежно від потреб суспільства та держави, що дозволяє адміністративним органам оперативно реагувати на виклики часу, такі як кризи, війни або інші надзвичайні ситуації; 4) інструменти публічного адміністрування забезпечують прозорість і підзвітність адміністративних органів. Вони сприяють відкритості процесу прийняття управлінських рішень та контролю з боку громадськості, що підвищує рівень довіри до державних інституцій; 5) інструменти публічного адміністрування мають багатофункціональний характер, оскільки їх застосування дозволяє вирішувати різноманітні питання публічного адміністрування. Вони спрямовані на забезпечення ефективності публічне адміністрування, виконання правових норм та захист прав і свобод громадян [161, с. 48–49; 168].

Аналізуючи особливості змісту вказаної категорії, В. М. Шевченко та Л. В. Зінич зауважують: «У юридичній літературі адміністративно-правові інструменти розглядають під різними кутами зору, зокрема адміністративно-правові інструменти запобігання корупції, адміністративно-правові інструменти у сфері торгівельної діяльності, адміністративно-правові інструменти у сфері національної безпеки й оборони. Поштовхом до широких наукових пошуків є універсальність адміністративно-правових інструментів, саме тому окремі автори класифікують їх за різними критеріями, за рівнем об’єктивізації; за характером дії; залежно від сфери застосовування адміністративно-правових інструментів». Далі науковці

доходять висновку, що вибір адміністративно-правових інструментів обумовлений передусім метою превентивної діяльності, яка вимагає застосування проактивних заходів, а не лише реагування на вчинені порушення. З огляду на це, вони (інструменти) повинні відповідати певним критеріям. Насамперед, за допомогою адміністративно-правових засобів досягається виконання визначених завдань. По-друге, вони застосовуються виключно в межах повноважень державних органів. По-третє, вибір конкретних інструментів залежить від цілі й конкретних завдань. По-четверте, адміністративно-правові інструменти мають чітку законодавчу регламентацію і призводять до певних юридично значущих наслідків [48, с. 122; 170, с. 152].

У багатьох випадках змістову характеристику інструментів надається з огляду на конкретну сферу застосування категорії. Наприклад, І. В. Іщенко адміністративно-правові інструменти діяльності органів Національної поліції як суб'єкта реалізації превентивної функції пропонує розуміти як врегульовану нормами адміністративного права сукупність відповідних форм і методів діяльності поліції, спрямованих на забезпечення та реалізацію превентивної функції держави відповідно до основних напрямів поліції у сфері підтримання публічної безпеки та порядку, забезпечення охорони прав і свобод людини [51, с. 175]. Д. С. Дронік сформулював поняття адміністративно-правових інструментів в діяльності поліції та розтлумачив їх таким чином: зовнішнє організаційно-правове, практичне вираження їх діяльності у сфері забезпечення публічного порядку й безпеки, дотримання прав і законних інтересів громадян, забезпечення безпеки дорожнього руху, протидії злочинності у вигляді сукупності дій правового та неправового характеру, що здійснюються уповноваженими посадовими особами патрульної поліції в межах їхньої компетенції [39, с. 121, 122].

Своєю чергою О. П. Махмурова-Дишлюк у контексті дослідження проблеми адміністративно-правового забезпечення прав і свобод людини в

умовах збройних конфліктів зазначає, що «основні, як законодавчо сформовані, так і визначені теорією права, засади так би й залишилися нереалізованими позитивними чинниками, якби не було в арсеналі суб'єктів публічної адміністрації певних інструментів, за допомогою яких вони б забезпечували права свободи та інтереси приватних осіб і публічний інтерес держави». Вказані інструменти вчений визначає як юридичні знаряддя адміністративної діяльності суб'єктів публічної адміністрації (правові, організаційно-правові й організаційні), що реалізуються в межах відповідної, визначеної законом компетенції з метою захисту прав, свобод та інтересів осіб, які постраждали внаслідок збройних конфліктів в Україні [76, с. 42].

Адміністративно-правові інструменти взаємодії суб'єктів сектору безпеки й оборони А. Г. Вахров визначає як сукупність заходів і способів роботи уповноважених державних суб'єктів, до переліку яких відносить: нормотворчі (встановлення правил, процедур, зобов'язань тощо), організаційні (збір інформації, підготовка документів тощо), забезпечувальні (методичний супровід, технічне та матеріальне оснащення, фінансування тощо) та управлінські (заохочення, переконання, контрольно-наглядова діяльність тощо) [20, с. 62].

О. Д. Кузьмічов, ураховуючи позиції Р. С. Мельника та С. О. Мосьондза, визначає адміністративно-правові інструменти, які використовує публічна адміністрація у сфері забезпечення продовольчої безпеки, таким чином: «Урегульовані нормами загального адміністративного права та права продовольчої безпеки як галузі особливого адміністративного права юридичні засоби, використовуючи які, публічна адміністрація виконує ті завдання і функції, які покладені на неї в цій сфері публічного адміністрування». До переліку ключових ознак цих інструментів автор зараховує такі: 1) підзаконність, яка виявляється в тому, що такі адміністративно-правові інструменти застосовуються на підставі та для виконання завдань і функцій, які покладені на публічну адміністрацію в цій

сфері публічного адміністрування; 2) обов'язковість – суть цієї ознаки адміністративно-правових інструментів полягає у тому, що вони містять обов'язкові до виконання усіма фізичними та юридичними особами приписи; правомірність, яка виявляється у тому, що відповідний адміністративно-правовий інструмент використовується в межах компетенції та повноважень суб'єкта публічної адміністрації, який його застосовує; 3) юридична значущість. Ця ознака адміністративно-правових інструментів полягає у тому, що їхнє застосування породжує юридичні наслідки для адресатів відповідних правових інструментів; 4) належна оформленість, яка полягає в тому, що інструменти діяльності публічної адміністрації у випадках, визначених законодавством, мають відповідати певним вимогам щодо їхнього оформлення; 5) вони є зовнішнім виразом форми адміністративної діяльності публічної адміністрації; 6) такі інструменти відображають правову динаміку публічного адміністрування; 7) їх вибір зумовлюється специфікою поставленої мети щодо певного об'єкта публічного впливу, що встановлює найбільш ефективний варіант діяльності [69, с. 123–124; 78, с. 152].

У цьому контексті Н. П. Новак і Є. В. Сердюк зауважують, що адміністративні інструменти становлять системну сукупність правових, організаційних та інформаційних дій, спрямованих на досягнення публічно значущих результатів у межах компетенції адміністративних органів. У сфері запобігання тінізації економіки вони забезпечують реалізацію контролю, планування, правового впливу, електронного врядування та інших форм адміністративної діяльності. «Такі інструменти використовуються для виявлення та попередження нелегальної економічної активності, формування прозорого підприємницького середовища й підвищення підзвітності суб'єктів господарювання. Їх ефективність залежить від нормативної визначеності, узгодженості механізмів впливу та здатності реагувати на динаміку економічних загроз», – пишуть автори [91, с. 293].

Оцінка значного комплексу наукових підходів щодо змісту і значення адміністративно-правових інструментів дає підстави виокремити такі ознаки вказаної категорії: 1) зміст інструментів становлять форми, заходи, засоби та способи публічно-управлінської, офіційної діяльності суб'єктів владних повноважень щодо реалізації покладених на них законодавством функцій і завдань у певних сферах та галузях суспільних відносин; 2) перелік доступних до використання адміністративно-правових інструментів визначається нормативно-правовими засадами діяльності кожного окремого суб'єкта владних повноважень; 3) адміністративно-правові інструменти мають різний обсяг, зміст і результат здійснення. Це гнучка категорія, у якій може знаходити вираження як об'ємна, стратегічно орієнтована активність, так і дії, спрямовані на отримання певного оперативного, точкового результату; 4) зазвичай результат використання адміністративно-правових інструментів – це приведення до дії приписів нормативно-правових актів, за рахунок чого упорядковуються суспільно-правові відносини певного типу та поведінка їх учасників.

Адміністративно-правові інструменти захисту об'єктів критичної інфраструктури Службою безпеки України – це передбачені законодавством України форми, засоби, способи та заходи, які використовуються органами й підрозділами СБУ для формування необхідного стану безпеки об'єктів критичної інфраструктури, підтримання стійкості їх функціонування, а також безпосереднього захисту від будь-яких загроз і ризиків.

Чинне законодавство України наділяє СБУ широким колом адміністративних інструментів, які доцільно поділити на дві великі групи, а саме: загальні та спеціальні. Перші – це інструменти, використання яких детерміновано участю СБУ в правовідносинах із забезпеченням безпеки та стійкості функціонування об'єктів критичної інфраструктури та притаманні діяльності інших суб'єктів даної сфери. Наприклад, сюди належить планування заходів щодо забезпечення стійкості й захисту об'єктів критичної

інфраструктури. Стаття 22 Закону України «Про критичну інфраструктуру» від 16 листопада 2021 року № 1882-IX визначає, що для організації функціонування національної системи захисту критичної інфраструктури Кабінетом Міністрів України, центральними органами виконавчої влади, місцевими органами виконавчої влади (військово-цивільними адміністраціями – у разі створення), органами місцевого самоврядування розробляються та затверджуються відповідні плани та програми реагування на кризові ситуації. Так, Національна поліція України, Національна гвардія України, Служба безпеки України, Збройні Сили України, Державна служба України з питань надзвичайних ситуацій та інші складові сектору безпеки і оборони в межах компетенції здійснюють планування відповідних заходів із захисту критичної інфраструктури [123].

Наступним адміністративним інструментом загального значення є моніторинг рівня безпеки об’єктів критичної інфраструктури, який затверджується Законом України «Про критичну інфраструктуру» від 16.11.2021 №1882-IX, а операційні особливості здійснення уточнено Постановою КМУ «Про затвердження Порядку проведення моніторингу рівня безпеки об’єктів критичної інфраструктури» від 22 липня 2022 року № 821. Відповідно до зазначених нормативних актів, метою проведення моніторингу є встановлення відповідності стану захищеності об’єкта критичної інфраструктури вимогам законодавства, достовірності наданої інформації визначеним суб’єктам національної системи захисту критичної інфраструктури, надання методичної допомоги операторам об’єктів критичної інфраструктури в удосконаленні системи захисту критичної інфраструктури. Моніторинг передбачає здійснення заходів, спрямованих на отримання, узагальнення, оброблення, збереження та проведення аналізу інформації про фактичний стан захищеності об’єкта критичної інфраструктури, дотримання вимог законодавства у сфері критичної інфраструктури, здійснення контролю за ризиками безпеки й удосконалення

заходів, які здійснюються для забезпечення безпеки та стійкості об’єкта критичної інфраструктури, а також на визначення перспектив подальшого функціонування і розвитку національної системи захисту критичної інфраструктури. Проведення моніторингу здійснюється шляхом проведення один раз на три роки оцінки стану захищеності об’єктів критичної інфраструктури секторальними та функціональними органами у сфері захисту критичної інфраструктури [118; 123].

За результатами оцінки стану захищеності суб’єктом моніторингу складають акт оцінки стану захищеності, у якому зазначають: а) критерії оцінки стану захищеності та результати оцінки за кожним критерієм; б) дані про стан захищеності об’єкта критичної інфраструктури, який визначається відповідно до критеріїв оцінки стану захищеності та оцінюється як «забезпечує», «обмежено забезпечує», «не забезпечує»; в) дані про порушення (у разі їх наявності) вимог законодавства у сфері критичної інфраструктури, а також інші недоліки, що впливають на захищеність об’єкта критичної інфраструктури; г) результати оцінки стану безпеки об’єкта критичної інфраструктури суб’єктом моніторингу; д) пропозиції щодо удосконалення системи захисту об’єктів критичної інфраструктури, усунення порушень та/або недоліків (у разі їх наявності) із зазначенням строків вжиття відповідних заходів [118; 123].

Наступними варто виділити адміністративно-правові інструменти міжвідомчого співробітництва СБУ та інших суб’єктів національної системи захисту критичної інфраструктури. Сюди відноситься обмін інформацією, регламентований постановою КМУ від 14 жовтня 2022 року № 1174 «Про затвердження Регламенту обміну інформацією між суб’єктами національної системи захисту критичної інфраструктури» [81; 119].

Згідно до положень постанови інформаційна взаємодія забезпечується шляхом послідовного обміну інформацією між суб’єктами національної системи захисту критичної інфраструктури, що здійснюється

відповідальними особами, визначеними такими суб'єктами, з використанням засобів електронних комунікацій, національної системи конфіденційного зв'язку, спеціального зв'язку, шифрувального зв'язку та інформаційно-комунікаційних систем. У штатному режимі, режимі готовності та запобігання реалізації загроз, а також у режимі відновлення штатного функціонування обмін інформацією щодо функціонування об'єктів критичної інфраструктури здійснюється щодня шляхом інформування засобами зв'язку з одночасним письмовим інформуванням. Обмін інформацією здійснюється послідовно між операторами критичної інфраструктури та секторальними органами у сфері захисту критичної інфраструктури, між секторальними органами та уповноваженим органом у сфері захисту критичної інфраструктури. У разі виникнення кризової ситуації на об'єктах критичної інфраструктури обмін інформацією здійснюється протягом 30 хвилин з моменту отримання операторами інформації про її виникнення. Обмін інформацією здійснюється послідовно між операторами та секторальними органами, між секторальними органами та уповноваженим органом, а також між секторальними органами та Кабінетом Міністрів України. Усне інформування протягом години підтверджується секторальними органами письмово шляхом надсилання повідомлення за допомогою шифрувального зв'язку або спеціальної інформаційної системи уповноваженому органу та Кабінетові Міністрів України [119].

Водночас інформаційний обмін – це не єдиним адміністративний інструмент вказаного типу. Багато інших прикладів можна виділити в контексті взаємодії СБУ з окремими суб'єктами національної системи захисту об'єктів критичної інфраструктури. Наприклад, постановою КМУ від 13 листопада 2025 року № 1471 «Про затвердження Порядку взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-

розшукової діяльності» визначено, що взаємодія вказаних суб'єктів, до переліку яких належить СБУ, охоплює: проведення спільних заходів під час реагування на кіберінциденти, кібератаки, кіберзагрози; надання та отримання в установленому законодавством порядку доступу до технічних та інших деталей кіберінциденту чи кібератаки (відомостей про кіберінцидент чи кібератаку) для проведення слідчих (розшукових) дій, контррозвідувальних або оперативно-розшукових заходів; функціонування міжвідомчих груп із реагування на кіберінциденти, кібератаки, кіберзагрози або кризову ситуацію у сфері кібербезпеки [117].

Звернутися також варто до положень спільного наказу СБУ та Міноборони від 13 січня 2014 року № 24/6 «Про затвердження Інструкції про порядок взаємодії Державної служби України з надзвичайних ситуацій і Служби безпеки України у сфері запобігання виникненню та реагування на надзвичайні ситуації», згідно з яким взаємодія ДСНС України та СБУ здійснюється шляхом: обміну інформацією про загрозу або виникнення надзвичайних ситуацій; проведення спільних оперативних нарад керівного складу ДСНС України, головних управлінь (управлінь) ДСНС України в Автономній Республіці Крим, областях, містах Києві та Севастополі та їх структурних підрозділів з керівним складом СБУ, відповідних регіональних органів СБУ; здійснення спільних заходів за планами, що розробляються на державному та регіональному рівнях; проведення командно-штабних, тактико-спеціальних навчань, спільних тренувань та занять; здійснення інших заходів, передбачених чинним законодавством [111].

Поряд із загальним переліком адміністративно-правових інструментів захисту критичної інфраструктури в роботі Служби безпеки України мають місце спеціальні, які виходять із особливого юридичного статусу СБУ та покладених на відомство функцій і повноважень. Наприклад, сюди належать адміністративні інструменти, передбачені Законом України «Про боротьбу з тероризмом» від 20 березня 2003 року № 638-IV. Як головний орган у

загальнодержавній системі боротьби з терористичною діяльністю СБУ здійснює боротьбу з тероризмом наступним чином: збирає інформацію про діяльність іноземних та міжнародних терористичних організацій; забезпечує через Антитерористичний центр при Службі безпеки України організацію і проведення антитерористичних заходів, координацію діяльності суб'єктів боротьби з тероризмом відповідно до визначеної законодавством України компетенції; забезпечує у взаємодії з розвідувальними органами України безпеку від терористичних посягань установ України за межами її території, їх співробітників та членів їхніх сімей; надає рекомендації, пропозиції, застереження та приписи іншим суб'єктам боротьби з тероризмом з питань боротьби з тероризмом, які є обов'язковими для врахування та виконання. Крім того, Служба безпеки України спільно з центральним органом виконавчої влади, що реалізує державну політику у сфері цивільного захисту, через свої територіальні органи (у разі їх утворення) здійснюють антитерористичну підготовку населення та науково-методологічне забезпечення антитерористичної діяльності з метою підготовки населення до дій в умовах терористичного акту [106].

Крім визначеного, СБУ, а також інші суб'єкти боротьби з тероризмом відповідно до Закону зобов'язані: 1) взаємодіяти з метою припинення кримінально протиправної діяльності осіб, причетних до тероризму, зокрема міжнародного, фінансування, підтримки чи вчинення терористичних актів та кримінальних правопорушень, які скоєні з терористичною метою; 2) здійснювати обмін інформацією щодо: заволодіння чи виникнення загрози заволодіння терористичними групами (терористичними організаціями) зброєю, вибуховими речовинами, іншими засобами масового ураження; перетинання державного кордону України її громадянами, іноземцями та особами без громадянства з метою вчинення терористичних актів; виявлених у пасажирів проїзних документів, що дають право на проїзд у транспортних засобах міжміського та міжнародного сполучення, з ознаками підроблення;

використання чи загрози використання терористами, терористичними групами чи терористичними організаціями засобів зв'язку та комунікаційних технологій; 3) сприяти забезпеченню ефективного прикордонного контролю, контролю за видачею документів, що посвідчують особу, та проїзних документів з метою запобігання їх фальсифікації, підробленню або незаконному використанню; 4) запобігати діям або пересуванню терористів, терористичних груп чи терористичних організацій, а також осіб, які підозрюються у вчиненні терористичних актів або причетності до міжнародних терористичних груп чи організацій; 5) припиняти спроби іноземців, щодо яких є дані про їх причетність до міжнародних терористичних груп чи організацій, здійснювати транзитний проїзд через територію України; 6) надавати персональні дані громадян України, іноземців або осіб без громадянства, що перебувають на території України, на підставі запитів (звернень) державних органів, які мають право на здійснення контррозвідувальної діяльності [106].

Спеціальними також є інструменти, які застосовуються органами та підрозділами СБУ в межах виконання норм Закону України «Про контррозвідувальну діяльність» від 26 грудня 2002 року № 374-IV. Відповідно до вказаного нормативного акта, контррозвідувальна діяльність – це спеціальний вид діяльності у сфері забезпечення державної безпеки, яка здійснюється з використанням системи контррозвідувальних, пошукових, режимних, адміністративно-правових заходів, спрямованих на попередження, своєчасне виявлення і запобігання зовнішнім та внутрішнім загрозам безпеці України, розвідувальним, терористичним та іншим протиправним посяганням спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на інтереси України. Метою контррозвідувальної діяльності є попередження, своєчасне виявлення і запобігання зовнішнім та внутрішнім загрозам безпеці України, припинення розвідувальних, терористичних та інших протиправних посягань

спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на державну безпеку України, усунення умов, що їм сприяють, та причин їх виникнення. Своєю чергою завданнями контррозвідувальної діяльності визначено: добування, аналітична обробка та використання інформації, що містить ознаки або факти розвідувальної, терористичної та іншої діяльності спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на шкоду державній безпеці України; протидія розвідувальній, терористичній та іншій діяльності спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на шкоду державній безпеці України; розроблення і реалізація заходів щодо запобігання, усунення та нейтралізації загроз інтересам держави, суспільства та правам громадян [122].

У межах реалізації контррозвідувальної діяльності органи та підрозділи СБУ мають право: 1) витребовувати, збирати і вивчати, за наявності визначених законом підстав, документи та відомості, що характеризують діяльність підприємств, установ, організацій, а також спосіб життя окремих осіб, джерела і розміри їх доходів для попередження та припинення розвідувальних, терористичних та інших протиправних посягань на державну безпеку України; 2) перебувати в порядку, погодженому з керівниками органів охорони державного кордону Державної прикордонної служби України, для вжиття контррозвідувальних заходів у межах прикордонної смуги, контрольованого прикордонного району, у пунктах пропуску через державний кордон і територіальному морі України; 3) у невідкладних випадках під час здійснення контррозвідувальних заходів безперешкодно користуватися засобами зв’язку, що належать підприємствам, установам і організаціям, а засобами зв’язку, що належать громадянам, – за їх згодою, з наступним відшкодуванням витрат за їх вимогою; 4) в інтересах забезпечення державної безпеки та виконання завдань контррозвідувальної діяльності

організовувати, координувати і проводити наукові та науково-технічні дослідження, створювати в порядку, визначеному законодавством України, відповідні наукові установи та міжвідомчі координаційно-дорадчі органи; 5) зберігати, носити, застосовувати, використовувати зброю, спеціальні засоби, вживати заходів фізичного впливу відповідно до законів України та інших актів законодавства України, провозити зброю та спеціальні засоби в усіх видах транспорту тощо [122].

Отже, адміністративно-правові інструменти є важливою складовою діяльності Служби безпеки України у сфері захисту критичної інфраструктури, оскільки саме через них забезпечується превентивний, регулятивний та охоронний вплив держави на стратегічно значущі об'єкти. Попри те, що СБУ традиційно асоціюється передусім з кримінально-процесуальними формами протидії злочинності, її роль як суб'єкта публічної адміністрації є не менш значущою. Використовуючи надані законом повноваження, СБУ формує та реалізує комплекс управлінських і контрольно-наглядових механізмів, спрямованих на попередження загроз, підтримання стійкості та безперебійності функціонування критичної інфраструктури. Крім того, у цьому контексті Служба не обмежується загальними адміністративними засобами, адже її спеціальний статус передбачає можливість застосування більш складних правових інструментів, характерних для контррозвідувальної, антитерористичної та інформаційно-аналітичної діяльності. Таким чином, саме поєднання цих загальних і спеціальних адміністративно-правових механізмів забезпечує комплексний, системний характер державного впливу на сферу, що має вирішальне значення для національної безпеки [81].

2.3. Взаємодія Служби безпеки України з державними та громадськими інституціями в процесі запобігання несанкціонованому втручанню у функціонування об’єктів критичної інфраструктури

В умовах зростання гібридних загроз і посилення залежності держави від сталого функціонування критичної інфраструктури питання забезпечення її захисту набуває особливої ваги. Сучасні виклики демонструють, що несанкціоноване втручання в енергетичні, транспортні, інформаційно-комунікаційні та інші життєво важливі системи може мати масштабні наслідки для національної безпеки, економічної стабільності та суспільного добробуту. У цьому контексті Служба безпеки України відіграє провідну роль як ключовий суб’єкт сектору безпеки, відповідальний за протидію загрозам, які здатні поставити під загрозу функціонування держави. Водночас ефективність цієї діяльності неможлива без налагодженої, системної та багаторівневої взаємодії з іншими державними органами й громадськими інституціями. Саме міжвідомча координація, обмін інформацією, спільна оцінка ризиків і залучення громадського середовища формують підґрунтя для створення комплексної системи запобігання несанкціонованим втручанням у роботу критично важливих об’єктів.

У сучасному філософському дискурсі поняття взаємодії використовується для опису впливів, які різні об’єкти чинять один на одного, а також для відображення зв’язків між ними у контексті людського буття, діяльності та пізнання. Це поняття охоплює як прямі, так і зворотні впливи, що виявляються через обмін речовиною, енергією та інформацією між об’єктами, живими організмами та навколишнім середовищем, а також через різні форми кооперації людей у ситуаціях спільної діяльності. Взаємодія включає як безпосередні, так і опосередковані зв’язки між системами та елементами. Класична механіка демонструє приклади прямих взаємодій, досліджуючи зіткнення та відштовхування тіл, під час яких рух передається

від одного об’єкта до іншого. У соціальній сфері взаємодію можна спостерігати у формі безпосереднього міжособистісного спілкування. Таке трактування поняття є універсальним і дозволяє застосовувати його для опису найрізноманітніших процесів та форм вияву людської свідомості [93]. Своєю чергою в соціології взаємодія – це форма соціальних зв’язків, що реалізуються в обміні діяльністю, інформацією, досвідом, здібностями, уміннями, навичками та у взаємному впливі людей, соціальних спільнот. Об’єктивною основою соціальної взаємодії є спільність чи розбіжність інтересів, близьких чи віддалених цілей, поглядів. Її посередниками, проміжними її ланками, наприклад у сфері праці, є знаряддя і предмети праці, матеріальні й духовні блага та досвід. Інтеракція (тобто соціальна взаємодія) – динамічна взаємодія і співвідношення між двома чи більше перемінними, коли величина одної перемінної впливає на величину інших перемінних. Головна особливість соціальної взаємодії, наголошує Г. В. Дворецька, полягає в тому, що вона є процесом впливу індивідів один на одного. Інакше кажучи, у процесі взаємодії має місце вплив свідомості, інтересів, потреб, поведінкових установок однієї людини на іншу та навпаки. Соціальні взаємодії за формами вияву є більш складними, ніж соціальні дії. До складу соціальних взаємодій входять окремі соціальні дії, статуси, ролі, відносини, символи тощо. Соціальна взаємодія відрізняється від дії зворотним зв’язком. Дія індивіда може бути спрямована та не спрямована на іншого індивіда. Отже, взаємодія – двосторонній процес обміну діями між людьми [28].

Цікаву позицію обстоює В. В. Топчій, акцентуючи на тому, що всі наявні визначення взаємодії об’єднує спільна думка, згідно з якою взаємодія – це передусім взаємний зв’язок між двома (або більше) суб’єктами (об’єктами), які здійснюють вплив один на одного. Усі суб’єкти (об’єкти) взаємодії є складовими певної системи. Проте ми дійшли висновку, що наведені визначення слід поділити на дві групи: взаємодія неживих об’єктів

та явищ і взаємодія наділених розумом живих суб'єктів. Відмінність між ними полягає в тому, що в межах взаємодії неживі об'єкти та явища здійснюють безпосередній або опосередкований вплив один на одного, викликаючи нову дію (наприклад, передача енергії під час контакту). Натомість під час взаємодії наділених розумом живих суб'єктів їх діяльність цілеспрямована, осмислена, має мету. Взаємодія суб'єктів виникає не в результаті здійснення впливу один на одного, а з усвідомлення необхідності здійснення спільних дій, спрямованих на досягнення спільної мети. Під час взаємодії суб'єкти впливають на якісні характеристики один одного [156, с. 166].

Досліджуючи поняття «взаємодія» з точки зору теорії управління, Л. Г. Шморгун зазначає, що взаємодія – це процес безпосереднього чи опосередкованого впливу об'єктів (суб'єктів) один на одного, що породжує їх взаємні зумовленість і зв'язок. У взаємодії реалізується ставлення людини до іншої людини як до суб'єкта, у якого є власний світ. Під взаємодією в соціальній філософії та психології, а також теорії менеджменту, крім того, розуміється не лише вплив людей один на одного, а й безпосередня організація їх спільних дій, що дає змогу групі реалізувати спільну для її членів діяльність [172]. Таким чином, підсумовує згаданий вище автор, взаємодія є систематичним і постійним учиненням дій, спрямованих на те, щоб викликати відповідну реакцію з боку інших людей. Спільне життя і діяльність людей як у суспільстві, так і в організації на відміну від індивідуального має більш жорсткі обмеження будь-яких виявів активності чи пасивності. У процесі реальної взаємодії формуються також адекватні уявлення працівника про себе та інших людей. Взаємодія людей – провідний фактор у регуляції їх самооцінок і поведінки в суспільстві [172].

Аналізуючи різні наукові позиції, О. Ю. Процких поділяє позицію А. М. Подоляка, який терміном «взаємодія» пропонує позначати погоджену діяльність різних суб'єктів для реалізації спільних дій щодо виконання

завдань із досягнення загальних цілей правоохоронної діяльності. Водночас взаємодія може здійснюватися на двох рівнях – спільної організації (планування) співпраці керівниками взаємодіючих сторін і безпосередньої реалізації (на рівні виконавців) [104, с. 338–339; 134]. Згаданий вище науковець до характерних ознак взаємодії відносить: 1) погодженість діяльності як обов'язкову ознаку взаємодії елементів системи, що використовується у військовій науці. Вона впливає на спільні дії, об'єднуючи їх у єдине ціле – систему. Погодженість передбачає низку відповідних дій та використання загальних або взаємодоповнюючих форм і методів реалізації цих дій; 2) певну кількість суб'єктів. Допускається участь як мінімум двох сторін, причому кожну з цих сторін можуть представляти кілька учасників; 3) поєднання зусиль суб'єктів, що визначають відносини співпраці між ними та мають спільні цілі й інтереси для взаємодіючих сторін. Виходячи з практичних потреб і теоретичних засад, можна виділити дві основні концепції взаємодії. Перша полягає в тому, що взаємодія – це погоджена діяльність. Вказана концепція призводить до виникнення ілюзії прямої регламентації владного характеру. Сутність другої концепції полягає в тому, що взаємодія – це доповнення можливостей один одного на умовах спільної користі від цього для всіх учасників взаємодії. Саме друга концепція забезпечує об'єктивність взаємозв'язків між суб'єктами. Взаємодія не може відбутися без ініціативи як мінімум однієї зі сторін. Крім того, необхідна наявність зустрічних пропозицій іншої сторони щодо ініціатора; 4) партнерський характер відносин, що здійснюється в межах співпраці, причому сторони рівні й незалежні одна від одної; 5) законність, відповідно до якої реалізуються дії та використовуються форми, методи, сили й засоби [104, с. 338–339; 134].

Таким чином, взаємодія Служби безпеки України з державними і громадськими інституціями в процесі запобігання несанкціонованому втручанню у функціонування об'єктів критичної інфраструктури – це

урегульована нормами чинного законодавства система узгоджених дій, заходів, інформаційного обміну тощо між СБУ та іншими уповноваженими органами державної влади, органами місцевого самоврядування, суб'єктами управління критичною інфраструктурою та інститутами громадянського суспільства, яка спрямована на виявлення, запобігання і нейтралізацію загроз незаконного втручання, а також на забезпечення безперервності та стійкості функціонування об'єктів критичної інфраструктури.

Варто зазначити, що взаємодії у сфері критичної інфраструктури приділено окрему увагу в ст. 24 Закону України «Про критичну інфраструктур». Зокрема, у документі зазначено, що для забезпечення безпеки і стійкості критичної інфраструктури до загроз усіх видів, реалізації національних інтересів, функціонування суспільства та забезпечення соціально-економічного розвитку національна система захисту критичної інфраструктури взаємодіє з іншими системами захисту у сфері національної безпеки: 1) з єдиною державною системою запобігання, реагування та припинення терористичних актів та мінімізації їх наслідків, з територіальною та функціональною підсистемами, структурними підрозділами суб'єктів боротьби з тероризмом; 2) з національною системою захисту інформаційних ресурсів в інформаційно-телекомунікаційних системах; 3) з національною системою кібербезпеки; 4) з правоохоронними органами у сфері протидії злочинності, а також з контррозвідувальними та розвідувальними органами у сфері забезпечення державної безпеки; 5) з об'єднаною цивільно-військовою системою організації повітряного руху України; 6) з єдиною державною системою цивільного захисту; 7) з державною системою фізичного захисту з питань охорони і оборони важливих державних об'єктів, захищеності та охорони ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання державної власності, запобігання диверсіям, крадіжкам або будь-якому іншому неправомірному вилученню радіоактивних матеріалів, протидії незаконному використанню безпілотних

літальних апаратів; 8) із системою захисту персональних даних [123]. Окрім того, у частині 2 згаданої вище статті Закону визначено, що взаємодія між державними системами захисту здійснюється в разі загрози виникнення або виникнення: 1) протиправних дій (у тому числі із застосуванням безпілотних літальних апаратів), захоплення об'єктів критичної інфраструктури або важливих державних об'єктів, що загрожують безпеці громадян і порушують функціонування систем життєзабезпечення; 2) диверсій, терористичних актів, викрадення, навмисного знищення, пошкодження майна та інших дій на об'єктах критичної інфраструктури, важливих державних об'єктах, внаслідок яких загинули люди або заподіяно значну матеріальну шкоду; 3) масштабних кібератак, актів кібертероризму проти систем управління, операційних та інших систем об'єктів критичної інфраструктури; 4) надзвичайних ситуацій або інших небезпечних подій на об'єктах критичної інфраструктури та важливих державних об'єктах; 5) аварій та технічних збоїв, кризових ситуацій на об'єктах критичної інфраструктури, що створюють загрозу життю та здоров'ю персоналу таких об'єктів та місцевого населення [123]. Таким чином, вказані вище положення ст. 24 Закону України «Про критичну інфраструктуру» мають системоутворююче значення, оскільки встановлює базовий обов'язок суб'єктів критичної інфраструктури брати активну участь у забезпеченні її захисту та взаємодіяти з державними органами. Це положення спрямоване на формування інтегрованої моделі безпеки, у якій стійкість критичних систем розглядається як результат узгоджених дій держави та операторів, а не як виключна компетенція однієї сторони. Норма є прогресивною та відповідає сучасним підходам до управління ризиками, адже підсилює відповідальність операторів і водночас створює юридичні підстави для формалізованої координації з органами безпеки в умовах зростання гібридних і техногенних загроз.

Крім того, Законом передбачено, що організація взаємодії між суб'єктами національної системи захисту критичної інфраструктури здійснюється шляхом: 1) оперативного обміну інформацією щодо виконання завдань із захисту критичної інфраструктури; 2) проведення спільних оперативних нарад керівного складу уповноваженого органу у сфері захисту критичної інфраструктури України, центральних і територіальних органів Національної поліції України, Служби безпеки України, Національної гвардії України, Збройних Сил України, Державної служби України з питань надзвичайних ситуацій та інших заінтересованих державних органів; 3) здійснення спільних заходів із захисту критичної інфраструктури за планами, що розробляються на загальнодержавному, галузевому, регіональному місцевому та об'єктовому рівнях; 4) проведення спільних командно-штабних, тактико-спеціальних навчань, спільних тренувань і занять із захисту, охорони, оборони, припинення злочинних дій, інцидентів та кібератак проти об'єктів критичної інформаційної інфраструктури; 5) регулярного уточнення розрахунків сил та засобів, що залучаються до спільного виконання завдань із захисту об'єктів критичної інфраструктури та важливих державних об'єктів; 6) спільних заходів з припинення протиправних дій проти об'єктів критичної інфраструктури або важливих державних об'єктів, що загрожують безпеці громадян і порушують функціонування таких об'єктів; 7) участі в реагуванні та ліквідації наслідків інцидентів, кризових ситуацій на об'єктах критичної інфраструктури; 8) координації дій з підтримання або відновлення правопорядку в місцях розташування об'єктів критичної інфраструктури у разі виникнення кризових ситуацій; 9) здійснення інших заходів, передбачених законодавством [123].

В окремих випадках взаємодія приймає індивідуальний характер з конкретними суб'єктами національної системи захисту критичної інфраструктури. Наприклад, спільним наказом СБУ та Міністерства оборони України затверджено Інструкцію про порядок взаємодії Державної служби

України з надзвичайних ситуацій і Служби безпеки України у сфері запобігання виникненню та реагування на надзвичайні ситуації від 13 січня 2014 року № 24/6. Відповідно до положень вказаного документа, взаємодія здійснюється в разі загрози або виникнення: 1) актів технологічного тероризму; 2) катастроф та аварій, пов'язаних з використанням зброї та військової техніки; 3) техногенних або природних катастроф та аварій на військових об'єктах, унаслідок яких загинули люди або заподіяно значну матеріальну шкоду; 4) диверсій, терористичних актів, викрадення, навмисного знищення, пошкодження майна та інших дій на військових об'єктах, внаслідок яких загинули люди або заподіяно значну матеріальну шкоду; 5) суттєвого погіршення технічного стану гідротехнічних споруд каскаду водосховищ на річці Дніпро; 6) небезпечних подій на атомних електростанціях та інших ядерних об'єктах України, що можуть призвести до порушення ядерної безпеки, аварійної зупинки ядерної установки, виникнення надзвичайної ситуації, втрати контролю за ядерними матеріалами; 7) стихійних лих, епідемій, епізоотій та інших надзвичайних ситуацій [111].

Переходячи безпосередньо до характеристики взаємодії Служби безпеки України з державними і громадськими інституціями в процесі запобігання несанкціонованого втручання у функціонування об'єктів критичної інфраструктури, варто зазначити, що в реаліях сьогодення така спільна діяльність зазнала суттєвих змін, а роль СБУ значно зросла. Крім того, розширились також напрями такої спільної діяльності. Так, СБУ активно почала працювати у складі міжвідомчих робочих груп. Наприклад, В. С. Коренькова зазначає, що спільна робоча група – це група з представників різних органів виконавчої влади, які разом працюють над спільними завданнями. Робочі групи зазвичай мають тимчасовий характер і строюються для глибокого вивчення конкретних питань і підготовки на підставі чого відповідних доповідей, звітів для їх обговорення на

міжвідомчих нарадах, колегіях. Важливість вказаної форми координації полягає в тому, що в її межах забезпечується максимально професійний підхід до конкретних, найбільш складних завдань. До участі в робочих групах мають залучатися найбільш кваліфіковані працівники, які володіють знаннями, навичками та досвідом, що необхідні для виконання відповідних завдань, які вміють і хочуть працювати в групі з іншими фахівцями [65]. На нашу думку, створення міжвідомчих робочих груп у сфері запобігання несанкціонованому втручанню у функціонування об'єктів критичної інфраструктури має важливе значення, адже саме такий формат взаємодії забезпечує цілісність та узгодженість дій між СБУ та іншими державними та недержавними інституціями. Сучасні загрози критичній інфраструктурі мають комплексний характер, поєднуючи кібернетичні, технічні, інформаційні та організаційні складові, і жоден орган не володіє одноосібно всією необхідною інформацією, ресурсами чи компетенціями для їхнього ефективного нейтралізування. Таким чином, міжвідомча робоча група дозволяє об'єднати розрізнені можливості, експертизу та інформаційні масиви, що перебувають у віданні різних органів влади, зменшуючи ризики інформаційних прогалин, дублювання функцій або несинхронних рішень.

Так, Міністерство економічного розвитку і торгівлі та СБУ створили міжвідомчу експертну групу з питань захисту критичної інфраструктури, яка стане платформою для створення Національного переліку об'єктів критичної інфраструктури, а також визначення основ категоризації і паспортизації зазначених об'єктів [80]. Зокрема, постановою Кабінету Міністрів України від 15 липня 2025 року № 885 «Про утворення Міжвідомчої комісії з питань захисту критичної інфраструктури» було закріплено, що основними завданнями Міжвідомчої комісії є: 1) сприяння забезпеченню взаємодії, координації діяльності органів виконавчої влади та інших державних органів, органів місцевого самоврядування, операторів критичної інфраструктури та інших підприємств, установ, організацій з питань захисту критичної

інфраструктури; 2) підготовка пропозицій та рекомендацій щодо формування і реалізації державної політики у сфері захисту критичної інфраструктури; 3) визначення шляхів, механізмів і способів вирішення проблемних питань захисту критичної інфраструктури; 4) проведення моніторингу ефективності заходів із захисту об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури, зокрема щодо забезпечення охорони, оборони, фізичного захисту, інженерного захисту, кіберзахисту, а також захисту від усіх проєктних загроз критичній інфраструктурі національного рівня; 5) удосконалення нормативно-правової бази у сфері захисту критичної інфраструктури [133].

Міжвідомча комісія відповідно до покладених на неї завдань: 1) проводить аналіз стану справ у сфері захисту критичної інфраструктури та готує рекомендації, зокрема щодо: захисту критичної інфраструктури; стану організації та забезпечення необхідними силами, засобами і ресурсами функціонування національної системи захисту критичної інфраструктури; забезпечення безпеки об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури, їх кібербезпеки, запобігання несанкціонованому втручанню в їх функціонування, прогнозування та запобігання кризовим ситуаціям на об'єктах критичної інфраструктури та об'єктах критичної інформаційної інфраструктури і реагування на них; механізму та способів охорони, оборони, фізичного захисту, інженерного захисту, а також захисту від усіх проєктних загроз критичній інфраструктурі національного рівня, кіберзахисту об'єктів критичної інформаційної інфраструктури; здійснення заходів із встановлення фактичного стану забезпечення охорони, оборони, фізичного захисту, захисту від усіх проєктних загроз критичній інфраструктурі національного рівня, а також оцінювання стану інженерного захисту об'єктів критичної інфраструктури, кіберзахисту об'єктів критичної інформаційної інфраструктури, а також залучення представників органів виконавчої влади та інших державних

органів, функціональних і секторальних органів у сфері захисту критичної інфраструктури, Адміністрації Держспецзв'язку до їх проведення; здійснення міжнародного співробітництва у сфері захисту критичної інфраструктури, організації взаємодії з іноземними державами та міжнародними організаціями у частині залучення міжнародної допомоги для забезпечення захисту критичної інфраструктури; 2) вивчає результати діяльності органів виконавчої влади та інших державних органів, органів місцевого самоврядування, операторів критичної інфраструктури та інших підприємств, установ, організацій, а також функціональних і секторальних органів у сфері захисту критичної інфраструктури, Адміністрації Держспецзв'язку з питань, що належать до її компетенції; 3) подає Кабінетові Міністрів України розроблені за результатами своєї роботи пропозиції та рекомендації [133].

Створюються міжвідомчі робочі групи і у науковій сфері. Зокрема, з метою вирішення питань про встановлення критеріїв віднесення об'єктів інфраструктури у сфері охорони здоров'я до критичної інфраструктури, оцінки загроз та формування заходів реагування на них і підготовки пропозицій до проєкту Закону України «Про критичну інфраструктуру та її захист», Президія Національної академії медичних наук України постановила створити експертну групу з числа фахівців НАМН України та співробітників Головного управління контррозвідувального захисту інтересів держави у сфері економічної безпеки СБ України. Така міжвідомча співпраця зініційована Службою безпеки України, що було зумовлено в першу чергу виконанням Указу Президента України від 16 січня 2017 № 8 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про вдосконалення заходів забезпечення захисту об'єктів критичної інфраструктури України"» [150].

Зазначене вище дає змогу дійти висновку, що участь СБУ у міжвідомчих робочих групах забезпечує безперервний обмін оперативною інформацією, яка є критично важливою для раннього виявлення загроз, адже

втручання у функціонування об’єктів критичної інфраструктури часто має багатоетапний характер і може виявлятися паралельно у різних сферах. У свою чергу інші інституції, залучені до робочої групи, отримують доступ до аналітичних можливостей СБУ та її здатності реагувати на загрози державного рівня, що підсилює їхню власну спроможність діяти у сфері захисту критичної інфраструктури. Крім того, міжвідомчі робочі групи створюють умови для вироблення спільних стандартів, процедур і механізмів взаємодії, які дозволяють забезпечити єдиний підхід до реагування на загрози. Таким чином, створення міжвідомчих робочих груп є ключовим елементом ефективної моделі безпеки, що дозволяє забезпечити інтеграцію зусиль, оперативність реагування, координацію дій і системну підготовку до запобігання загрозам, які можуть завдати шкоди життєво важливим інфраструктурним системам. Це робить таку взаємодію не просто бажаною, а необхідною умовою забезпечення національної безпеки.

З огляду на зазначене вище, важливим напрямом взаємодії СБУ з державними та громадськими інституціями в процесі запобігання несанкціонованого втручання у функціонування об’єктів критичної інфраструктури є розробка спільних нормативних документів, зокрема різноманітних рекомендацій. Так, адміністрація Державної служби спеціального зв’язку та захисту інформації України разом із Службою безпеки України затвердили оновлені рекомендації та нову форму плану кіберзахисту для об’єктів критичної інфраструктури (ОКІ). Ці документи запроваджують сучасні вимоги до кібербезпеки та порядку реагування на кіберінциденти, враховуючи актуальні загрози у сфері інформаційної безпеки. Наказом визначено оновлені шаблони планів, які відображають актуальні ризики й виклики. Держспецзв’язку підготувала комплекс рекомендацій, що є обов’язковими для використання під час розроблення планів захисту. До них належать оцінювання кіберризиків, аналіз критичних залежностей між елементами інфраструктури та врахування нових типів

загроз, зокрема пов’язаних із збройною агресією. Організації-власники ОКІ повинні регулярно надавати оновлену інформацію щодо виконання заходів з кіберзахисту та реагування на інциденти. Документ також змінює порядок погодження планів захисту ОКІ. Відтепер їх затвердження відбувається у два етапи: спочатку погодження плану з Держспецзв’язку, а потім – із Службою безпеки України. Раніше погодження здійснювалося виключно Держспецзв’язку. Скоординована взаємодія двох органів формує більш ефективну систему захисту критично важливих об’єктів та зменшує ризики для інфраструктури, від функціонування якої залежить надання essentialних послуг населенню та загальний рівень безпеки держави [30].

Слід зауважити, що СБУ в межах контрдиверсійних і антитерористичних заходів відстежує діяльність співробітників об’єктів критичної інфраструктури з метою виявлення серед них осіб, які можуть співпрацювати з РФ. Про це в інтерв’ю «Інтерфакс-Україна» розповів Василь Малюк: «Буквально на днях затриманий один зі співробітників однієї ТЕС, який займався нібито ремонтом. Насправді він передавав ворогу дані щодо актуальних координат енергетичних об’єктів, а потім збирав результати обстрілів і передавав окупантам. Він вже дає викривальні покази», – зазначив В. Малюк [142].

Як приклад також можемо вказати, що на Рівненщині СБУ викрила працівника одного з об’єктів критичної інфраструктури на виправдовуванні війни РФ проти України. У прокуратурі зазначили, що йдеться про уродженця Луганщини, який тривалий час живе та працює у Вараші. За даними слідства, працівник одного із об’єктів критичної інфраструктури публічно глорифікував дії Росії у забороненій соцмережі та поширював антиукраїнські наративи російських пропагандистів. У службі безпеки розповіли, що чоловік неодноразово підтримував загарбницьку політику путінського режиму, дискредитував військовослужбовців України та

співчував втратам збройним силам РФ. Місце роботи чоловіка в СБУ не називають [57].

Варто зазначити, що СБУ веде активну спільну діяльність з іншими правоохоронними органами щодо протидії підривній та злочинній діяльності за напрямом запобігання несанкціонованого втручання у функціонування об'єктів критичної інфраструктури. Про це яскраво свідчить правозастосовна практика. Наприклад, Служба безпеки й Національна поліція запобігли чотирьом терактам і диверсіям, які планувалися в Україні на замовлення Росії, а саме:

1) Київщина. Правоохоронці затримали чоловіка з міста Ірпінь – його підозрюють у підготовці підриву одного з військових у місті Буча. Фігуранту 31 рік, його раніше неодноразово притягували до кримінальної відповідальності за розбій;

2) за даними досудового розслідування, чоловік виготовив саморобну бомбу за інструкцією свого куратора і для ліквідації військового вивчав його графік дня та маршрути пересування. Підозрюваного затримали за місцем проживання;

3) Львів. Кіберфахівці СБУ запобігли серії терактів, які мали відбутися біля місцевих будівель ТЦК та СП і Головного залізничного вокзалу. Розслідування з'ясувало, що виконавцем злочину мав бути 23-річний агент із Київщини. Попередньо після доставки вибухівки на визначені локації російська спецслужба планувала вбити і свого агента як «зайвого свідка». Правоохоронці затримали чоловіка на гарячому, коли він закладав вибухівку біля залізничного вокзалу;

4) Чернігів. СБУ та Нацполіція викрили чоловіка, якого вважають причетним до підготовки низки терактів в області. За матеріалами справи, фігурант мав виготовити вибухівку й передати її іншим людям, щоб ті підірвали військових ЗСУ, працівників Національної поліції та інших силових структур. Також слідчі встановили, що фігурант виконував ще одне

завдання від Росії — за допомогою пляшок із легкозаймистою сумішшю він підпалив будівлю одного з районних ЦНАПів.

5) Вінниця. Служба безпеки та Національна поліція нейтралізували групу підпалювачів, які на замовлення РФ спалили дві релейні шафи сигнальних установок, які регулюють рух на важливих ділянках «Укрзалізниці». Усі фігуранти справ отримали підозру за такими статтями Кримінального кодексу України: ст.111 (державна зрада); ст. 113 (диверсія); ст. 258 (терористичний акт); ст. 263 (незаконне поводження зі зброєю, бойовими припасами або вибуховими речовинами) [16].

СБУ затримала іноземця, який на замовлення фсб збирав дані про енергооб'єкти в Житомирській та Хмельницькій областях і коригував ракетно-дронові удари по цих регіонах. Контррозвідка СБУ викрила агента фсб, який передавав росії фото енергогенерувальних і теплопостачальних підприємств, зокрема об'єктів поблизу Хмельницької АЕС. Через ці матеріали ворог планував оцінити стан обладнання та рівень його захисту. Фігурантом виявився громадянин однієї з країн Близького Сходу, який проживає у Звягелі на Житомирщині. Він потрапив у поле зору російських спецслужб після того, як шукав «легкий заробіток» у телеграм-каналах. СБУ викрила планування терактів у ТРЦ й метро в Києві. Після вербування чоловік на власному авто об'їжджав визначений маршрут, зупинявся біля підстанцій, теплоелектроцентралі та об'єктів поблизу АЕС, фотографував периметри та пости охорони. Під час таких поїздок він також фіксував блокпости Сил оборони. СБУ затримала агента на початковому етапі діяльності, коли він знімав одну з електропідстанцій. Під час обшуків у нього вилучили смартфон із доказами співпраці з ворогом [54].

Контррозвідка СБУ запобігла серії російських диверсій у Харкові, затримавши агента ФСБ, який готував підриви ключових електропідстанцій, що живлять місто. Про це повідомляє РБК-Україна з посиланням на пресслужбу СБУ. Зазначається, що замовлення РФ виконував завербований

російською спецслужбою дитячий аніматор з обласного центру. До уваги окупантів він потрапив через свою знайому, яка проживає в росії. Після дистанційного вербування агент отримав завдання від куратора: підірвати опорну електропідстанцію, яка забезпечує електропостачання одного з районів міста [171]. Для вчинення злочину фігурант отримав інструкцію на виготовлення саморобного вибухового пристрою. Співробітники СБУ затримали агента, коли він робив вибухівку у своєму помешканні. СБУ також встановила, що фігурант фіксував локації Сил оборони по дорозі на дитячі свята. У разі успішного підриву першої електропідстанції, агент мав вчинити аналогічні диверсії на інших енергооб'єктах міста. Під час обшуків у помешканні та автомобілі затриманого вилучено складові до вибухового пристрою, а також планшет і телефон із доказами роботи на ворога. Слідчі СБУ повідомили йому про підозру, наразі підозрюваний перебуває під вартою. Йому загрожує довічне позбавлення волі з конфіскацією майна [171].

Служба безпеки України затримала двох агентів російської військової розвідки, причетних до планування авіаударів по життєво важливих об'єктах інфраструктури в Києві та його околицях. Згідно з повідомленням СБУ підозрюваних звинуватили в зборі розвідувальних даних для російських ракетних атак та атак безпілотників на теплові й гідроелектростанції столиці України, ключові цілі в триваючій кампанії Москви проти енергетичного сектору України. Двоє чоловіків були ідентифіковані як безробітні мешканці Одеської та Хмельницької областей. За даними СБУ, їх завербувало ГРУ восени 2025 року, шукаючи «легкого заробітку» через Telegram-канали. Після вербування чоловіків було направлено до Києва та сусідніх регіонів, де вони проводили розвідувальні місії, визначаючи та документуючи координати енергетичних об'єктів та оцінюючи їхній стан після російських бомбардувань [79].

Окрему увагу слід приділити взаємодії СБУ з громадськістю. Наприклад, СБУ провела в Дніпрі тренінг із протидії кібератакам на об'єкти

критичної інфраструктури. На заході представили алгоритм дій для убезпечення державних інформаційних ресурсів, а також об'єктів логістики і транспорту, енергетичної галузі та виробничих підприємств. Оскільки Дніпропетровська область є одним з найбільших промислових регіонів України, ворог намагається вразити її інфраструктурні об'єкти не лише ракетно-дроновими ударами, а й методами кібертероризму. Тож кіберфахівці СБУ постійно взаємодіють з місцевими органами державної влади та приватним сектором, щоб підвищити їхню кіберстійкість і кіберобізнаність. З початку повномасштабного вторгнення Служба безпеки нейтралізувала понад 350 кібератак і кіберінцидентів на об'єкти критичної інфраструктури, органів державної влади й місцевого самоврядування саме в Дніпропетровській області. Загалом по Україні спецслужба блокувала майже 10 тис. таких кібератак. Під час тренінгу в Дніпрі фахівці Центру забезпечення кібербезпеки СБУ розповіли про методи захисту та стратегію зміцнення кіберпростору у кризових умовах, про застосування сучасних технологій, а також про важливість координації дій усіх учасників. Подібні центри створені Службою безпеки у всіх регіонах, як регіональні осередки для реагування на загрози на місцевому рівні. До їх основних завдань належать моніторинг кіберзагроз і вчасне реагування на них [159].

Таким чином, проведений аналіз дає змогу виокремити такі характерні особливості взаємодії Служби безпеки України з державними та громадськими інституціями в процесі запобігання несанкціонованого втручання у функціонування об'єктів критичної інфраструктури:

1) у відповідних правовідносинах СБУ переважно відіграє роль координатора, а отже, вона є обов'язковим учасником процесу погодження стратегічно важливих рішень, пов'язаних із захистом об'єктів критичної інфраструктури;

2) така спільна діяльність передбачає узгодження рішень і дій СБУ з одним або декількома органами влади, а також операторами критичної

інфраструктури, що необхідно через високий рівень взаємозалежності систем;

3) до взаємодії активно залучається громадський сектор, представники якого беруть участь у моніторингу, аналізі ризиків, обговоренні політик безпеки та формуванні культури кібер- та фізичної стійкості;

4) специфіка взаємодії полягає в тому, що СБУ передає іншим інституціям релевантні, а іноді й засекречені дані про загрози, що дозволяє прискорити реагування на ризики, а також покладає на інші сторони взаємодії додаткову відповідальність;

5) акцент у межах практичної реалізації відповідної спільної діяльності, переважно, робиться на профілактиці, яке включає раннє виявлення та блокування загроз, включно з попередженням диверсій, кібератак, інсайдерських дій;

6) спрямована на синхронізацію стандартів та вимог безпеки між різними секторами;

7) взаємодія включає об’єднання кібербезпеки, фізичного захисту, антикризового управління, антитерористичної діяльності та розвідки, що відповідає сучасним реаліям;

8) інклюзивність взаємодії, адже СБУ залучає та обговорює ключові питання безпеки з професійними об’єднаннями, галузевими асоціаціями та профільними експертами;

9) ключовою метою взаємодії створення такої системи захисту критичної інфраструктури, яка здатна витримати тривалі та комбіновані впливи, характерні для сучасних воєнних і кібервикликів.

У підсумку слід узагальнити, що взаємодія Служби безпеки України з державними та громадськими інституціями в процесі запобігання несанкціонованому втручанню в роботу об’єктів критичної інфраструктури має ключове значення для формування комплексної, стійкої та превентивної системи національної безпеки. Сучасні загрози, які поєднують кібератаки,

диверсійні дії, інформаційні операції та технологічні ризики, роблять ізольовану діяльність будь-якого одного органу недостатньою. Участь СБУ в широкій мережі взаємодії забезпечує своєчасне виявлення небезпек, оперативний обмін інформацією та залучення необхідних компетенцій для захисту критично важливих систем, від яких залежить функціонування держави та базові потреби громадян. Співпраця з державними структурами дозволяє узгоджувати стандарти безпеки, формувати спільну політику реагування та координувати дії у разі кризових ситуацій. Водночас взаємодія з громадськими організаціями та професійними спільнотами посилює прозорість, забезпечує додаткові канали моніторингу загроз, сприяє поширенню знань про безпеку й залучає експертний потенціал, що є особливо важливим у сфері швидко змінюваних технологій. Така модель співпраці створює багаторівневу систему захисту, у якій Служба безпеки слугує центральним координатором, а державні та громадські партнери – активними учасниками процесу, що підвищує стійкість критичної інфраструктури і мінімізує ризики її виведення з ладу чи використання у шкідливих цілях. У результаті саме синергія державних і суспільних інституцій із СБУ забезпечує необхідний рівень безпеки в умовах гібридних викликів та високої залежності країни від безперервної роботи інфраструктурних систем.

Висновок до розділу 2

Встановлено, що правовий механізм – це спеціальна юридична конструкція, яку становлять інструменти, організоване та послідовне використання яких дозволяє реалізувати положення норм чинного законодавства, суб’єктивні права, свободи, законні інтереси, а також

отримати будь-який інший юридично значущий результат, який змінює, припиняє чи зумовлює появу нових суспільно-правових відносин.

З'ясовано, що загальними характерними властивостями поняття «адміністративно-правовий механізм» є такі: 1) це – явища суворо регламентовані нормами адміністративного законодавства й уточнені положеннями підзаконних, відомчих актів тощо; 2) основу цього механізму становлять інструментальні, прикладні елементи, які застосовуються для досягнення юридично значущого результату; 3) їх реалізація відбувається в діяльності спеціального кола уповноважених законодавством носіїв публічної влади, які становлять інституційну складову механізму; 4) зазвичай результатом втілення у життя такого механізму є ефективне та успішне виконання суб'єктом публічних повноважень покладених на нього завдань і функцій, завдяки чому відбувається реалізація певних суспільно-правових відносин та поведінки їх учасників.

Констатовано, що адміністративно-правовий механізм захисту об'єктів критичної інфраструктури Службою безпеки України – це юридична конструкція, яку становлять адміністративно-правові інструменти, що реалізуються уповноваженими органами, підрозділами, окремими посадовими особами Служби з метою впливу на сферу критичної інфраструктури, а також забезпечення стійкості, безпеки функціонування зарахованих до неї об'єктів. Структуру цього адміністративно-правового механізму становлять: 1) адміністративно-правові інструменти захисту об'єктів критичної інфраструктури; 2) інституційна основа реалізації відповідних інструментів; 3) нормативні акти, що визначають порядок і специфіку реалізації останніх.

Визначено глибоку інтегрованість Служби безпеки України в роботу системи органів забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури. Водночас реалізація інструментарію відповідного механізму відбувається із суворим дотриманням принципу дотримання

державної таємниці та не допускає публічного розголошення операційного порядку діяльності СБУ. Подібне ускладнює теоретико-правові дослідження, що цілком логічне з міркувань національної безпеки та ризику потрапляння секретів і специфіки роботи СБУ до осіб та груп, які можуть використати вказану інформацію для завдавання шкоди суспільству або державі.

Здійснено оцінку комплексу наукових підходів щодо змісту і значення адміністративно-правових інструментів, що дало підстави виокремити такі ознаки вказаної категорії: 1) зміст інструментів становлять форми, заходи, засоби та способи публічно-управлінської, офіційної діяльності суб'єктів владних повноважень щодо реалізації покладених на них законодавством функцій і завдань у певних сферах та галузях суспільних відносин; 2) перелік доступних до використання адміністративно-правових інструментів визначається нормативно-правовими засадами діяльності кожного окремого суб'єкта владних повноважень; 3) адміністративно-правові інструменти мають різний обсяг, зміст і результат здійснення. Це – гнучка категорія, у якій може набувати вираження як об'ємна, стратегічно орієнтована активність, так і дії, спрямовані на отримання певного оперативного, точкового результату; 4) зазвичай результат використання адміністративно-правових інструментів – це приведення в дію приписів нормативно-правових актів, завдяки чому впорядковуються суспільно-правові відносини певного типу та поведінка їх учасників.

Доведено, що адміністративно-правові інструменти захисту об'єктів критичної інфраструктури Службою безпеки України – це передбачені законодавством України форми, засоби, способи й заходи, які використовуються органами та підрозділами Служби безпеки України для формування необхідного стану безпеки об'єктів критичної інфраструктури, підтримання стійкості їх функціонування, а також безпосереднього захисту від будь-яких загроз і посягань.

Обґрунтовано, що адміністративно-правові інструменти є важливою складовою діяльності Служби безпеки України у сфері захисту критичної інфраструктури, оскільки саме через них забезпечується превентивний, регулятивний та охоронний вплив держави на стратегічно значущі об’єкти. Попри те, що Служба традиційно асоціюється передусім з кримінально-процесуальними формами протидії злочинності, її роль як суб’єкта публічної адміністрації є не менш значущою. Використовуючи надані законом повноваження, Служба безпеки України формує та реалізує комплекс управлінських і контрольно-наглядових механізмів, спрямованих на попередження загроз, підтримання стійкості та безперебійності функціонування критичної інфраструктури. Крім того, у цьому контексті Служба не обмежується загальними адміністративними засобами, адже її спеціальний статус передбачає можливість застосування більш складних правових інструментів, характерних для контррозвідувальної, антитерористичної та інформаційно-аналітичної діяльності. Саме поєднання цих загальних і спеціальних адміністративно-правових механізмів забезпечує комплексний, системний характер державного впливу на сферу, що має вирішальне значення для національної безпеки.

Встановлено, що взаємодія Служби безпеки України з державними і громадськими інституціями в процесі запобігання несанкціонованому втручанню у функціонування об’єктів критичної інфраструктури – це врегульована нормами чинного законодавства система узгоджених дій, заходів, інформаційного обміну тощо між Службою безпеки України та іншими уповноваженими органами державної влади, органами місцевого самоврядування, суб’єктами управління критичною інфраструктурою та інститутами громадянського суспільства, спрямована на виявлення, запобігання і нейтралізацію загроз незаконного втручання, а також на забезпечення безперервності та стійкості функціонування об’єктів критичної інфраструктури.

Сформульовано висновок про те, що участь СБУ в міжвідомчих робочих групах забезпечує безперервний обмін оперативною інформацією, яка є критично важливою для раннього виявлення загроз, адже втручання у функціонування об'єктів критичної інфраструктури часто має багатоетапний характер і може виявлятися паралельно в різних сферах. Своєю чергою інші інституції, залучені до робочої групи, отримують доступ до аналітичних можливостей СБУ та її здатності реагувати на загрози державного рівня, що підсилює їхню власну спроможність діяти у сфері захисту критичної інфраструктури. Крім того, міжвідомчі робочі групи створюють умови для вироблення спільних стандартів, процедур і механізмів взаємодії, які дозволяють забезпечити єдиний підхід до реагування на загрози. Таким чином, створення міжвідомчих робочих груп є ключовим елементом ефективної моделі безпеки, що дозволяє забезпечити інтеграцію зусиль, оперативність реагування, координацію дій і системну підготовку до запобігання загрозам, які можуть завдати шкоди життєво важливим інфраструктурним системам. Це робить таку взаємодію не лише бажаною, а й необхідною умовою забезпечення національної безпеки.

Визначено характерні особливості взаємодії Служби безпеки України з державними та громадськими інституціями в процесі запобігання несанкціонованого втручання у функціонування об'єктів критичної інфраструктури: 1) у відповідних правовідносинах Служба безпеки України переважно відіграє роль координатора, а отже, вона є обов'язковим учасником процесу погодження стратегічно важливих рішень, пов'язаних із захистом об'єктів критичної інфраструктури; 2) така спільна діяльність передбачає узгодження рішень і дій Служби безпеки України з одним або декількома органами влади, а також операторами критичної інфраструктури, що необхідно через високий рівень взаємозалежності систем; 3) до взаємодії активно залучається громадський сектор, представники якого беруть участь у моніторингу, аналізі ризиків, обговоренні політик безпеки та формуванні

культури кібер- та фізичної стійкості; 4) специфіка взаємодії полягає в тому, що Служба безпеки України передає іншим інституціям релевантні, а іноді й засекречені дані про загрози, що дозволяє прискорити реагування на ризики, а також покладає на інші сторони взаємодії додаткову відповідальність; 5) у межах практичної реалізації відповідної спільної діяльності увагу зосереджено переважно на профілактиці, що охоплює раннє виявлення та блокування загроз, включно з попередженням диверсій, кібератак, інсайдерських дій; 6) спрямована на синхронізацію стандартів і вимог безпеки між різними секторами; 7) взаємодія передбачає об'єднання кібербезпеки, фізичного захисту, антикризового управління, антитерористичної діяльності й розвідки, що відповідає сучасним реаліям; 8) інклюзивність взаємодії, адже Служба безпеки України залучає та обговорює ключові питання безпеки з професійними об'єднаннями, галузевими асоціаціями та профільними експертами; 9) ключовою метою взаємодії є створення такої системи захисту критичної інфраструктури, яка здатна витримати тривалі й комбіновані впливи, характерні для сучасних воєнних і кібервикликів.

Узагальнено, що взаємодія Служби безпеки України з державними та громадськими інституціями в процесі запобігання несанкціонованому втручанню в роботу об'єктів критичної інфраструктури має ключове значення для формування комплексної, стійкої та превентивної системи національної безпеки. Сучасні загрози, які поєднують кібератаки, диверсійні дії, інформаційні операції та технологічні ризики, роблять ізольовану діяльність будь-якого одного органу в досліджуваній сфері недостатньою. Участь СБУ в широкій мережі взаємодії забезпечує своєчасне виявлення небезпек, оперативний обмін інформацією та залучення необхідних компетенцій для захисту критично важливих систем, від яких залежить функціонування держави та базові потреби громадян. Співпраця з державними структурами дозволяє узгоджувати стандарти безпеки,

формувати спільну політику реагування та координувати дії в разі кризових ситуацій. Водночас взаємодія з громадськими організаціями та професійними спільнотами посилює прозорість, забезпечує додаткові канали моніторингу загроз, сприяє поширенню знань про безпеку та залучає експертний потенціал, що є особливо важливим у сфері швидко змінюваних технологій. Отже, така модель співпраці створює багаторівневу систему захисту, у якій Служба безпеки слугує центральним координатором, а державні та громадські партнери – активними учасниками процесу, що підвищує стійкість критичної інфраструктури й мінімізує ризики її виведення з ладу чи використання в шкідливих цілях. У результаті саме синергія державних і суспільних інституцій з СБУ забезпечує необхідний рівень безпеки в умовах гібридних викликів та високої залежності країни від безперервної роботи інфраструктурних систем.

РОЗДІЛ 3
ШЛЯХИ ВДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО МЕХАНІЗМУ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ СЛУЖБОЮ БЕЗПЕКИ УКРАЇНИ

3.1. Стратегічне планування забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури й місце в ньому Служби безпеки України

Забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури є складним та багатоаспектним процесом, який вимагає побудови ефективної системи стратегічного планування. Загалом планування – це вид управлінської діяльності, який визначає перспективу і майбутній стан організації, шляхи та способи його досягнення. Процес планування сприяє прийняттю обґрунтованих управлінських рішень. Його мета полягає у визначенні необхідної кількості ресурсів, впровадженні нововведень для адекватного реагування на зміни зовнішнього середовища. Планування є необхідною передумовою успішної діяльності організації в майбутньому, є процесом підготовки обґрунтованих перспективних рішень [140]. С. К. Гречанюк планування пропонує тлумачити як процес утілення стратегії, який полягає в прийнятті та реалізації конкретних рішень, які можуть забезпечити ефективне функціонування та розвиток установи, організації в майбутньому. Планові рішення можуть бути пов'язані з визначенням цілей і задач, виробленням стратегії, розподілом та перерозподілом певних ресурсів, визначенням певних стандартів діяльності на майбутній період. Прийняття таких рішень становить планування в широкому значенні. Щодо більш вузького трактування планування, то воно полягає в складанні спеціальних документів – планів, які визначають

конкретні кроки діяльності установи з досягнення цілей. У планах відображаються: прогнози розвитку установи в майбутньому; проміжні та кінцеві задачі й цілі установи та окремих підрозділів; механізми координації поточної діяльності та розподілення ресурсів; стратегії дій на випадок надзвичайних обставин [27].

З точки зору теорії управління планування – це найперша функція управління, вона передує іншим управлінським функціям і визначає їх сутність. Планування залежить від ефективного аналізу зовнішнього середовища, об'єктивного оцінювання власних позицій, потребує спільних зусиль та участі всіх складових організацій. Також ця функція передбачає вибір мети, розробку шляху її досягнення та просування ним. Планування як функція менеджменту, пишуть Н. В. Дикань та І. І. Борисенко, полягає в розв'язанні таких глобальних проблем: 1) якими мають бути цілі організації; 2) як має діяти організація, щоб їх досягти. Планування дає змогу будь-якій організації передбачати майбутнє. Воно виявляється в програмі дій, що охоплюють усі операції підприємства (технічні, фінансові, комерційні). Планування має враховувати періоди, джерела та витрати. Процес планування передбачає складання перспективних і поточних планів-прогнозів, призначення яких полягає в забезпеченні колективного розуміння загальних завдань, стратегії й тактики їх виконання, а також урахування ресурсів, що є в розпорядженні [36].

Досліджуючи сутність планування, В. Я. Малиновський зазначає, що це – «стержнева частина всіх систем управління, процес, за допомогою якого система пристосовує свої ресурси до змін зовнішніх і внутрішніх умов. Планування є найпершою функцією управління, яка передує всім іншим, визначаючи їх природу. Планування залежить від ефективного аналізу зовнішнього середовища, об'єктивної оцінки власних ресурсів, вимагає спільних зусиль і участі всіх складових частин організації. Особливо важливою ця функція є для органів державного управління, коли під впливом

зовнішніх чинників перед ними ставляться невизначені до кінця завдання, а подекуди – нездійсненні цілі, поставлені політиками. Планування – найбільш динамічна функція, а тому вона повинна виконуватися професійно й постійно для забезпечення надійної основи здійснення інших видів управлінської діяльності» [75, с. 169].

Отже, планування в загальному значенні усвідомлюється як процес цілеспрямованого передбачення майбутньої діяльності, у межах якого визначаються цілі та способи їх досягнення з урахуванням наявних ресурсів і умов. Таке розуміння планування, як вбачається, містить орієнтацію на майбутнє і необхідність свідомого вибору напрямів дій, однак саме по собі воно ще не уточнює ні масштабів цього майбутнього, ні рівня управлінських рішень. У міру ускладнення діяльності та зростання впливу зовнішніх чинників виникає потреба не просто планувати окремі дії, а заздалегідь визначати загальний напрям розвитку, який задаватиме рамки для всіх подальших рішень. Саме на цьому етапі загальне планування логічно трансформується в стратегічне, оскільки акцент зміщується з короткострокових завдань на довгострокові цілі та принципові орієнтири розвитку.

У цьому контексті В. П. Збукар стверджує, що стратегічне планування – це адаптивний процес, за допомогою якого здійснюються регулярна розробка та корекція системи досить формалізованих планів, перегляд змісту заходів щодо їхнього виконання на основі безперервного контролю та оцінки змін, що відбуваються зовні та всередині системи. Стратегічне планування охоплює систему довго-, середньо- та короткострокових планів, проєктів і програм [45]. Аналізуючи різні наукові підходи, Н. В. Щербак доходить висновку, що якісний стратегічний план органу державної влади має бути: комплексним, тобто охоплювати всі аспекти діяльності органу виконавчої влади, зважаючи на зовнішні й внутрішні умови його функціонування, а також брати до уваги всі

можливості органу виконавчої влади та фактори впливу на його діяльність; спрямованим на перспективу, тобто здійснюватися протягом декількох років для того, щоб визначити головний напрям діяльності органу виконавчої влади; цілеспрямованим, тобто таким, що надає розуміння цілей органу виконавчої влади та прогресу, а також встановлює пріоритетність досягнення цілей; гнучким (еластичним), тобто вплив зміни одного зі складників на інші має бути зведений до мінімуму; аналітичним, тобто таким, що подає дані та наводить потрібні інтерпретації інформації; обґрунтованим, тобто містити факти та пропозиції, зокрема щодо організаційних змін, потрібних для виконання плану; орієнтованим на конкретні дії, тобто бути спрямованим на виконання конкретних завдань у конкретних проміжках часу; лаконічним, тобто досить коротким для того, щоб високопосадовці могли швидко з ним ознайомитися, але водночас містити достатньо інформації, щоб бути зрозумілим [174].

Таким чином, стратегічне планування забезпечення безпеки та стійкості функціонування об’єктів критичної інфраструктури – це довгостроковий, системний та комплексний процес формування цілей, принципів, пріоритетів і механізмів, спрямованих на попередження, мінімізацію та нейтралізацію загроз, що можуть порушити безперервність роботи життєво важливих інфраструктурних систем держави. Таке планування має комплексний характер, адже передбачає узгодження дій між різними державними органами, операторами критичної інфраструктури, силовими структурами, науковими установами та громадськими інституціями, що забезпечує всебічне бачення ризиків і подальшого опрацювання шляхів їх подолання. Стратегічне планування в досліджуваній сфері, як вбачається, охоплює визначення потенційних сценаріїв небезпеки, моделювання їх впливу, створення превентивних програм, розробку політик реагування та механізмів відновлення, а також забезпечення необхідних ресурсів, компетенцій і нормативної підтримки для досягнення стабільного

та безпечного функціонування інфраструктурних об’єктів у мирний час і за умов криз чи воєнних загроз. Усе зазначене вище призводить до того, що в результаті стратегічне планування слугує фундаментальним інструментом державного управління, який забезпечує прогнозованість, адаптивність та стійкість систем, від яких залежить життєдіяльність і стабільність функціонування суспільства.

Стратегічне планування в досліджуваній сфері суспільного життя означене такими особливостями:

– орієнтація на довгостроковий прогноз ризиків і сценаріїв загроз, які можуть бути скореговані залежно від безпекової, економічної та інших ситуацій;

– має комплексний характер, адже покликане враховувати й поєднувати фізичну, технологічну, інформаційну, організаційну та кібербезпеку;

– передбачає узгодження та координацію дій різними державними органами, операторами інфраструктури та суспільними інституціями;

– має не лише превентивний характер, спрямований на запобігання інцидентам, а й реактивний;

– враховує критичні залежності між різними секторами інфраструктури взагалі та критичної зокрема;

– потребує чіткого розподілу ресурсів, компетенції спеціально уповноважених суб’єктів;

– передбачає регулярне оновлення планів на основі аналізу інцидентів і результатів моніторингу.

Н. В. Трушкіна слушно зазначає, що в процесі стратегічного аналізу керівництво об’єктів критичної інфраструктури оцінює зовнішні чинники, а також потенціал внутрішніх ресурсів. На основі цього визначають подальші цілі й завдання функціонування інфраструктури. Під час розроблення стратегічних рішень оцінюють варіанти розроблених стратегій, а також вибір

найбільш функціональної стратегії. У межах цього елемента проводять аналіз стратегічних планів, потреби в трудових ресурсах і капіталі, додаткові економічні та наукові дослідження. У процесі реалізації стратегії здійснюється її безпосередня реалізація. У разі суттєвих змін зовнішніх чинників, які мають прямий вплив на розвиток критичної інфраструктури, а також змінах внутрішнього потенціалу, що перешкоджають реалізації заздалегідь запланованого процесу стратегування, керівництво коригує модель на необхідних етапах. Таким чином, основою моделі стратегування є орієнтир для стратегічних дій, який через реалізацію стратегічного процесу трансформується в результат стратегічного управління. Умовою реалізації моделі має бути досягнення конкурентних переваг у розвитку критичної інфраструктури [157].

Варто зауважити, що з огляду на прагнення України до європейської інтеграції, важливо, щоб стратегічне планування було здійснено відповідно до Директиви про стійкість критично важливих об'єктів, яка набула чинності 16 січня 2023 року. Директива спрямована на посилення стійкості критично важливих об'єктів до низки загроз, включаючи стихійні лиха, терористичні атаки, внутрішні загрози або саботаж, а також надзвичайні ситуації у сфері охорони здоров'я. Згідно з новими правилами:

1) державам-членам потрібно буде прийняти національну стратегію та проводити регулярні оцінки ризиків, щоб визначити об'єкти, які вважаються критично важливими або життєво важливими для суспільства та економіки. Комісія прийняла перелік життєво важливих послуг у всіх секторах, що охоплюються Директивою. Оцінки ризиків будуть проводитися стосовно цих життєво важливих послуг, щоб можна було визначити критично важливі об'єкти в кожній державі;

2) критично важливим організаціям потрібно буде проводити власні оцінки ризиків і вживати технічних, безпекових та організаційних заходів для підвищення своєї стійкості та повідомлення про інциденти;

3) критично важливі установи ЄС, які надають основні послуги в шести або більше державах-членах, отримають додаткові консультації щодо того, як найкраще виконувати свої зобов'язання щодо оцінки ризиків і вжиття заходів щодо підвищення стійкості;

4) державам-членам необхідно буде надавати підтримку критично важливим організаціям у підвищенні їхньої стійкості. Комісія надаватиме додаткову підтримку державам-членам та критично важливим організаціям, розробляючи, серед іншого, огляд транскордонних та міжгалузевих ризиків на рівні Союзу, передовий досвід, інструктивні матеріали, методології, транскордонні навчальні заходи та вправи для перевірки стійкості критично важливих організацій [177].

Рекомендація Ради щодо загальносоюзного скоординованого підходу до посилення стійкості критичної інфраструктури, прийнята 8 грудня 2022 року, стала реакцією на заклики до вжиття додаткових заходів після актів саботажу проти критичної інфраструктури в ЄС. Вона базується на п'ятиетапному плані щодо стійкої критичної інфраструктури, представленому президентом фон дер Ляєн у жовтні 2022 року. У Рекомендації Ради пропонуються дії щодо підвищення готовності та реагування на поточні загрози , як шляхом передбачення певних елементів Директиви про стійкість критичних об'єктів, так і шляхом скоординованого використання додаткових інструментів. Рекомендація охоплює три пріоритетні сфери: готовність, реагування та міжнародна співпраця [177]. Директива передбачає кожна стратегія повинна містити принаймні такі елементи: стратегічні цілі та пріоритети для посилення загальної стійкості критично важливих суб'єктів з урахуванням транскордонної та міжсекторальної залежності та взаємозалежності; рамка управління для досягнення таких стратегічних цілей і пріоритетів, включно з описом ролей та обов'язків різних органів, критично важливих суб'єктів та інших сторін, що беруть участь у реалізації цієї стратегії; опис заходів, необхідних для

посилення загальної стійкості критично важливих суб'єктів, включно з описом оцінювання ризиків; опис процесу, за допомогою якого визначають критично важливі суб'єкти; опис процесу підтримки критично важливих суб'єктів відповідно до цієї глави, включно із заходами для посилення співпраці між публічним сектором, з одного боку, і приватним сектором і публічними й приватними суб'єктами, з іншого боку; перелік основних органів і відповідних стейкхолдерів, крім критично важливих суб'єктів, що беруть участь у реалізації стратегії; рамка політики щодо координації між компетентними органами згідно з цією Директивою («компетентні органи») та компетентними органами згідно з Директивою (ЄС) 2022/2555 з метою обміну інформацією щодо ризиків для кібербезпеки, кіберзагроз та кіберінцидентів, а також не пов'язаних із кібербезпекою ризиків, загроз та інцидентів і виконання наглядових завдань; опис уже запроваджених заходів, спрямованих на сприяння виконанню обов'язків відповідно до глави III цієї Директиви малими й середніми підприємствами у розумінні додатка до Рекомендації Комісії 2003/361/ЄС, які відповідна держава-член визначила як критично важливі суб'єкти [37].

Розглядаючи стратегічне планування забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури варто виділити увагу «Національному плану захисту та забезпечення безпеки та стійкості критичної інфраструктури», затвердженого розпорядженням Кабінету Міністрів України від 19 вересня 2023 року № 825-р. У документі визначено п'ять стратегічних цілей у досліджуваній сфері суспільного життя, а саме:

Стратегічна ціль 1. Правова регламентація діяльності суб'єктів національної системи захисту критичної інфраструктури. У межах цієї цілі передбачено виконання таких завдань: удосконалення законодавства, що регламентує діяльність суб'єктів національної системи захисту критичної інфраструктури; розроблення вимог щодо захисту об'єктів критичної

інфраструктури; проведення моніторингу стану виконання вимог законодавства та звітування з питань захисту критичної інфраструктури.

Стратегічна ціль 2. Створення системи координації та взаємодії суб'єктів національної системи захисту критичної інфраструктури. Завданнями є: удосконалення порядку взаємодії суб'єктів національної системи захисту критичної інфраструктури; запровадження планів взаємодії суб'єктів національної системи захисту критичної інфраструктури щодо забезпечення стійкості надання життєво важливих функцій та/або послуг; удосконалення порядку обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури в разі порушення функціонування об'єктів критичної інфраструктури.

Стратегічна ціль 3. Запровадження управління ризиками критичної інфраструктури. Завданнями, які слід вирішити для досягнення вказаної цілі, є такі: оцінка ризиків і загроз критичній інфраструктурі; проєктні загрози; розвиток спроможності суб'єктів національної системи захисту критичної інфраструктури реагувати на загрози критичній інфраструктурі, що виникають.

Стратегічна ціль 4. Посилення стійкості національної системи захисту критичної інфраструктури, завданнями якої є: розроблення механізмів співпраці на секторальному та регіональному рівні в кризових ситуаціях для забезпечення споживачів визначеним мінімальним рівнем надання життєво важливих функцій та/або послуг; запровадження системи постійного підвищення рівня кваліфікації персоналу операторів критичної інфраструктури; розроблення оптимальних методів забезпечення безпечного середовища та мінімізації наслідків надзвичайних ситуацій на об'єктах критичної інфраструктури; розвиток спроможностей територіальних громад підтримувати власними силами мінімальний рівень життєво важливих функцій та/або послуг; запровадження механізму державної підтримки

здійснення заходів щодо підвищення стійкості населення у ситуаціях порушення функціонування критичної інфраструктури.

Стратегічна ціль 5. Налагодження міжнародної співпраці. У межах цієї цілі завданням визначено взаємодію національної системи захисту критичної інфраструктури з відповідними міжнародними системами, передусім європейськими та євроатлантичними [112].

Крім того, у Національному плані захисту та забезпечення безпеки та стійкості критичної інфраструктури, затвердженому розпорядженням Кабінету Міністрів України від 19 вересня 2023 року № 825-р, визначено строки: проведення моніторингу рівня безпеки об'єктів критичної інфраструктури; підготовки пропозицій до проєктів документів стратегічного планування щодо забезпечення безпеки та стійкості критичної інфраструктури, здійснення її захисту; розроблення, оновлення та забезпечення виконання об'єктових планів заходів щодо забезпечення безпеки і стійкості критичної інфраструктури, правил управління ризиками безпеки, планів локалізації та ліквідації наслідків аварій, а також заходів щодо забезпечення кіберзахисту; затвердження секторальних планів проведення моніторингу рівня безпеки об'єктів критичної інфраструктури; розроблення та затвердження місцевих програм забезпечення безпеки та стійкості критичної інфраструктури [6; 112].

Таки чином, Національний план формує єдину державну політику у сфері захисту та стійкості критичної інфраструктури. Документ закріплює системний підхід до управління ризиками, орієнтований не лише на фізичний захист об'єктів, а й на їхню функціональну стійкість та відновлюваність. Важливою перевагою є чітке розмежування ролей і відповідальності між органами державної влади, секторальними органами й операторами критичної інфраструктури, що створює передумови для підвищення керованості та координації в умовах криз і надзвичайних ситуацій. План також має стратегічний характер, узгоджений з європейськими та

євроатлантичними підходами до захисту критичної інфраструктури, що є важливим у контексті євроінтеграції та безпекової співпраці. Окремим позитивом є акцент на підготовці кадрів та розвитку інституційної спроможності системи захисту критичної інфраструктури.

Водночас слід виокремити й недоліки вказаного вище нормативно-правового акта: *по-перше*, План видається досить загальним і містить відносно розмиті адміністративно-правові механізми для практичного виконання; *по-друге,* у ньому немає чітких показників оцінки ефективності, через що складно оцінити, чи досягнуто поставлені цілі; *по-третє*, недостатньо визначено питання ресурсів, зокрема фінансових, технічних і кадрових, які описані поверхово; *по-четверте,* механізми взаємодії з приватним сектором та громадськістю практично не деталізовані, хоча ці суб'єкти відіграють важливу роль у забезпечення безпеки критичної інфраструктури; *по-п'яте,* процедура обміну інформацією залишається нечіткою, що може впливати на швидкість і якість реагування на загрози.

Окрему увагу слід приділити Плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України, у якій наведено завдання щодо захисту критичної інфраструктури: 1) посилення спроможностей щодо проведення негласних перевірок стану готовності об'єктів критичної інфраструктури до можливих кібератак і кіберінцидентів, поступове охоплення такими заходами всіх об'єктів, у межах якого треба вирішити такі завдання: здійснення запланованих заходів із проведення негласних перевірок стану готовності об'єктів критичної інфраструктури до можливих кібератак і кіберінцидентів, зокрема шляхом здійснення пошуку та виявлення потенційних вразливостей інформаційно-комунікаційних систем об'єктів критичної інфраструктури; проведено заплановані негласні перевірки стану готовності об'єктів критичної інфраструктури до можливих кібератак і кіберінцидентів, зокрема шляхом здійснення пошуку та виявлення потенційних вразливостей інформаційно-комунікаційних систем об'єктів критичної інфраструктури;

2) впровадження ризик-орієнтованого підходу в частині заходів із забезпечення кібербезпеки об’єктів критичної інфраструктури та державних органів, зокрема розроблення методики ідентифікації та оцінки кіберризиків на національному рівні та для секторів критичної інфраструктури держави, забезпечення нормативного врегулювання питань щодо впровадження обов’язкового проведення періодичної оцінки кіберризиків на підставі розроблених методик, що передбачає: розроблення та затвердження методики ідентифікації та оцінки кіберризиків на національному рівні; нормативне врегулювання питань щодо впровадження обов’язковості проведення періодичної оцінки кіберризиків; 3) забезпечення розвитку систем криптографічного й технічного захисту інформації, пріоритетності використання засобів криптографічного та технічного захисту інформації вітчизняного виробництва для кіберзахисту державних інформаційних ресурсів та об’єктів критичної інформаційної інфраструктури, що включає: проведення державної експертизи у сфері криптографічного та технічного захисту інформації; ліцензування господарської діяльності в галузі криптографічного й технічного захисту інформації [113].

Визначаючи місце Служби безпеки України у Стратегічному плануванні забезпечення безпеки та стійкості функціонування об’єктів критичної інфраструктури, слід звернути увагу на зміст наказу СБУ «Про затвердження форм планів захисту об’єктів критичної інфраструктури та рекомендацій з розроблення планів захисту» від 19 січня 2024 року № 21, яким було затверджено: форму плану захисту об’єкта критичної інфраструктури за проєктною загрозою національного рівня «Терористичний акт або диверсія»; рекомендації з розроблення плану захисту об’єкта критичної інфраструктури за проектною загрозою національного рівня «Терористичний акт або диверсія»; форму плану захисту об’єкта критичної інфраструктури за проєктною загрозою національного рівня «Економічний тероризм»; рекомендації з розроблення плану захисту об’єкта критичної

інфраструктури за проєктною загрозою національного рівня «Економічний тероризм» [120]. Так, документом передбачено основи організації антитерористичного/контрдиверсійного захисту. Зокрема, зазначено, що підрозділ охорони об'єкта виконує такі основні завдання: захист об'єкта від актів втручання; забезпечення на об'єкті пропускного та внутрішньооб'єктового режимів; попередження та припинення правопорушень на об'єкті критичної інфраструктури; пошук та затримання осіб, які незаконно проникли на об'єкт; забезпечення публічної безпеки та порядку на об'єкті; контроль за дотриманням протипожежного режиму, а також участь у ліквідації наслідків аварій, катастроф, стихійних лих та інших надзвичайних ситуацій на об'єктів [120]. Служба безпеки та підрозділ охорони комплектуються громадянами України віком не молодше 18 років. Захист об'єкта здійснюється підрозділами охорони за допомогою стаціонарних і рухомих постів, а також мобільних груп. Стаціонарні пости виставляються на контрольно-пропускних пунктах об'єкта, що охороняється, і на постах охорони по його периметру. Для контролю за обстановкою всередині та навколо ОКІ, що охороняється, використовуються рухомі пости охорони й мобільні групи, у разі необхідності, залежно від ландшафту, з використанням транспортних засобів високої прохідності [120].

Своєю чергою організаційно-правові заходи із фізичного захисту передбачають: організацію спеціальної перевірки осіб, які мають бути допущені до особливих робот, відповідно до чинного законодавства; порядок допуску екстрених служб на територію об'єкта в разі виникнення надзвичайних подій; порядок взаємодії між різними службами охорони, які задіяні до охорони об'єкта; інструкцію першочергових та подальших дій служб охорони та працівників об'єкта при виявленні вибухонебезпечних та інших речовин, які можуть становити загрозу; забезпечення захисту інформації з обмеженим доступом; визначення рівнів фізичного захисту, виходячи з проєктної загрози, урахування особливостей конструкції ОКІ та

регіону її розташування, категорій та характеристик ядерних матеріалів; підбір кадрів з фізичного захисту та необхідний рівень їх кваліфікації; забезпечення охорони; проведення оцінки вразливості; розробку та підтримку дієздатності об'єктового плану взаємодії на випадок вчинення актів ядерного тероризму чи диверсії; забезпечення надійного зв'язку між учасниками об'єктового плану взаємодії на випадок вчинення актів тероризму чи диверсії; розробку та дотримання плану забезпечення фізичного захисту; фінансове забезпечення фізичного захисту [120].

Аналізуючи наказ СБУ від 19 січня 2024 року № 21 «Про затвердження форм планів захисту об'єктів критичної інфраструктури та рекомендацій з розроблення планів захисту», варто зазначити, що він, безперечно, не розкриває всі важливі внутрішні аспекти діяльності СБУ за цим напрямом, що є цілком логічним і зрозумілим з точки зору закритості відомства. Втім, з огляду на наявний матеріал, зауважимо, що вказаний наказ загалом виконує важливу нормативну функцію щодо уніфікації підходів до планування захисту об'єктів критичної інфраструктури та створює підґрунтя для взаємодії СБУ з різними суб'єктами у досліджуваній сфері суспільного життя. Водночас, з погляду забезпечення реальної безпеки та стійкості функціонування таких об'єктів, документ має низку концептуальних і практичних недоліків, які обмежують його прикладну цінність у сучасних умовах. Зокрема, наказ орієнтований переважно на формальне планування та документування заходів, а не на управління ризиками як безперервним процесом. Запропоновані форми та рекомендації фіксують поточний стан об'єкта й перелік базових організаційних і технічних заходів, але не забезпечують належної глибини аналізу загроз, особливо комбінованих та динамічних, характерних для воєнного часу, гібридних впливів і швидкої ескалації інцидентів. У результаті плани захисту ризикують перетворюватися на статичні документи, які швидко втрачають актуальність і не відображають реального профілю загроз.

Стратегічне планування має передбачати вивчення позитивного зарубіжного досвіду. Так, наприклад, у Великій Британії існують Стратегічні координаційні групи (англ. Strategic Coordinating Group, SCG) при місцевих форумах стійкості, які активуються в разі виникнення надзвичайних ситуацій, ліквідація наслідків яких потребує: ефективного антикризового управління; централізованої координації дій на оперативному й тактичному рівнях; забезпечення якісної взаємодії з вищими органами влади (автономії, держави); забезпечення додатковими спроможностями; об'єднання зусиль місцевих громад. Стратегічні координаційні групи формуються заздалегідь із досвідчених представників категорії 1, керівників цільових робочих підгруп місцевих форумів стійкості, а також фахівців категорії 2, досвід яких може бути корисним для вирішення кризової ситуації. Глави та склад учасників SCG обираються з урахуванням типу надзвичайної ситуації, що виникла (пожежа, повінь, техногенні чи транспортні аварії, пандемія тощо). Завданнями SCG є: забезпечення координації дій під час ліквідації надзвичайних ситуацій та підтримання внутрішніх і зовнішніх комунікацій; узгодження стратегічних пріоритетів щодо реагування на надзвичайні ситуації, які виникли; розроблення загальної стратегії та завдань для сил оперативного реагування; об'єктивне визначення необхідних додаткових ресурсів і їх розподіл; здійснення фінансового контролю над використанням ресурсів; підтримання комунікативних зв'язків із сусідніми місцевими форумами стійкості, координаційними структурами вищого рівня (автономії, держави); інформаційне забезпечення всіх учасників ліквідації надзвичайних ситуацій; інформування місцевих громад через медіа. Для функціонування SCG створюється Центр стратегічної координації (англ. Strategic Coordination Centre, SCC) [136, с. 34–35].

Підбиваючи підсумки представленого підрозділу наукового дослідження, слід зазначити, що стратегічне планування забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури є

ключовим елементом національної політики у сфері безпеки, оскільки воно визначає довгострокові підходи до захисту систем, від яких залежить життєдіяльність держави та суспільства. Таке планування спрямоване не лише на забезпечення безперервного функціонування об'єктів критичної інфраструктури, а й на підвищення її здатності протистояти комплексним, гібридним і технологічно складним загрозам, характерним для сучасного безпекового середовища.

У межах стратегічного планування Служба безпеки України посідає центральне та системоутворююче місце. Її роль визначається тим, що СБУ є основним державним органом, відповідальним за захист національної безпеки від диверсій, терактів, агентурної діяльності, кібератак та інших форм несанкціонованого втручання, які здатні порушити роботу критично важливих систем. У межах стратегічного планування Служба забезпечує аналітичну підтримку, виявляє загрози, проводить контррозвідувальні заходи, координує діяльність інших суб'єктів безпеки та здійснює погодження документів, пов'язаних із кіберзахистом та фізичною безпекою об'єктів. Її участь гарантує включення до планів реалістичних оцінок ризиків, своєчасного отримання інформації про потенційні небезпеки та впровадження заходів, що відповідають актуальним викликам. Таким чином, стратегічне планування у сфері критичної інфраструктури набуває цілісного та дієвого характеру саме завдяки тому, що СБУ слугує інтегруючою ланкою між різними державними органами, операторами інфраструктури та іншими учасниками системи безпеки. Її діяльність забезпечує злагодженість процесів, підвищує ефективність превентивних заходів і формує підґрунтя для стійкості держави до загроз, що здатні мати стратегічні наслідки.

3.2. Напрями вдосконалення адміністративно-правового регулювання діяльності Служби безпеки України щодо захисту об’єктів критичної інфраструктури в умовах правового режиму воєнного стану

У реаліях сьогодення діяльність Служби безпеки України, зокрема у сфері захисту об’єктів критичної інфраструктури, ускладнюється низкою чинників, серед яких, безперечно, ключовим є військова агресія з боку російської федерації та введення у зв’язку з нею правового режиму воєнного стану. Останній, відповідно до Закону України «Про правовий режим воєнного стану», становить особливий правовий режим, що вводиться в Україні або в окремих її місцевостях у разі збройної агресії чи загрози нападу, небезпеки державній незалежності України, її територіальній цілісності та передбачає надання відповідним органам державної влади, військовому командуванню, військовим адміністраціям та органам місцевого самоврядування повноважень, необхідних для відвернення загрози, відсічі збройної агресії та забезпечення національної безпеки, усунення загрози небезпеки державній незалежності України, її територіальній цілісності, а також тимчасове, зумовлене загрозою, обмеження конституційних прав і свобод людини та громадянина, прав і законних інтересів юридичних осіб із зазначенням строку дії цих обмежень [129].

Протягом війни критична інфраструктура України зазнала суттєвих втрат. Так, наприклад, станом на початок 2024 року прямі збитки, завдані українській енергетиці, становили 9 млрд доларів США. Під час оцінки пошкоджень у сфері енергетики використовували як прямі, так і непрямі методи розрахунку вартості втрачених і пошкоджених об’єктів. Вартість пошкоджених об’єктів визначено на основі первісної балансової вартості основних засобів, вартості поточних ремонтів, відновлення (ринкова вартість заміщення зруйнованого). Основна інформація щодо втрат в енергетиці надана Міністерством розвитку громад, територій та інфраструктури

України, Міністерством енергетики України. Для оцінки збитків на окремих великих об'єктах використовується індивідуальний підхід відповідно до інформації з відкритих джерел, від власників та керівників підприємств, центральних органів виконавчої влади. Збір даних щодо збитків об'єктів електрогенерації здійснювався агреговано, а також за відкритими джерелами у зв'язку із високим ризиком розповсюдження інформації щодо деталізованих пошкоджень об'єктів критичної інфраструктури в умовах війни [46].

Слід зауважити, що за час повномасштабної війни кількість кібератак на об'єкти систем зв'язку, управління Сил оборони, об'єкти критичної інфраструктури України та банківського сектору суттєво зросла. За даними Державної служби спеціального зв'язку та захисту інформації України (Держспецзв'язку) та CERT-UA (Урядова команда реагування на комп'ютерні надзвичайні події України), кількість кібератак на Україну суттєво збільшилася. У 2024 році кількість кіберінцидентів збільшилася майже на 70 % порівняно з 2023 роком, досягнувши 4315 інцидентів (проти 2541 у 2023 році). Така тенденція збереглась і 2025 року. Основними цілями атак були: 1) енергетичний сектор (залишається пріоритетною мішенню). Атаки спрямовані на дестабілізацію енергосистеми, спричинення відключень та психологічного тиску; 2) урядові установи та місцеві органи влади. Цілі атак включають викрадення чутливої інформації, отримання доступу до даних, компрометацію облікових записів і систем; 3) сектор безпеки й оборони. Хакери намагаються отримати розвідувальні дані, інформацію про плани Збройних Сил України, дані підприємств оборонно-промислового комплексу; 4) телекомунікації. Атаки спрямовані на порушення зв'язку, що може мати істотні наслідки для координації. Приклад – масштабна атака на «Київстар» у грудні 2023 року; 5) комерційні організації. Викрадення інформації та руйнівні атаки [55].

Найбільш поширеними типами атак були: а) розповсюдження шкідливого програмного забезпечення. Ідеться про програми-вимагачі, шпигунське програмне забезпечення, вайпери; б) фітинг, тобто створення підроблених електронних листів або вебсайтів для викрадення облікових даних. Часто використовується для поширення шкідливого програмного забезпечення; в) компрометація облікових записів/систем, а саме отримання несанкціонованого доступу до систем через скомпрометовані облікові записи; г) зловмисні підключення (несанкціонований доступ до мереж) [55].

У цьому контексті варто зауважити, що динаміка щодо кількості нейтралізованих атак за участю Служби безпеки України виглядає так: 2020 рік – 800 кібератак; 2021 рік – 1400 кібератак; 2022 рік – 4500 кібератак; 2023 рік – 4500 кібератак. Абсолютну більшість кібератак в Україні здійснюють російські спецслужби або хакерські угруповання, пов’язані з ними. Незначний відсоток атак проводять білоруські спецслужби, які сприяють росії. Одним із способів ефективно протидіяти кібератакам на об’єкти критичної інфраструктури є використання СБУ платформи MISP-UA (Malware Information Sharing Platform Ukrainian Advantage)» [56].

У війні залізниця відчутно продемонструвала свою роль як об’єкт критичної інфраструктури, забезпечивши безкоштовну евакуацію мільйонів українських громадян (а також значної кількості бізнесів), що опинились у зоні бойових дій; доставку критично важливих матеріалів та обладнання в ці регіони. У відповідь, українська залізниця стала активною мішенню для російських обстрілів та атак. За попередніми оцінками, загальний обсяг пошкодженого залізничного полотна становить до 507 км; кількість пошкоджених залізничних вокзалів і станцій – 126, з яких пошкоджено або знищено на підконтрольній території більше 53 і решта на неконтрольованих територіях. Понад 700 км залізничних колій знаходяться на тимчасово окупованій (після 24 лютого 2022 року) території. Загальна кількість пошкоджених, знищених і втрачених будівель, які належать Укрзалізниці,

оцінюється в 5,5 тис. і близько 4 тис. споруд. Причому є підстави вважати, що все рухоме майно Укрзалізниці, яке не було вивезено з таких територій вчасно, можна вважати повністю втраченим (зруйнованим або викраденим військами країни-агресора). Таким чином, загальні прямі збитки в цьому секторі станом на 2024 рік оцінюються в 4,3 млрд доларів США [46].

Усе зазначене вище суттєво вплинуло на функціонування і Служби безпеки України в межах захисту критичної інфраструктури, а також виявило прогалини та недоліки правового й організаційного характеру в роботі цього державного органу спеціального призначення з правоохоронними функціями, який забезпечує державну безпеку України. Специфіка правового статусу Служби безпеки України, а також особливості функціонування та необхідності захисту об'єктів критичної інфраструктури, обумовлюють той факт, що значна частина нормативно-правового матеріалу є засекреченою, що ускладнює оцінку стану адміністративно-правового регулювання досліджуваної сфери суспільного життя. Передусім варті уваги прогалини законів України «Про Службу безпеки України» та «Про критичну інфраструктуру».

Проведений у дисертаційному дослідженні аналіз, а також розгляд правозастосовної практики дав змогу визначити недоліки вказаних вище законодавчих актів. Так, недоліками Закону України «Про Службу безпеки України» в контексті представленої в роботі проблематики є такі:

1) документ не містить спеціальних адміністративно-правових норм, які б комплексно регулювали діяльність СБУ саме в умовах воєнного стану, зокрема щодо посиленого захисту об'єктів критичної інфраструктури;

2) у Законі відсутнє пряме закріплення та розкриття функцій СБУ як ключового суб'єкта захисту критичної інфраструктури;

3) положення цього законодавчого акта переважно орієнтовані на правоохоронну та контррозвідувальну складову, тоді як такі адміністративно-

превентивні механізми, як оцінка ризиків, адміністративний нагляд тощо, не набули належного нормативного закріплення;

4) в умовах воєнного стану розширення повноважень СБУ не супроводжується адекватним розвитком механізмів адміністративного контролю, що створює ризики: надмірного втручання в діяльність операторів критичної інфраструктури; порушення принципів законності та пропорційності.

Що ж стосується Закону України «Про критичну інфраструктуру», то ключовою проблемою цього документа є те, що він не визначає її провідної ролі в умовах воєнного стану, що: знижує ефективність управлінських рішень; ускладнює реалізацію спеціальних безпекових заходів.

З огляду на зазначене вище, удосконалення адміністративно-правового регулювання діяльності Служби безпеки України в умовах режиму воєнного стану щодо захисту об'єктів критичної інфраструктури має передбачати:

– по-перше, забезпечення гармонізації законів України «Про Службу безпеки України» та «Про критичну інфраструктуру» в частині: а) визначення місця СБУ в системі суб'єктів захисту критичної інфраструктури; б) закріплення та деталізації повноважень Служби в межах захисту об'єктів критичної інфраструктури;

– по-друге, уточнення правового статусу СБУ в межах виконання завдань у сфері захисту критичної інфраструктури, а також окреслення кола таких завдань і визначення повноважень;

– по-третє, узгодженість норм, що регулюють правовий статус режиму воєнного стану, з нормами, що регулюють питання захисту критичної інфраструктури, включно з уніфікацією процедур прийняття управлінських рішень;

– по-четверте, розробку та прийняття Типового положення про порядок взаємодії суб'єктів захисту критичної інфраструктури, метою якого має бути створення єдиного, чіткого та обов'язкового для застосування

адміністративно-правового механізму координації діяльності суб'єктів захисту критичної інфраструктури, спрямованого на забезпечення безперервного, узгодженого й ефективного функціонування об'єктів критичної інфраструктури, своєчасне виявлення, запобігання та нейтралізацію загроз їх безпеці, особливо в умовах дії правового режиму воєнного стану, з дотриманням принципів законності, пропорційності, відповідальності та розмежування компетенції між усіма учасниками.

Запровадження будь-яких нормативно-правових змін є фактично неможливим поза вдосконаленням організаційних та управлінських аспектів діяльності Служби безпеки України в умовах режиму воєнного стану щодо захисту об'єктів критичної інфраструктури. У цьому контексті, як вбачається, першим кроком має бути створення системи оцінювання ефективності діяльності СБУ за відповідним напрямом. Ефективність є багатоаспектним і складним економічним поняттям, що передбачає: по-перше, результативність діяльності (процесу, проєкту, реалізації заходів), що характеризується відношенням отриманого економічного ефекту до витрат ресурсів, які зумовили отримання цього результату; по-друге, комплексну оцінку результатів використання всіх видів ресурсів; по-третє, міру досягнення поставлених цілей [88]. Ефективність, пишуть А. О. Демченко та О. І. Момот, слугує як індикатор розвитку. Вона ж – його найважливіший стимул. Прагнучи підвищити ефективність конкретного виду діяльності та їх сукупності, ми визначаємо конкретні заходи, що сприяють процесу розвитку, і відсікаємо ті з них, що ведуть до регресу. Як категорія вона має два аспекти – якісний і кількісний. Перший відображає її логічне, теоретичний зміст, тобто сутність категорії. Кількісний аспект, продовжують автори, розкриває дію закону економії часу, а саме відображає економію часу під час досягнення цілей суспільного виробництва в ході всього відтворювального процесу і на окремих його фазах у масштабі всього народного господарства, окремих його регіонів, галузей, господарських суб'єктів. Тобто на всіх

історичних етапах розвитку людського суспільства воно має економно витрачати свої сили, досягаючи розширення випуску продукції при мінімальних витратах засобів. Це і є об'єктивно існуючим критерієм економічної ефективності на всіх щаблях розвитку суспільства [29, с. 208].

Отже, ефективність діяльності Служби безпеки України в умовах режиму воєнного стану щодо захисту об'єктів критичної інфраструктури – це інтегральна характеристика спроможності СБУ шляхом правомірного, своєчасного та скоординованого застосування адміністративно-управлінських, контррозвідувальних і безпекових заходів забезпечувати досягнення визначених цілей із запобігання, нейтралізації та мінімізації загроз об'єктам критичної інфраструктури, збереження їхньої функціональної стійкості та безперервності надання критично важливих послуг у воєнних умовах за оптимального використання наявних ресурсів і з дотриманням принципів законності, пропорційності та підзвітності. Для того, щоб визначити чи є діяльність ефективною, необхідним кроком є її оцінювання.

У словниковій літературі оцінюванням найбільш доцільно вважати систематичний процес порівняння діяльності та/чи результатів виконання програми або політики із цілями, завданнями, комплексом явних або неявно виражених стандартів з метою внесення необхідних адміністративних чи політичних змін. Причому оцінювання може бути зовнішнім і внутрішнім, кількісним та якісним, формувальним та підсумковим, бути орієнтованим на цілі, рішення, клієнта, практичне використання тощо. У системі органів публічної влади оцінювання є аналітичною діяльністю, спрямованою на збір, аналіз, тлумачення та передавання інформації про економічність, ефективність, результативність політики, програм, проєктів, які здійснюються з метою поліпшення соціальних умов. Для того, щоб оцінювання можна було вважати коректним і корисним, воно має бути систематичним та об'єктивним [43, с. 504].

Е. Ведунг розглядає оцінювання як процес встановлення значущості, вартості й цінності певних явищ або дій, що полягає у відмежуванні важливого та доцільного від другорядного або непотрібного. На думку дослідника, оцінювання слугує ключовою аналітичною процедурою, притаманною всім організованим інтелектуальним і практичним видам діяльності. Процес визначення переваг, вартості та цінності, зауважує автор, пронизує всі сфери теорії та практики, зокрема державну службу й урядове управління. У контексті публічного управління оцінювання Е. Ведунг трактує як ґрунтовний ретроспективний аналіз якості адміністрування, результатів і наслідків діяльності органів державної влади, що має практичну значущість для прийняття рішень у майбутньому. Оцінювання, яке за своєю суттю є формою професійного моніторингу, становить звичний елемент систем державного прийняття рішень. Поряд з постійним або періодичним моніторингом у певних випадках здійснюється й оцінювання впливу. Незалежно від форми реалізації, оцінювання проводиться з метою забезпечення звітності, вдосконалення діяльності або розширення базових знань. Саме ці три складові – звітність, удосконалення та формування базових знань – становлять загальну мету оцінювання. Водночас звітність і вдосконалення визнаються найбільш очевидними підставами для його здійснення, тоді як накопичення базових знань зазвичай розглядають як можливий, але побічний позитивний результат [22, с. 123].

О. І. Пікулик та Н. І. Власюк акцентують увагу на тому, що для оцінки діяльності державного органу управління можна використовувати кількісний, якісний і змішаний підхід. Кількісна оцінка проводиться в абсолютних та відносних величинах, які обчислюються на основі статистичних даних. Якісна оцінка базується на вивченні суб’єктивних думок щодо основної діяльності державних органів в межах їх компетенції. Змішаний тип оцінки передбачає одночасне використання кількісних та якісних методик для кращого врахування впливу внутрішніх і зовнішніх факторів на результати

функціонування державних інституцій. Залежно від підходу, різні дослідники у ході розгляду проблеми оцінки діяльності органів державного управління використовують різноманітну термінологію: оцінка результативності, оцінка якості та оцінка ефективності. Під оцінкою результативності розуміють міру досягнення очікуваного результату. Під оцінкою якості розуміють ступінь відповідності властивостей процесу чи явища його сутності. Чимало міркувань науковців стосуються оцінки ефективності, що засвідчує існування різного розуміння цієї категорії. Тому для оцінки ефективності діяльності державних інституцій, спрямованої на покращення соціально-економічного розвитку країни, необхідно передусім розглянути основні підходи до визначення та розуміння категорії «ефективність» [100].

Оцінювання діяльності Служби безпеки України в умовах режиму воєнного стану щодо захисту об’єктів критичної інфраструктури – це системний, цілеспрямований, науково й методично обґрунтований процес ретроспективного та поточного аналізу змісту, результатів і наслідків адміністративно-управлінських, контррозвідувальних та координаційних заходів, що здійснюються Службою безпеки України з метою забезпечення стійкого функціонування, захищеності та безпеки об’єктів критичної інфраструктури в умовах дії воєнного стану, шляхом визначення їхньої ефективності, результативності, законності та відповідності характеру воєнних і гібридних загроз, з подальшим використанням отриманих висновків для підзвітності, удосконалення управлінських рішень і формування науково обґрунтованої бази для розвитку системи національної безпеки.

Відповідно оцінювання має здійснюватись за певними критеріями, які мають бути точними, змістовними та практично орієнтованими. Розглядаючи різноманітні підходи до трактування оцінювання, особливу увагу Г. Кохан звернув увагу на визначення, запропоноване К. Вайс. Науковець називає оцінюванням систематичну оцінку операцій та/або результатів програми чи

політики у порівнянні з комплексом явних чи неявних стандартів з метою вдосконалення програми чи політики. Тут виокремлено п’ять ключових елементів [19, с. 25; 66]. Перший – систематична оцінка. Наголос на систематичність свідчить про науково-дослідницьку природу процедур оцінювання. Оцінювання здійснюється за строгими правилами, прийнятими у сфері дослідження. Другий і третій елементи визначають, на що саме спрямовується дослідження – на результати програми чи на вивчення процесів. У багатьох оцінювальних кампаніях для реципієнтів, замовників важливі і процес виконання програми, і її результати. Четвертим елементом є стандарти (норми), згідно з якими здійснюється порівняння. Після того, як дані про процеси і результати зібрано, настає етап оцінки якості програми шляхом порівняння її показників з певним комплексом очікуваних результатів. Незалежно від того, на чому зосереджується оцінювання (на процесах чи результатах програми), елемент порівняння і ухвалення рішень існує завжди. Іноді критерії, за якими ухвалюють рішення, випливають з офіційного переліку цілей програми і політики, що визначаються до початку впровадження програми. Цілі програми під час її виконання можуть змінюватись. Іншими стандартами (критеріями) оцінювання можуть бути очікування учасників програми і політичного процесу. Критерії оцінювання застосовуються за фактом (ретроспективно) [19, с. 25; 66].

На нашу думку, у межах порушеної в роботі проблематики найбільш доцільно використовувати класичний підхід до виділення подібних критеріїв та поділити їх на дві групи:

1) якісні, а саме: законність та обґрунтованість управлінських рішень і заходів; відповідність діяльності СБУ характеру та рівню воєнних і гібридних загроз; рівень превентивності у виявленні та нейтралізації загроз об’єктам критичної інфраструктури; ефективність міжвідомчої координації та взаємодії з операторами критичної інфраструктури; адаптивність управлінських рішень до динаміки воєнної обстановки; дотримання

принципу пропорційності й балансу між безпекою та правами людини; якість організаційно-правового забезпечення захисту об'єктів критичної інфраструктури; рівень підзвітності й контрольованості діяльності;

2) кількісні, зокрема: кількість виявлених і нейтралізованих загроз об'єктам критичної інфраструктури; кількість попереджених диверсійних, терористичних загроз та кібератак; частка об'єктів критичної інфраструктури, охоплених превентивними заходами безпеки; середній час реагування на загрози й інциденти; кількість проведених координаційних заходів, спільних операцій і нарад; кількість обов'язкових приписів, рекомендацій або заходів реагування, реалізованих операторами критичної інфраструктури; рівень безперервності функціонування об'єктів критичної інфраструктури під час воєнних загроз; динаміка зниження інцидентів безпеки порівняно з попередніми періодами.

Останнім важливим кроком є розв'язання проблем кадрового забезпечення СБУ. Служба безпеки України виконує надзвичайно важливі функції, спрямовані на захист національної безпеки та забезпечення стабільності в країні. Її робота є надзвичайно відповідальною та різноманітною, охоплюючи багато аспектів, від контррозвідки до кібербезпеки. Завдяки діяльності СБУ Україна може ефективно протидіяти внутрішнім і зовнішнім загрозам, забезпечуючи безпеку своїх громадян та збереження державного суверенітету, а правничі компетентності є фундаментом цієї діяльності. Без належної правової основи та юридичної підтримки виконання завдань СБУ було б неможливим, оскільки всі операції та заходи мають проводитися відповідно до закону та з дотриманням прав людини. Автори слушно наголошують, що правничі компетентності включають здатність співробітників СБУ розуміти та застосовувати закони, що регулюють їхню діяльність. Це забезпечує легітимність дій служби та довіру з боку громадськості. Крім того, правова грамотність сприяє ефективній співпраці з іншими правоохоронними органами та державними

структурами, що є необхідним для успішного виконання завдань, покладених на СБУ [143]. В. В. Блуд зазначає, що сутність кадрової роботи в органах і підрозділах Служби безпеки України виявляється в тому, що: 1) у ній набуває реалізації кадрова політика СБУ як державного органу спеціального призначення з правоохоронними функціями; 2) кадрова робота є актом правореалізації, яким забезпечуються регулювання службових відносин, що виникають між звичайними працівниками, державними службовцями, співробітниками військовослужбовцями та Службою безпеки України; 3) одним з напрямів кадрової роботи є забезпечення і підтримка службової дисципліни в органах та підрозділах СБУ; 4) кадрова робота здійснюється спеціальними кадровими підрозділами, передбаченими структурою СБУ. Таким чином, вказаний вище автор дійшов висновку, що кадрова робота в органах і підрозділах Служби безпеки України як напрям внутрішньоорганізаційної управлінської діяльності – це регламентована нормами чинного законодавства України та відомчими актами СБУ спеціалізована, процедурна діяльність кадрових підрозділів Служби, яка спрямована на формування та реалізацію кадрової політики, упорядкування службових відносин і забезпечення дисципліни [12].

Таким чином, кадрове забезпечення відіграє визначальну роль у діяльності Служби безпеки України в умовах режиму воєнного стану щодо захисту об’єктів критичної інфраструктури, оскільки саме людський фактор є ключовим елементом реалізації її адміністративно-правових, оперативно-службових і координаційних повноважень. Кадрове забезпечення визначає реальну спроможність Служби виконувати покладені на неї завдання в досліджуваній сфері суспільного життя. Особливо це актуально в умовах воєнного стану, коли суттєво зростає інтенсивність і складність загроз, що потребує наявності достатньої кількості підготовлених фахівців, здатних діяти в умовах підвищеного ризику, дефіциту часу та високої відповідальності. Недостатність або неякісність кадрового потенціалу

безпосередньо знижує ефективність навіть найбільш досконалих правових і організаційних механізмів. У цьому контексті В. В. Сліпенюк та А. С. Клименко вказує, що морально-психологічний стан працівника СБУ безпосередньо пов'язаний з усвідомленістю та відповідальністю здійснення ним своїх посадових обов'язків забезпечення національної безпеки та захисту національних інтересів. Посадові обов'язки співробітників СБУ призначені для убезпечення держави, боротьби із загрозами тероризму, розвідки, злочинності та іншими небезпечними явищами. Ця відповідальність може супроводжуватись високим рівнем стресу та психологічного навантаження в небезпечних ситуаціях, враховуючи конфліктні, кризові ситуації та загрози безпеці. Цей стрес може впливати на психологічний стан і загальне благополуччя працівників. Крім того, низький рівень морально-психологічного стану співробітників СБУ може призводити до колабораціоністської поведінки, яка підриває національну безпеку України, що є особливо небезпечним в умовах російсько-української війни [146, с. 78].

Отже, запровадження вказаних вище кроків дозволить комплексно підійти до вирішення не лише правових, а й організаційних аспектів діяльності Служби безпеки України в умовах режиму воєнного стану щодо захисту об'єктів критичної інфраструктури. Усе це своєю чергою позитивно вплине не лише на роботу СБУ, а й на загальний стан функціонування критичної інфраструктури в сучасних реаліях.

Висновок до розділу 3

З'ясовано, що стратегічне планування забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури – це довгостроковий, системний та комплексний процес формування цілей, принципів, пріоритетів і механізмів, спрямованих на попередження,

мінімізацію та нейтралізацію загроз, що можуть порушити безперервність роботи життєво важливих інфраструктурних систем держави. Таке планування має комплексний характер, адже передбачає узгодження дій між різними державними органами, операторами критичної інфраструктури, силовими структурами, науковими установами та громадськими інституціями, що забезпечує всебічне бачення ризиків і подальшого опрацювання шляхів їх подолання. Стратегічне планування в досліджуваній сфері охоплює визначення потенційних сценаріїв небезпеки, моделювання їх впливу, створення превентивних програм, розробку політик реагування та механізмів відновлення, а також забезпечення необхідних ресурсів, компетенцій і нормативної підтримки для досягнення стабільного та безпечного функціонування інфраструктурних об’єктів у мирний час і за умов криз чи воєнних загроз. Усе зазначене вище сприяє тому, що стратегічне планування слугує фундаментальним інструментом державного управління, який забезпечує прогнозованість, адаптивність та стійкість систем, від яких залежить життєдіяльність і стабільність функціонування суспільства.

Окреслено особливості стратегічного планування забезпечення безпеки та стійкості функціонування об’єктів критичної інфраструктури, до яких віднесено такі: 1) орієнтація на довгостроковий прогноз ризиків і сценаріїв загроз, які можуть бути скореговані залежно від безпекової, економічної та інших ситуацій; 2) має комплексний характер, адже має враховувати й поєднувати фізичну, технологічну, інформаційну, організаційну складові та кібербезпеку; 3) передбачає узгодження та координацію дій різними державними органами, операторами інфраструктури та суспільними інституціями; 4) має не лише превентивний характер, спрямований на запобігання інцидентам, а й реактивний; 5) враховує критичні залежності між різними секторами інфраструктури, зокрема критичної; 6) потребує чіткого розподілу ресурсів і компетенції спеціально уповноважених суб’єктів;

7) передбачає регулярне оновлення планів на основі аналізу інцидентів і результатів моніторингу.

Зауважено, що Національний план захисту та забезпечення безпеки та стійкості критичної інфраструктури, затверджений розпорядженням Кабінету Міністрів України від 19 вересня 2023 року № 825-р, формує єдину державну політику у сфері захисту та стійкості критичної інфраструктури. Документ закріплює системний підхід до управління ризиками, орієнтований не лише на фізичний захист об'єктів, а й на їхню функціональну стійкість та відновлюваність. Важливою перевагою є чітке розмежування ролей і відповідальності між органами державної влади, секторальними органами й операторами критичної інфраструктури, що створює передумови для підвищення керованості та координації в умовах криз і надзвичайних ситуацій. План також має стратегічний характер, узгоджений з європейськими та євроатлантичними підходами до захисту критичної інфраструктури, що є важливим у контексті євроінтеграції та безпекової співпраці. Окремим позитивом є акцент на підготовці кадрів та розвитку інституційної спроможності системи захисту критичної інфраструктури.

Встановлено недоліки Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури, а саме: по-перше, План видається досить загальним і містить відносно розмиті адміністративно-правові механізми для практичного виконання; по-друге, у ньому немає чітких показників оцінки ефективності, через що складно оцінити, чи досягнуто поставлені цілі; по-третє, недостатньо визначено питання ресурсів, зокрема фінансових, технічних і кадрових, які описані поверхово; по-четверте, механізми взаємодії з приватним сектором та громадськістю практично не деталізовані, хоча ці суб'єкти відіграють важливу роль у забезпечення безпеки критичної інфраструктури; по-п'яте, процедура обміну інформацією залишається нечіткою, що може впливати на швидкість і якість реагування на загрози.

Здійснено аналіз наказу СБУ від 19 січня 2024 року № 21 «Про затвердження форм планів захисту об’єктів критичної інфраструктури та рекомендацій з розроблення планів захисту», на основі чого зазначено, що він, безперечно, не розкриває всі важливі внутрішні аспекти діяльності СБУ за цим напрямом, що є цілком логічним і зрозумілим з точки зору закритості відомства. Зауважено, що вказаний наказ загалом виконує важливу нормативну функцію щодо уніфікації підходів до планування захисту об’єктів критичної інфраструктури та створює підґрунтя для взаємодії СБУ з різними суб’єктами у досліджуваній сфері суспільного життя. Водночас, з погляду забезпечення реальної безпеки та стійкості функціонування таких об’єктів, документ має низку концептуальних і практичних недоліків, які обмежують його прикладну цінність у сучасних умовах. Зокрема, наказ орієнтований переважно на формальне планування та документування заходів, а не на управління ризиками як безперервним процесом. Запропоновані форми та рекомендації фіксують поточний стан об’єкта й перелік базових організаційних і технічних заходів, але не забезпечують належної глибини аналізу загроз, особливо комбінованих та динамічних, характерних для воєнного часу, гібридних впливів і швидкої ескалації інцидентів. У результаті плани захисту ризикують перетворюватися на статичні документи, які швидко втрачають актуальність і не відображають реального профілю загроз.

Узагальнено, що стратегічне планування забезпечення безпеки та стійкості функціонування об’єктів критичної інфраструктури є ключовим елементом національної політики у сфері безпеки, оскільки воно визначає довгострокові підходи до захисту систем, від яких залежить життєдіяльність держави та суспільства. Таке планування спрямоване не лише на забезпечення безперервного функціонування об’єктів критичної інфраструктури, а й на підвищення її здатності протистояти комплексним, гібридним і технологічно складним загрозам, характерним для сучасного

безпекового середовища. Констатовано, що в межах стратегічного планування Служба безпеки України посідає центральне та системоутворююче місце. Її роль визначається тим, що Служба безпеки України є основним державним органом, відповідальним за захист національної безпеки від диверсій, терактів, агентурної діяльності, кібератак та інших форм несанкціонованого втручання, які здатні порушити роботу критично важливих систем. У межах стратегічного планування Служба забезпечує аналітичну підтримку, виявляє загрози, проводить контррозвідувальні заходи, координує діяльність інших суб'єктів безпеки та здійснює погодження документів, пов'язаних з кіберзахистом і фізичною безпекою об'єктів. Її участь гарантує включення до планів реалістичних оцінок ризиків, своєчасного отримання інформації про потенційні небезпеки та впровадження заходів, що відповідають актуальним викликам. Таким чином, стратегічне планування у сфері критичної інфраструктури набуває цілісного та дієвого характеру саме завдяки тому, що Служба безпеки України слугує інтегруючою ланкою між різними державними органами, операторами інфраструктури та іншими учасниками системи безпеки. Її діяльність забезпечує злагодженість процесів, підвищує ефективність превентивних заходів і формує підґрунтя для стійкості держави до загроз, що здатні мати стратегічні наслідки.

Доведено, що недоліками Закону України «Про Службу безпеки України» в контексті представленої в роботі проблематики є такі: 1) документ не містить спеціальних адміністративно-правових норм, які б комплексно регулювали діяльність СБУ саме в умовах воєнного стану, зокрема щодо посиленого захисту об'єктів критичної інфраструктури; 2) у Законі відсутнє пряме закріплення та розкриття функцій СБУ як ключового суб'єкта захисту критичної інфраструктури; 3) положення цього законодавчого акта переважно орієнтовані на правоохоронну та контррозвідувальну складову, тоді як такі адміністративно-превентивні

механізми, як оцінка ризиків, адміністративний нагляд тощо, не набули належного нормативного закріплення; 4) в умовах воєнного стану розширення повноважень СБУ не супроводжується адекватним розвитком механізмів адміністративного контролю, що створює ризики: надмірного втручання в діяльність операторів критичної інфраструктури; порушення принципів законності та пропорційності.

Констатовано, що вдосконалення адміністративно-правового регулювання діяльності Служби безпеки України в умовах режиму воєнного стану щодо захисту об'єктів критичної інфраструктури має передбачати: по-перше, забезпечення гармонізації законів України «Про Службу безпеки України» та «Про критичну інфраструктуру» в частині: а) визначення місця Служби безпеки України в системі суб'єктів захисту критичної інфраструктури; б) закріплення та деталізації повноважень Служби в межах захисту об'єктів критичної інфраструктури; по-друге, уточнення правового статусу Служба безпеки України в межах виконання завдань у сфері захисту критичної інфраструктури, а також окреслити коло таких завдань і визначити повноваження; по-третє, узгодженість норм, що регулює правовий статус режиму воєнного стану нормам законів, які регулюють питання захисту критичної інфраструктури, включно з уніфікацією процедур прийняття управлінських рішень; по-четверте, розробку та прийняти Типового положення про порядок взаємодії суб'єктів захисту критичної інфраструктури, метою якого має бути створення єдиного, чіткого й обов'язкового для застосування адміністративно-правового механізму координації діяльності суб'єктів захисту критичної інфраструктури, спрямованого на забезпечення безперервного, узгодженого й ефективного функціонування об'єктів критичної інфраструктури, своєчасне виявлення, запобігання та нейтралізацію загроз їх безпеці, особливо в умовах дії правового режиму воєнного стану, з дотриманням принципів законності,

пропорційності, відповідальності та розмежування компетенції між усіма учасниками.

Зауважено, що оцінювання діяльності Служби безпеки України в умовах режиму воєнного стану щодо захисту об'єктів критичної інфраструктури – це системний, цілеспрямований та науково і методично обґрунтований процес ретроспективного та поточного аналізу змісту, результатів і наслідків адміністративно-управлінських, контррозвідувальних й координаційних заходів, що здійснюються Службою безпеки України з метою забезпечення стійкого функціонування, захищеності та безпеки об'єктів критичної інфраструктури в умовах дії воєнного стану, шляхом визначення їхньої ефективності, результативності, законності та відповідності характеру воєнних і гібридних загроз, з подальшим використанням отриманих висновків для підзвітності, удосконалення управлінських рішень і формування науково обґрунтованої бази для розвитку системи національної безпеки.

Аргументовано, що критерії оцінювання діяльності Служби безпеки України в умовах режиму воєнного стану щодо захисту об'єктів критичної інфраструктури слід поділити на дві групи: 1) якісні, а саме: законність та обґрунтованість управлінських рішень і заходів; відповідність діяльності СБУ характеру та рівню воєнних і гібридних загроз; рівень превентивності у виявленні та нейтралізації загроз об'єктам критичної інфраструктури; ефективність міжвідомчої координації та взаємодії з операторами критичної інфраструктури; адаптивність управлінських рішень до динаміки воєнної обстановки; дотримання принципу пропорційності й балансу між безпекою та правами людини; якість організаційно-правового забезпечення захисту об'єктів критичної інфраструктури; рівень підзвітності й контрольованості діяльності; 2) кількісні, зокрема: кількість виявлених і нейтралізованих загроз об'єктам критичної інфраструктури; кількість попереджених диверсійних, терористичних загроз та кібератак; частка

об’єктів критичної інфраструктури, охоплених превентивними заходами безпеки; середній час реагування на загрози й інциденти; кількість проведених координаційних заходів, спільних операцій і нарад; кількість обов’язкових приписів, рекомендацій або заходів реагування, реалізованих операторами критичної інфраструктури; рівень безперервності функціонування об’єктів критичної інфраструктури під час воєнних загроз; динаміка зниження інцидентів безпеки порівняно з попередніми періодами.

Наголошено, що кадрове забезпечення визначає реальну спроможність Служби виконувати покладені на неї завдання в досліджуваній сфері суспільного життя. Особливо це актуально в умовах воєнного стану, коли суттєво зростає інтенсивність і складність загроз, що потребує наявності достатньої кількості підготовлених фахівців, здатних діяти в умовах підвищеного ризику, дефіциту часу та високої відповідальності. Недостатність або неякісність кадрового потенціалу безпосередньо знижує ефективність навіть найбільш досконалих правових і організаційних механізмів.

ВИСНОВКИ

У дисертації наведено теоретичне узагальнення та нове вирішення наукового завдання, яке полягало в тому, щоб встановити сутність і розкрити особливості адміністративно-правових засад діяльності Служби безпеки України щодо захисту об’єктів критичної інфраструктури, а також на основі узагальнення правозастосовної практики надати обґрунтовані пропозиції та рекомендації, спрямовані на вдосконалення адміністративного законодавства в цій сфері. У результаті дослідження сформульовано низку нових наукових висновків, основні з них такі:

1. Розкрито сутність захисту критичної інфраструктури, зокрема доведено, що це – комплексна, систематична, багатовекторна діяльність, яка реалізується в процесі створення та управління об’єктом критичної інфраструктури та спрямовується на профілактику, попередження, виявлення та припинення загроз безпеці функціонування та власне факту існування такого об’єкта, відшкодування шкоди та виправлення негативних наслідків у разі реалізації загроз. Зауважено, що захист об’єктів критичної інфраструктури як об’єкта адміністративно-правового регулювання характеризується тим, що ця діяльність: по-перше, детермінована обов’язком держави забезпечувати права, свободи, законні інтереси людини та громадянина, а також створювати безпечні для життя та здоров’я нації умови існування; по-друге, організовується та здійснюється у форматі окремої ланки державної політики; по-третє, проводиться щодо об’єктів, віднесення яких до критичної інфраструктури відбувається за волею уповноважених органів державної влади в нормативно встановленому порядку. Крім того, захист критичної інфраструктури належить до предмета діяльності Служби безпеки України, яка протидіє правопорушенням у цій сфері та є одним з правоохоронних органів, що входять до складу системи відповідних суб’єктів захисту.

2. Доведено, що Служба безпеки України має досить вузьке спрямування діяльності у сфері забезпечення безпеки та стійкості функціонування об’єктів критичної інфраструктури. Служба є спеціалізованим правоохоронним органом, уповноваженим протидіяти загрозам, що мають підвищений рівень публічної небезпеки та які здатні завдати шкоди не лише окремим об’єктам критичної інфраструктури, а й життєво важливим інтересам суспільства та держави загалом. Наголошено, що саме комплексний характер цих загроз, які можуть зачіпати безпеку населення, суверенітет і конституційний лад, зумовлює унікальне місце Служби безпеки України в системі суб’єктів забезпечення безпеки та стійкості функціонування досліджуваної сфери, а її повноваження дозволяють не лише реагувати на посягання та різноманітні загрози, а й здійснювати превентивний вплив, формуючи ключову ланку державного механізму захисту критично важливих об’єктів.

3. З’ясовано, що завданнями забезпечення безпеки та стійкості функціонування об’єктів критичної інфраструктури Службою безпеки України є такі: 1) участь у реалізації (у межах визначеної Законом України «Про Службу безпеки України» та відповідними відомчими нормативно-правовими актами компетенції, мети й завдань) державної політики у сфері захисту об’єктів критичної інфраструктури; 2) здійснення у встановленому законодавством порядку попередження, профілактики, виявлення, розкриття та розслідування злочинів, які належать до підслідності органів Служби безпеки України та вчинені на об’єктах критичної інфраструктури або стосовно них; 3) організація та реалізація заходів, спрямованих на боротьбу з тероризмом, диверсіями, зокрема з використанням інформаційних і цифрових технологій, на об’єктах критичної інфраструктури; 4) виявлення осіб, організованих злочинних груп та злочинних організацій, діяльність яких спрямована на порушення безпеки об’єктів критичної інфраструктури, перешкоджання їх нормальній роботі, а також забезпечення притягнення цих

осіб до встановленої законом відповідальності; 5) організаційне, матеріально-технічне, кадрове, фінансово-господарське та інше забезпечення діяльності органів і підрозділів Служби безпеки України, залучених до забезпечення безпеки й захисту об'єктів критичної інфраструктури від злочинів, що належать до її підслідності; 6) систематична оцінка ризиків, моніторинг наявних загроз критичній інфраструктурі держави з огляду на умови об'єктивної дійсності політичного, економічного, військового та іншого змісту, а також планування заходів протидії таким загрозам, мінімізації їх негативного впливу; 7) особлива процедура організації та забезпечення системної взаємодії між органами, підрозділами Служби безпеки України та іншими суб'єктами національної системи захисту критичної інфраструктури з питань обміну інформацією, планування спільних профілактичних заходів, реагування на загрози безпеки функціонування об'єктів критичної інфраструктури; 8) забезпечення захисту відомостей, що становлять державну таємницю, у сфері роботи об'єктів критичної інфраструктури.

Встановлено, що принципи забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури Службою безпеки України – це нормативно закріплені та засновані на загальновизнаних цінностях і призначенні права, базові юридичні засади, які визначають зміст, організацію та порядок діяльності Служби безпеки України щодо запобігання загрозам, охорони й підтримання стабільного функціонування об'єктів критичної інфраструктури. До таких принципів віднесено: законність та верховенство права; принцип забезпечення та дотримання прав та свобод людини і громадянина; координованості та взаємодії; гнучкості та адаптивності до змін; конфіденційності та захисту таємної інформації.

Обґрунтовано, що стан нормативних засад забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури в діяльності Служби безпеки України можна оцінити як загалом сформований, але такий, що залишається недостатньо систематизованим і орієнтованим передусім на

безпекові та контррозвідувальні аспекти. Досліджуване нормативне регулювання забезпечує Службу безпеки України необхідними повноваженнями для виявлення та нейтралізації загроз об’єктам критичної інфраструктури, однак воно переважно зосереджене на реагуванні на загрози, а не на комплексному забезпеченні стійкості та безперервності їх функціонування. Водночас спостерігається недостатня деталізація механізмів координації з іншими суб’єктами захисту критичної інфраструктури й обмежена регламентація превентивних заходів, що знижує ефективність практичної реалізації відповідних повноважень.

4. Зазначено, що адміністративно-правовий статус Служби безпеки України щодо захисту об’єктів критичної інфраструктури – це системна сукупність визначених законодавством України юридичних елементів, які встановлюють місце, роль і призначення Служби безпеки України в суспільно-правових відносинах, що виникають з метою реалізації діяльності, спрямованої на забезпечення безпеки і стійкості функціонування об’єктів критичної інфраструктури. Наголошено, що адміністративно-правовий статус Служби безпеки України характеризується багатьма відмінними аспектами, які визначають унікальність органу та його впливовість, що передбачає статус правоохоронного та спеціально уповноваженого органу з питань забезпечення охорони державної таємниці, ключове місце серед суб’єктів боротьби з тероризмом, а також високий рівень управлінської незалежності. Безпосередньо структура цього статусу охоплює компетенцію, повноваження, гарантії діяльності із захисту критичної інфраструктури та відповідальність за ефективність провадження останньої.

5. З’ясовано, що адміністративно-правовий механізм захисту об’єктів критичної інфраструктури Службою безпеки України – це юридична конструкція, яку становлять адміністративно-правові інструменти, що реалізуються уповноваженими органами, підрозділами, окремими посадовими особами Служби з метою впливу на сферу критичної

інфраструктури, а також забезпечення стійкості, безпеки функціонування зарахованих до неї об'єктів. Структуру цього адміністративно-правового механізму становлять: 1) адміністративно-правові інструменти захисту об'єктів критичної інфраструктури; 2) інституційна основа реалізації відповідних інструментів; 3) нормативні акти, що визначають порядок і специфіку реалізації останніх.

6. Констатовано, що адміністративно-правові інструменти є важливою складовою діяльності Служби безпеки України у сфері захисту критичної інфраструктури, оскільки саме через них забезпечується превентивний, регулятивний та охоронний вплив держави на стратегічно значущі об'єкти. Попри те, що Служба традиційно асоціюється передусім з кримінально-процесуальними формами протидії злочинності, її роль як суб'єкта публічної адміністрації є не менш значущою. Використовуючи надані законом повноваження, Служба безпеки України формує та реалізує комплекс управлінських і контрольно-наглядових механізмів, спрямованих на попередження загроз, підтримання стійкості та безперебійності функціонування критичної інфраструктури. Крім того, у цьому контексті Служба не обмежується загальними адміністративними засобами, адже її спеціальний статус передбачає можливість застосування більш складних правових інструментів, характерних для контррозвідувальної, антитерористичної та інформаційно-аналітичної діяльності. Саме поєднання цих загальних і спеціальних адміністративно-правових механізмів забезпечує комплексний, системний характер державного впливу на сферу, що має вирішальне значення для національної безпеки.

7. Аргументовано, що взаємодія Служби безпеки України з державними та громадськими інституціями в процесі запобігання несанкціонованому втручанню в роботу об'єктів критичної інфраструктури має ключове значення для формування комплексної, стійкої та превентивної системи національної безпеки. Сучасні загрози, такі як кібератаки, диверсійні дії,

інформаційні операції та технологічні ризики, роблять ізольовану діяльність будь-якого одного суб'єкта протидії недостатньою та неефективною. Участь Служби безпеки України в широкій мережі взаємодії забезпечує своєчасне виявлення небезпек, оперативний обмін інформацією та залучення необхідних компетенцій для захисту критично важливих систем, від яких залежить функціонування держави та базові потреби громадян. Співпраця з державними структурами дозволяє узгоджувати стандарти безпеки, формувати спільну політику реагування та координувати дії в разі кризових ситуацій. Водночас взаємодія з громадськими організаціями та професійними спільнотами посилює прозорість, забезпечує додаткові канали моніторингу загроз, сприяє поширенню знань про безпеку й залучає експертний потенціал, що є особливо важливим у сфері швидко змінюваних технологій. Така модель співпраці створює багаторівневу систему захисту, у якій Служба безпеки України слугує центральним координатором, а державні та громадські партнери – активними учасниками процесу, що підвищує стійкість критичної інфраструктури та мінімізує ризики її виведення з ладу чи використання в шкідливих цілях.

8. Узагальнено, що стратегічне планування забезпечення безпеки та стійкості функціонування об'єктів критичної інфраструктури є ключовим елементом національної політики у сфері безпеки, оскільки воно визначає довгострокові підходи до захисту систем, від яких залежить життєдіяльність держави та суспільства. Таке планування спрямоване не лише на забезпечення безперервного функціонування об'єктів критичної інфраструктури, а й на підвищення її здатності протистояти комплексним, гібридним і технологічно складним загрозам, характерним для сучасного безпекового середовища. Констатовано, що в межах стратегічного планування Служба безпеки України посідає центральне та системоутворююче місце. Її роль визначається тим, що Служба безпеки України є основним державним органом, відповідальним за захист

національної безпеки від диверсій, терактів, агентурної діяльності, кібератак та інших форм несанкціонованого втручання, які здатні порушити роботу критично важливих систем. У межах стратегічного планування Служба забезпечує аналітичну підтримку, виявляє загрози, проводить контррозвідувальні заходи, координує діяльність інших суб'єктів безпеки та здійснює погодження документів, пов'язаних з кіберзахистом і фізичною безпекою об'єктів. Її участь гарантує включення до планів реалістичних оцінок ризиків, своєчасного отримання інформації про потенційні небезпеки та впровадження заходів, що відповідають актуальним викликам. Таким чином, стратегічне планування у сфері критичної інфраструктури набуває цілісного та дієвого характеру саме завдяки тому, що Служба безпеки України слугує інтегруючою ланкою між різними державними органами, операторами інфраструктури та іншими учасниками системи безпеки. Її діяльність забезпечує злагодженість процесів, підвищує ефективність превентивних заходів і формує підґрунтя для стійкості держави до загроз, що здатні мати стратегічні наслідки.

9. Встановлено, що вдосконалення адміністративно-правового регулювання діяльності Служби безпеки України в умовах режиму воєнного стану щодо захисту об'єктів критичної інфраструктури має передбачати: по-перше, забезпечення гармонізації законів України «Про Службу безпеки України» та «Про критичну інфраструктуру» в частині: а) визначення місця Служби безпеки України в системі суб'єктів захисту критичної інфраструктури; б) закріплення та деталізації повноважень Служби в межах захисту об'єктів критичної інфраструктури; по-друге, уточнення правового статусу Служба безпеки України в межах виконання завдань у сфері захисту критичної інфраструктури, а також окреслити коло таких завдань і визначити повноваження; по-третє, узгодженість норм, що регулює правовий статус режиму воєнного стану нормам законів, які регулюють питання захисту критичної інфраструктури, включно з уніфікацією процедур прийняття

управлінських рішень; по-четверте, розробку та прийняти Типового положення про порядок взаємодії суб'єктів захисту критичної інфраструктури, метою якого має бути створення єдиного, чіткого й обов'язкового для застосування адміністративно-правового механізму координації діяльності суб'єктів захисту критичної інфраструктури, спрямованого на забезпечення безперервного, узгодженого й ефективного функціонування об'єктів критичної інфраструктури, своєчасне виявлення, запобігання та нейтралізацію загроз їх безпеці, особливо в умовах дії правового режиму воєнного стану, з дотриманням принципів законності, пропорційності, відповідальності та розмежування компетенції між усіма учасниками.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Адміністративне право України (загальна частина) : навч. посіб. / О. І. Остапенко, М. В. Ковалів, С. С. Єсімов та ін. 2-е вид., доп. Львів : СПОЛОМ, 2021. 616 с.

2. Адміністративне право України. Академічний курс : підручник : у 2 т. / ред. колегія : В. Б. Авер'янов (голова). Київ : Юридична думка, 2004. Т. 1 : Загальна частина. 584 с.

3. Адміністративне право України. Повний курс : підручник / В. Галунько, П. Діхтієвський, О. Кузьменко та ін. ; за заг. ред. В. Галунька, О. Правотворової. 3-тє вид. Херсон : ОЛДІ-ПЛЮС, 2020. 584 с.

4. Алфьоров С. М. Адміністративно-правовий механізм протидії корупції в органах внутрішніх справ : автореф. дис. ... д-ра юрид. наук : 12.00.07. Харків, 2011. 38 с.

5. Антологія української юридичної думки : у 6 т. / редкол.: Ю. С. Шемшученко (голова) та ін. Київ : Юридична книга, 2003. Т. 4 : Конституційне (державне) право / упоряд. В. Ф. Погорілко, О. В. Батанов, В. Л. Федоренко ; відп. ред. В. Ф. Погорілко. 600 с.

6. Арсенович Л. А. Парадигма захисту критичної інфраструктури в системі національної безпеки України. *Державне управління: удосконалення та розвиток.* 2024. № 8. DOI: http://doi.org/10.32702/2307-2156.2024.8.7. URL: https://www.nayka.com.ua/index.php/dy/article/view/4404.

7. Балашов А. М. Формування механізмів державного управління сталим розвитком регіонів України : дис. … д-ра наук з держ. упр. : 25.00.02. Запоріжжя, 2010. 315 с.

8. Бевз С. І. Поняття та елементи механізму адміністративно-правового регулювання державного управління господарською діяльністю. *Прикарпатський юридичний вісник*. 2018. Вип. 4 (25), т. 2. С. 43–47.

9. Безпалова О. І. Адміністративно-правовий механізм реалізації правоохоронної функції держави : монографія. Харків : Харк. нац. ун-т внутр. справ, 2014. 544 с.

10. Безпалова О. І., Горбач Д. О. Поняття та структура адміністративно-правового статусу Національної гвардії України. *Форум права*. 2017. № 5. С. 31–38.

11. Белькова О. В. Поняття та особливості правового статусу свідка в кримінальному процесі України. *Право і безпека*. 2003. № 2’1. С. 52–54.

12. Блуд В. В. Сутність кадрової роботи в органах та підрозділах Служби безпеки України як напряму внутрішньо організаційної управлінської діяльності. *Юридичний науковий електронний журнал*. 2023. № 9. С. 598–600. URL: http://lsej.org.ua/9_2023/147.pdf.

13. Богдан Б. В. Інститут критичної інфраструктури як предмет наукового дослідження. *Юридичний електронний журнал*. 2025. № 3. С. 667–669.

14. Боняк В. О. Конституційне право людини і громадянина на освіту та його забезпечення в Україні : дис. … канд. юрид. наук. : 12.00.02. Київ, 2005. 205 с.

15. Браун М. Пол. Посібник з аналізу / пер. з англ. Київ : Основи, 2000. 243 с.

16. Бровко Л. За два дні правоохоронці запобігли чотирьом терактам і диверсіям в Україні. *Бабель.* URL: https://babel.ua/news/115899-za-dva-dni-pravoohoronci-zapobigli-chotirom-teraktam-i-diversiyam-v-ukrajini.

17. Бузунов Р. А. Адміністративно-правове регулювання кредитно-модульної системи організації навчального процесу (в ВНЗ системи МВС) : дис. … д-ра юрид. наук : 12.00.07. Ірпінь, 2007. 434 с.

18. Бурда С. Я. Адміністративно-правовий захист учасників виборів і референдумів в Україні : дис. … канд. юрид. наук. : 12.00.07. Львів, 2010. 223 с.

19. Вайс К. Оцінювання. Київ : Основи, 2000. 671 с.

20. Вахров А. Г. Адміністративно-правовий механізм взаємодії суб'єктів безпеки й оборони щодо забезпечення Національної безпеки: питання теорії та практики : дис. … канд. юрид. наук : 12.00.07. Кропивницький, 2023. 226 с.

21. Ведєрніков Ю. А., Папірна А. В. Теорія держави і права : навч. посіб. Київ : Знання, 2008. 333 с.

22. Ведунг Е. Оцінювання державної політики і програм / пер. з англ. В. Шульга. Київ : Всеувито, 2003. 350 с.

23. Великий тлумачний словник сучасної української мови (з дод. і допов.) / уклад, і голов. ред. В. Т. Бусел. Київ ; Ірпінь : Перун, 2005. 1728 с.

24. Великий тлумачний словник сучасної української мови / уклад. і голов. ред. В. Т. Бусел. Київ ; Ірпінь : Перун, 2001. 1440 с.

25. Герасименко О. М. Критична інфраструктура України як предмет наукового пізнання: теоретичні аспекти. *Науковий вісник Ужгородського національного університету.* Серія : Право. 2024. Вип. 85, ч. 4. С. 42–49.

26. Городяненко В. Г. Соціологія : підручник. Київ : Академія, 2003. 560 с.

27. Гречанюк С. К. Організаційно-правові засади взаємодії кримінально-виконавчих установ з державними органами та недержавними організаціями : дис. ... канд. юрид. наук : 12.00.07. Ірпінь, 2006. 253 с.

28. Дворецька Г. В. Соціологія : навч. посіб. Київ : КНЕУ, 2001. 244 с. URL: https://buklib.net/books/23421

29. Демченко А. О., Момот О. І. Про сутність понять „ефективність" та „результативність" в економіці. *Економічний вісник Донбасу*. 2013. № 3 (33). С. 207–210.

30. Держава посилює захист об'єктів критичної інфраструктури від кіберзагроз. *7eminar.ua*. URL: https://7eminar.ua/news/3463-derzava-posilyuje-zaxist-informaciyi-vid-kiberzagroz.

31. Державне управління в Україні: наукові, правові, кадрові та організаційні засади : навч. посіб. / за заг. ред. Н. Р. Нижник, В. М. Олуйка. Львів : Нац. ун-т «Львівська політехніка», 2002. 352 с.

32. Деякі питання об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 09.10.2020 р. № 1109. *Офіційний вісник України*. 2020. № 93. Ст. 2994.

33. Деякі питання паспортизації об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 04.08.2023 р. № 818. *Офіційний вісник України.* 2023. № 77. Ст. 4366.

34. Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози : Постанова Кабінету Міністрів України від 26.11.2025 р. №1533. *Урядовий кур'єр*. 2025. 2 грудня. (№ 246).

35. Деякі питання розробки, затвердження та погодження планів захисту об'єктів критичної інфраструктури за проектною загрозою національного рівня «кібератака/кіберінцидент» : наказ Служби безпеки України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 19.12.2024 р. № 627/772. *Державна служба спеціального зв'язку та захисту інформації України*. URL: https://cip.gov.ua/ua/news/spilnii-nakaz-sluzhbi-bezpeki-ukrayini-ta-administraciyi-derzhspeczv-yazku-vid-19-grudnya-2024-roku-627-772-deyaki-pitannya-rozrobki-zatverdzhennya-ta-pogodzhennya-planiv-zakhistu-ob-yektiv-kritichnoyi-infrastrukturi-za-proektnoyu-zagrozoyu-nacionalnogo-rivnya-kiberataka-kiberincident.

36. Дикань Н. В., Борисенко І. І. Менеджмент : навч. посіб. Київ : Знання, 2008. 389 с.

37. Директива Європейського Парламенту і Ради (ЄС) 2022/2557 про стійкість критично важливих суб'єктів та скасування Директиви Ради 2008/114/ЄС : ухв. від 14.12.2022 р. № 2022/2557. *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/9a3_002-22#Text.

38. Дрозд О. Ю., Сорока Л. В., Миськів Л. І. Загальнотеоретичні основи концепту «адміністративно-правовий статус державної служби» з оглядом його особливостей на прикладі органів Державної виконавчої служби. *Юридичний науковий електронний журнал*. 2023. № 5. С. 506–508.

39. Дронік Д. С. Адміністративно-правові засади діяльності патрульної поліції в Україні : дис. … д-ра філос. : 081. Кропивницький, 2023. 241 с.

40. Дубенко О. І. Адміністративно-правовий механізм забезпечення безпеки особи : автореф. дис. … канд. юрид. наук : 12.00.07. Ірпінь, 2009. 21 с.

41. Дуфенюк О. М. Філософсько-правова спадщина С. Оріховського: феномен і професіоналізм правоохоронця : дис. … канд. юрид. наук : 12.00.12. Львів, 2007. 223 с.

42. Дьомін І. Адміністративно-правові засади запобігання та протидії корупції міліцією України : автореф. дис. … канд. юрид. наук : 12.00.07. Київ, 2011. 19 с.

43. 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. Київ : НАДУ, 2010. 820 с.

44. Єрменчук О. П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України : монографія. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.

45. Збукар В. П. Взаємодія органів місцевого самоврядування в стратегічному плануванні розвитку територій : дис. … канд. юрид. наук : 25.00.04. Харків, 2010. 239 с.

46. Звіт про прямі збитки інфраструктури від руйнувань внаслідок військової агресії Росії проти України станом на початок 2024 року. Київ : квітень, 2024. 39 с. URL: https://kse.ua/wp-content/uploads/2024/04/01.01.24_Damages_Report.pdf.

47. Зелінська Н. С. Механізм державного управління упорядкуванням адміністративно-територіального устрою на регіональному рівні (на прикладі південних областей України) : дис. … канд. наук з держ. упр. : 25.00.02. Одеса, 2010. 222 с.

48. Зінич Л. В. Адміністративно-правові інструменти запобігання порушенням прав інтелектуальної власності: сучасний стан та перспективи розвитку. *Нове українське право*. 2025. Вип. 2. С. 120–126.

49. Зубко А. О. Адміністративно-правові механізми в контексті впровадження адміністративної політики України: проблематика теоретичного дискурсу. *Юридичний науковий електронний журнал*. 2024. № 3. С. 296–299.

50. Інфраструктура / О. В. Савченко, В. Й. Ольшевський, І. В. Барановська, О. Н. Тетіор, І. Р. Ковалів, О. Г. Стегній, В. І. Куценко. *Енциклопедія Сучасної України* / редкол. : І. М. Дзюба, А. І. Жуковський, М. Г. Железняк та ін. ; НАН України, НТШ. Київ : Ін-т енциклопедичних досліджень НАН України, 2011. Т. 11. URL: https://esu.com.ua/article-12489.

51. Іщенко І. Адміністративно-правові інструменти Національної поліції як суб'єкта реалізації превентивної функції держави: поняття та зміст. *KELM. (Knowledge, Education, Law, Management)*. 2022. № 6 (50). С. 171–177.

52. Іщук Д. О. Адміністративно-правовий статус спеціалізованих суб'єктів протидії корупції України : дис. … д-ра юрид. наук : 12.00.07. Київ, 2021. 404 с.

53. Карабін Т. О. Співвідношення повноважень місцевих органів виконавчої влади та органів місцевого самоврядування: теоретичні і практичні питання : дис. ... канд. юрид. наук : 12.00.07. Ужгород, 2007. 204 с.

54. Кишиневський М. СБУ затримала агента рф, який шпигував за об'єктами біля Хмельницької АЕС. *ШоТам*. URL: https://shotam.info/sbu-zatrymala-ahenta-rf-iakyy-shpyhuvav-za-ob-iektamy-bilia-khmelnytskoi-aes/.

55. Кібератаки на критичну інфраструктуру: кейси і рекомендації з досвіду впровадження захисту. *АМ Інтегратор Груп.* URL: https://amintegrator.com/kiberataky-na-krytychnu-infrastrukturu-kejsy-i-rekomendacziyi-z-dosvidu-vprovadzhennya-zahystu/.

56. Кількість кібератак на рік на критичну інфраструктуру України зросла з 800 до 4500: СБУ назвала організаторів. *Мінфін*. URL: https://minfin.com.ua/ua/2024/05/07/126427603/.

57. Климчук Т. На Рівненщині СБУ викрила працівника об'єкта критичної інфраструктури на виправдовуванні війни проти України. *Суспільне.* URL: https://suspilne.media/rivne/512063-na-rivnensini-sbu-vikrila-pracivnika-obekta-kriticnoi-infrastrukturi-na-vipravdovuvanni-vijni-proti-ukraini/.

58. Кобзєва Т. А. Адміністративно-правове забезпечення управління фінансовою системою України : дис. … д-ра юрид. наук : 12.00.07. Дніпро, 2018. 428 с.

59. Коваленко Ю. О. Адміністративно-правовий механізм інформаційного забезпечення протидії корупції в правоохоронних органах України : дис. … канд. юрид. наук : 12.00.07. Київ, 2018. 239 с.

60. Колодій А. М. Принципи права України : монографія. Київ : Юрінком Інтер, 1998. 208 с.

61. Коломоєць Т. О. Адміністративне право України. Академічний курс : підручник. Київ : Юрінком Інтер, 2011. 576 с.

62. Комзюк А. Т. Заходи адміністративного примусу в правоохоронній діяльності міліції: поняття, види та організаційно-правові питання реалізації : монографія / за заг. ред. д-ра юрид. наук, проф. О. М. Бандурки. Харків : Нац. ун-т внутр. справ, 2002. 336 с.

63. Кондратенко О. Ю. Політика. *Велика українська енциклопедія*. URL: https://vue.gov.ua/Політика.

64. Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР. *Офіційний вісник України*. 2010. № 72, ч. 1. Ст. 2598.

65. Коренькова В. С. Адміністративно-правові засади координації діяльності органів виконавчої влади у сферах європейської та євроатлантичної інтеграції : дис. ... канд. юрид. наук : 12.00.07. Харків, 2021. 230 с.

66. Кохан Г. Метод оцінювання в політичній науці. *Політичний менеджмент.* 2008. № 2. С. 33–41. URL: http://nbuv.gov.ua/UJRN/PoMe_2008_2_6.

67. Кримінальний кодекс України : Закон України від 05.04.2001 р. № 2341-III. *Відомості Верховної Ради України*. 2001. № 25–26. Ст. 131.

68. Крук С. І. Методологія побудови інституційних механізмів державного управління у сфері національної безпеки. *Вчені записки Таврійського національного університету імені В. І. Вернадського*. Серія : Державне управління. 2018. Т. 29 (68), № 6. С. 8–11.

69. Кузьмічов О. Д. Адміністративно-правові інструменти забезпечення продовольчої безпеки України. *Журнал східноєвропейського права*. 2024. № 120. С. 122–128.

70. Курило С. Л. Адміністративно-правовий статус органів внутрішніх справ як суб'єкта взаємодії з органами місцевої влади з питань забезпечення громадської безпеки та громадського порядку. *Форум права.* 2012. № 1. С. 523–526.

71. Лига А. І. Правові засади державної політики у сфері захисту прав споживачів. *Juridical scientific and electronic journal*. 2023. № 8. С. 191–196.

72. Литвин О. В. Адміністративно-правове регулювання статусу державного службовця в Україні : дис. … канд. юрид. наук : 12.00.07. Ірпінь, 2009. 210 с.

73. Лукашевич В. Г. Правоохоронна діяльність органів внутрішніх справ. Вступ до спеціальності : навч. посіб. Запоріжжя : Юридичний інститут МВС України, 1998. 67 с.

74. Лютіков П. С. Державний контроль у галузі чорної металургії в Україні: організаційно-правовий аспект : дис. ... канд. юрид. наук : 12.00.07. Запоріжжя, 2009. 212 с.

75. Малиновський В. Я. Державне управління : навч. посіб. 2-ге вид., доповн. та перероб. Київ : Атіка, 2003. 576 с.

76. Махмурова-Дишлюк О. П. Поняття інструментів публічного адміністрування у сфері адміністративно-правового забезпечення прав і свобод людини і громадянина в умовах збройних конфліктів в Україні. *Науковий вісник публічного та приватного права*. 2020. Вип. 3. С. 40–45.

77. Мельник М. І., Хавронюк М. І. Правоохоронні органи та правоохоронна діяльність : навч. посіб. Київ : Атіка, 2002. 576 с.

78. Мельник Р. С., Мосьондз С. О. Адміністративне право України (у схемах та коментарях) : навч. посіб. / за ред. Р. С. Мельника 2-ге вид., перероб. і допов. Київ : Юрінком Інтер ; Буква Закону, 2018. 344 с.

79. Михайленко Д. СБУ заарештувала двох російських агентів, які картографували ключову інфраструктуру Києва. *UNITED24 Media*. URL: https://united24media.com/latest-news/ukrainian-sbu-arrests-two-russian-agents-mapping-kyivs-key-infrastructure-14197.

80. Мінекономрозвитку та СБУ створять Національний перелік об’єктів критичної інфраструктури. *Урядовий портал. Єдиний веб-портал органів виконавчої влади України.* URL: https://www.kmu.gov.ua/news/minekonomrozvitku-ta-sbu-stvoryat-nacionalnij-perelik-obyektiv-kritichnoyi-infrastrukturi.

81. Монастирецький В. Л. Адміністративно-правові інструменти захисту об’єктів критичної інфраструктури Службою безпеки України. *Право і суспільство*. 2024. № 4. С. 865–870.

82. Монастирецький В. Л. До проблеми визначення поняття критичної інфраструктури та її захисту. *Науковий вісник публічного та приватного права*. 2025. Вип. 4. С. 246–250.

83. Монастирецький В. Л. Завдання забезпечення безпеки та стійкості функціонування об’єктів критичної інфраструктури Службою безпеки України. Актуальні проблеми імплементації наукових досягнень у практичну діяльність: матеріали Міжнар. наук.-практ. конф. (Київ, 4–5 черв. 2024 р.). Київ: Наук.-дослід. ін-т публіч. права, 2024. С. 98–100.

84. Монастирецький В. Л. Місце служби безпеки України в системі суб’єктів забезпечення безпеки та стійкості функціонування об’єктів критичної інфраструктури. *KELM*. 2023. № 7 (59). С. 477–480 (Республіка Польща).

85. Монастирецький В. Л. Поняття адміністративно-правового механізму захисту об’єктів критичної інфраструктури Службою безпеки України. *Право та державне управління*. 2022. № 3. С. 505–510.

86. Монастирецький В. Л. Принципи забезпечення безпеки та стійкості функціонування об’єктів критичної інфраструктури Службою безпеки України. *Виклики сучасності та наукові підходи до їх вирішення:* матеріали Міжнар. наук.-практ. конф. (Київ, 12–13 серп. 2020 р.). Київ: Наук.-дослід. ін-т публіч. права, 2020. С. 132–134.

87. Монастирецький В. Л. Структура адміністративно-правового статусу Служби безпеки України щодо захисту об’єктів критичної інфраструктури. *Інноваційні підходи до реформування сучасного законодавства:* матеріали Міжнар. наук.-практ. конф. (Київ, 20–21 квіт. 2023 р.). Київ: Наук.-дослід. ін-т публіч. права, 2023. С. 144–146.

88. Морщенок Т. С., Біляк О. М. Огляд підходів до визначення економічної сутності поняття "ефективність". *Економічний вісник Запорізької державної інженерної академії*. 2016. Вип. 1. С. 7–13.

89. Москвич Л. М. Організаційно-правові проблеми статусу суддів : дис. … канд. юрид. наук : 12.00.10. Харків, 2003. 224 с.

90. Нижник Н. Р. Природа та зміст адміністративної реформи в України. *Реформування державного управління в Україні: проблеми і*

перспективи / кол. авт. ; наук. керівн. В. В. Цвєтков. Київ : Оріяни, 1998. 364 с.

91. Новак Н. П., Сердюк Є. В. Інструменти публічного адміністрування запобігання тінізації економіки в Україні. *Право та державне управління.* 2025. № 1. С. 290–295.

92. Новиŭ тлумачниŭ словник української мови : в 4 т. / укл. : В. Яременко, О. Сліпушенко. Київ : Аконіт, 1998. Т. 1. 941 с.

93. Олійник І. Л. Організаційно-правові засади взаємодії міліції (поліції) країн-учасниць СНД у боротьбі з правопорушеннями : дис. ... канд. юрид. наук : 12.00.07. Донецьк, 2005. 232 с.

94. Осадчий В. Правоохоронні органи як суб'єкти кримінально-правового захисту. *Право України.* 1997. № 11. С. 71–75.

95. Перепелиця А. В. Адміністративно-правове регулювання підготовки персоналу для органів внутрішніх справ України : дис. … канд. юрид. наук : 12.00.07. Львів, 2009. 272 с.

96. Петренко І. Сутність державної політики та державних цільових програм. *Віче.* 2011. № 10. С. 23–25.

97. Петрушенко В. Тлумачний словник основних філософських термінів. Львів : Нац. ун-т ".Львівська політехніка", 2009. 264 с.

98. Питання Апарату Ради національної безпеки і оборони України: указ, положення від 14.10.2005 №1446/2005. *Офіційний вісник України*. 2005. №42. Ст.2651.

99. Питання Служби безпеки України : Указ Президента України від 27.12.2005 р. № 1860/2005. *Офіційний вісник України*. 2005. № 52. Ст. 3264.

100. Пікулик О. І. Власюк Н. І. Основні підходи до оцінювання ефективності діяльності органів державного управління. *Вчені записки Таврійського національного університету імені В. І. Вернадського*. Серія : Публічне управління та адміністрування. 2023. Т. 34 (73), № 1. С. 93–100.

101. План взаємодії функціональних органів у сфері захисту критичної інфраструктури для всіх режимів функціонування критичної інфраструктури : проект наказу Міністерства розвитку громад та територій України від 2025. *Міністерство розвитку громад та територій України*. URL: https://mindev.gov.ua.

102. Платон. Держава / пер. з давньогрецьк. Київ : Орієнтир, 2017. 336 с.

103. Погорілко В. Ф., Федоренко В. Л. Конституційне право України : підручник / за заг. ред. В. Ф. Погорілка. Київ : Наукова думка ; Прецедент, 2006. 344 с.

104. Подоляка А. М. Взаємодія державних органів в охороні громадського порядку. *Форум права*. 2009. № 2. С. 338–344.

105. Попович Т. П. Поняття обов'язку як елементу правового статусу особи. *Аналітично-порівняльне правознавство*. 2023. № 6. С. 714–718.

106. Про боротьбу з тероризмом : Закон України від 20.03.2003 р. № 638-IV. *Відомості Верховної Ради України*. 2003. № 25. Ст. 180.

107. Про державний захист працівників суду і правоохоронних органів : Закон України від 23.12.1993 р. № 3781-XII. *Відомості Верховної Ради України*. 1994. № 11. Ст. 50.

108. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 р. № 3475-IV. *Відомості Верховної Ради України*. 2006. № 30. Ст. 258.

109. Про державну таємницю : Закон України від 21.01.1994 р. № 3855-XII. *Відомості Верховної Ради України*. 1994. № 16. Ст. 93.

110. Про загальну структуру і чисельність Служби безпеки України : Закон України від 20.10.2005 р. № 3014-IV. *Відомості Верховної Ради України.* 2006. № 4. Ст. 53.

111. Про затвердження Інструкції про порядок взаємодії Державної служби України з надзвичайних ситуацій і Служби безпеки України у сфері

запобігання виникненню та реагування на надзвичайні ситуації : наказ Міністерства оборони України, Служби безпеки України від 13.01.2014 р. № 24/6. *Офіційний вісник України*. 2014. № 13. Ст. 402.

112. Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури : розпорядження Кабінету Міністрів України від 19.09.2023 р. № 825-р. *Офіційний вісник України*. 2023. № 90. Ст. 5230. URL: https://zakon.rada.gov.ua/laws/show/825-2023-р#Text.

113. Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України : розпорядження Кабінету Міністрів України від 07.03.2025 р. № 204-р. *Офіційний вісник України*. 2025. № 28. Ст. 1886. URL: https://zakon.rada.gov.ua/laws/show/204-2025-р#Text.

114. Про затвердження Положення про Державну службу України з надзвичайних ситуацій : Постанова Кабінету Міністрів України від 16.12.2015 р. № 1052. Офіційний вісник України. 2015. № 102. Ст. 3514.

115. Про затвердження Положення про Міністерство внутрішніх справ України : Постанова Кабінету Міністрів України від 28.10.2015 р. № 878. *Офіційний вісник України*. 2015. № 89. Ст. 2972.

116. Про затвердження Положення про організаційно-технічну модель кіберзахисту : Постанова Кабінету Міністрів України від 29.12.2021 р. № 1426. *Офіційний вісник України*. 2022. № 4. Ст. 247.

117. Про затвердження Порядку взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності : Постанова Кабінету Міністрів України від 13.11.2025 р. №1471. *Офіційний вісник України*. 2025. № 96. Ст. 6744.

118. Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури : Постанова Кабінету Міністрів

України від 22.07.2022 р. № 821. *Офіційний вісник України*. 2022. № 60. Ст. 3599.

119. Про затвердження Регламенту обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури : Постанова Кабінету Міністрів України від 14.10.2022 р. № 1174. *Офіційний вісник України*. 2022. № 84. Ст. 2304.

120. Про затвердження форм планів захисту об'єктів критичної інфраструктури та рекомендацій з розроблення планів захисту : наказ Центрального управління Служби безпеки України від 19.01.2024 р. № 21. URL: https://moz.gov.ua/uploads/ckeditor/%D0%9A%D1%80%D0%B8%D1%82%D0%B8%D1%87%D0%BD%D0%B0%20%D1%96%D0%BD%D1%84%D1%80%D0%B0/2024/15-02-2024/%D0%BD%D0%B0%D0%BA%D0%B0%D0%B7%20%D0%A1%D0%BB%D1%83%D0%B6%D0%B1%D0%B8%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8%20%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8%20%D0%B2%D1%96%D0%B4%2019.01.2024.

121. Про Кабінет Міністрів України : Закон України від 27.02.2014 р. № 794-VII. *Відомості Верховної Ради України*. 2014. № 13. Ст. 222.

122. Про контррозвідувальну діяльність : Закон України від 26.12.2002 р. № 374-IV. *Відомості Верховної Ради України*. 2003. № 12. Ст. 89.

123. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX. *Відомості Верховної Ради України*. 2023. № 5. Ст. 13. URL: https://zakon.rada.gov.ua/laws/show/1882-20/conv#Text.

124. Про місцеве самоврядування в Україні : Закон України від 21.05.1997 р. №280/97-ВР. *Відомості Верховної Ради України*. 1997. № 24. Ст. 170.

125. Про Національний банк України : Закон України від 20.05.1999 р. № 679-XIV. *Відомості Верховної Ради України*. 1999. № 29. Ст. 238.

126. Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII. *Відомості Верховної Ради України*. 2015. № 40–41. Ст. 379.

127. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 р. № 2135-XII. *Відомості Верховної Ради України*. 1992. № 22. Ст. 303.

128. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. *Офіційний вісник України*. 2017. № 91. Ст. 2765.

129. Про правовий режим воєнного стану : Закон України від 12.05.2015 р. № 389-VIII. *Відомості Верховної Ради України.* 2015. № 28. Ст. 250.

130. Про Раду національної безпеки і оборони України : Закон України від 05.03.1998 р. № 183/98-ВР. *Відомості Верховної Ради України*. 1988. № 35. Ст. 237.

131. Про Службу безпеки України : Закон України від 25.03.1992 р. № 2229-XII. *Відомості Верховної Ради України*. 1992. № 27. Ст. 382.

132. Про схвалення Концепції створення державної системи захисту критичної інфраструктури : розпорядження Кабінету Міністрів України від 06.12.2017 р. № 1009-р. *Офіційний вісник України*. 2018. № 7. Ст. 271.

133. Про утворення Міжвідомчої комісії з питань захисту критичної інфраструктури : Постанова Кабінету Міністрів України від 15.07.2025 р. № 885. *Офіційний вісник України*. 2025. № 64. Ст. 4408. URL: https://zakon.rada.gov.ua/laws/show/885-2025-п/conv#Text.

134. Процких О. Ю. Інформаційна взаємодія національної поліції України з органами публічної влади та громадськістю. *Право і безпека*. 2015. № 4. С. 50–55.

135. Пчеліна О. В. Теоретичні засади формування та реалізації методики розслідування злочинів у сфері службової діяльності : дис. … д-ра юрид. наук : 12.00.09. Харків, 2017. 568 с.

136. Резнікова О. О., Войтовський К. Є., Лепіхов А. В. Організація системи забезпечення національної стійкості на регіональному і місцевому рівнях : аналіт. доп. / за заг. ред. О. О. Резнікової. Київ : НІСД, 2021. 140 с.

137. Романов В., Рудік О., Брус Т. Вступ до аналізу державної політики : навч. посіб. Київ : Основи, 2001. 235 с.

138. Романов М. В. Правове регулювання заходів стягнення, що застосовуються до осіб, позбавлених волі : дис. … канд. юрид. наук. : 12.00.08. Харків, 2002. 208 с.

139. Руднєва О. М. Гендерна рівність у праві України : дис. … канд. юрид. наук : 12.00.01. Харків, 2002. 178 с.

140. Рульєв В. А., Гуткевич С. О. Менеджмент : навч. посіб. Київ : Центр учбової літератури, 2011. 312 с.

141. Рябічко О. В. Державна політика регулювання підприємницької діяльності: механізми формування. *Актуальні проблеми державного управління.* 2011. № 1 (39). С. 72–76.

142. СБУ відстежує діяльність працівників об’єктів критичної інфраструктури, щоб виявити агентів РФ – Малюк. *Радіо Свобода*. URL: https://www.radiosvoboda.org/a/news-sbu-kolaboranty-krytychna-infrastruktura/32103963.html.

143. Середа О. Г., Свічкарьова Я. В. Правничі компетентності та повноваження Служби безпеки України. *Вчені записки Таврійського національного університету імені В. І. Вернадського*. Серія : Юридичні науки. 2024. Т. 35 (74), № 3. С. 118–122.

144. Сірко В. С. Поняття та елементи механізму адміністративно-правового забезпечення волонтерської діяльності в Україні. *Юридичний науковий електронний журнал*. 2018. № 4. С. 109–112.

145. Скрипнюк В. М. Правоохоронна діяльність у системі органів державної влади. *Вісник Одеського інституту внутрішніх справ*. 2001. № 1. С. 8–16.

146. Сліпенюк В. В., Клименко А. С. Удосконалення кадрового забезпечення СБУ в контексті реалізації політики національної безпеки України. *Ефективність державного управління* : зб. наук. пр. 2023. Вип. 1–2 (74–75). С. 75–80.

147. Словник української мови : в 11 т. / редкол.: І. К. Білодід (голова) та ін. ; АН Української РСР ; Ін-т мовознав. ім. О. О. Потебні. Київ : Наук. думка, 1972. Т. 3 : З / ред. тому : Г. М. Гнатюк, Т. К. Черторизька. 744 с.

148. Снігур І. Й. Механізм реалізації права громадян на участь у здійсненні державної влади : дис. … канд. юрид. наук : 12.00.01. Київ, 2007. 225 с.

149. Соф'їна М. І. До проблеми визначення поняття механізму адміністративно-правового регулювання здійснення фіскальної політики в Україні. *Юридичний бюлетень*. 2018. Вип. 8. С. 258–264.

150. Спільно з СБУ Академія визначатиме об'єкти критичної інфраструктури у сфері охорони здоров'я. *Національна академія медичних наук.* URL: https://amnu.gov.ua/spilno-z-sbu-akademiya-vyznachatyme-obyekty-krytychnoyi-infrastruktury-v-sferi-ohorony-zdorovya/.

151. Суд, правоохоронні та правозахисні органи України : підручник / відп. ред. В. Маляренко. Київ : Юрінком Інтер, 2004. 376 с.

152. Сукманова О. В. Публічне адміністрування охорони права власності в Україні : дис. … д-ра юрид. наук : 12.00.07. Київ, 2019. 559 с.

153. Тарахонич Т. І. Механізм дії права, механізм правового регулювання, механізм реалізації права: особливості взаємодії. *Держава і право* : зб. наук. праць. Юридичні і політичні науки. 2010. Вип. 50. С. 12–18.

154. Теленик С. Правовий зміст поняття «критична інфраструктура». *NATIONAL LAW JOURNAL: TEORY AND PRACTICE*. 2019. DECEMBRIE. С. 34–38.

155. Тиндик Н. П. Адміністративно-правовий механізм регулювання міграції в Україні : автореф. дис. … д-ра юрид. наук : 12.00.07. Ірпінь, 2009. 47 с.

156. Топчій В. В. Взаємодія та координація в діяльності органів внутрішніх справ з виявлення та розкриття злочинів. *Науковий вісник Ужгородського національного університету*. Серія : Право. 2015. Вип. 30, т. 2. С. 165–169.

157. Трушкіна Н. В. Теоретичні аспекти стратегування розвитку критичної інфраструктури в умовах зовнішніх загроз. *Economic journal Odessa polytechnic university*. 2024. № 4 (30). С. 144–148. URL: https://economics.net.ua/ejopu/2024/No4/127.pdf.

158. Тюріна О. Правоохоронні органи: питання теоретичного осмислення та нормативного визначення. *Право України*. 2001. № 5. С. 79–80.

159. Управління СБ України у Дніпропетровській області. *Facebook*. URL: https://www.facebook.com/ssu.dnipro/posts/%D1%81%D0%B1%D1%83-%D0%BF%D1%80%D0%BE%D0%B2%D0%B5%D0%BB%D0%B0-%D1%83-%D0%B4%D0%BD%D1%96%D0%BF%D1%80%D1%96-%D1%82%D1%80%D0%B5%D0%BD%D1%96%D0%BD%D0%B3-%D1%96%D0%B7-%D0%BF%D1%80%D0%BE%D1%82%D0%B8%D0%B4%D1%96%D1%97-%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0%D0%BC-%D0%BD%D0%B0-%D0%BE%D0%B1%D1%94%D0%BA%D1%82%D0%B8-%D0%BA%D1%80%D0%B8%D1%82%D0%B8%D1%87%D0%BD%D0%BE%D1%97-%D1%96%D0%BD%D1%84%D1%80%D0%B0%D1%81%D1%82/757000123286782

160. Уряднікова І. В., Заплатинський В. М. Наукові підходи до визначення терміну «критична інфраструктура». *Вісті Донецького гірничого інституту*. 2020. № 2 (47). С. 184–193.

161. Фелик О. В. Сутність інструментів публічного адміністрування в Україні. *Право і суспільство*. 2024. № 4. С. 44–50.

162. Філософський енциклопедичний словник / редкол.: В. І. Шинкарук (голова) та ін. ; НАН України ; Ін-т філософії імені Г. С. Сковороди. Київ : Абрис, 2002. VI, 742 с.

163. Франчук В. І., Пригунов П. Я., Мельник С. І. Безпека об’єктів критичної інфраструктури в Україні: організаційно-нормативні проблеми та підходи. *Соціально-правові студії*. 2021. Вип. 3 (13). С. 142–148.

164. Фулей Т. І. Сучасні загальнолюдські принципи права та проблеми їх впровадження в Україні : автореф. дис. … канд. юрид. наук : 12.00.01. Київ, 2003. 24 с.

165. Хасанова В. В. Державне регулювання внутрішньої торгівлі в Україні (організаційно-правовий аспект) : дис. ... канд. юрид. наук : 12.00.07. Київ, 2009. 202 с.

166. Хміль І. В. Адміністративно-правовий механізм міжнародного співробітництва у сфері забезпечення Національної безпеки : дис. … канд. юрид. наук : 12.00.07. Київ, 2024. 224 с.

167. Цвєтков М. Ю. Регіоналізація транспортного обслуговування сфери обігу в ринкових умовах : дис. … канд. екон. наук : 08.00.05. Київ, 2009. 208 с.

168. Чепкова К. О. Поняття та види інструментів публічного адміністрування у сфері захисту прав дітей під час збройного конфлікту. Публічне право № 2 (58). 2025. URL: https://www.publichne-pravo.com.ua/files/58/7.pdf

169. Чумак В. В. Адміністративно-правові засади діяльності поліції Грузії, країн Балтії та України: порівняльний аналіз : монографія. Харків : Константа, 2019. 490 с.

170. Шевченко В. М. Поняття та ознаки адміністративно-правових інструментів здійснення превентивної діяльності Національною поліцією України. *Актуальні проблеми вітчизняної юриспруденції*. 2023. № 6. С. 148–153.

171. Широкун К. Планував знеструмити Харків: СБУ затримала російського диверсанта. *РБК-Україна.* URL: https://www.rbc.ua/rus/news/planuvav-znestrumiti-harkiv-sbu-zatrimala-1752137082.html.

172. Шморгун Л. Г. Менеджмент організацій : навч. посіб. Київ : Знання, 2010. 462 с.

173. Шумейко Т. А. Поняття та ознаки адміністративно-правового механізму формування та реалізації державної політики у сфері обігу зброї в Україні. *Юридична наука*. 2020. № 8 (110). С. 169–176.

174. Щербак Н. В. Стратегічне планування в системі державного управління. *Державне управління та місцеве самоврядування*. 2020. Вип. 3 (46). С. 52–60.

175. Юридична енциклопедія : в 6 т. / редкол. : Ю. С. Шемшученко (голова редкол.) та ін. Київ : Укр. енцикл., 1998. Т. 1 : А – Г. 656 с.

176. Юридичний словник / за ред. Б. М. Бабія, Ф. Г. Бурчака, В. М. Корецького, В. В. Цвєткова. Київ : Голов. ред. Української Радянської енциклопедії, 1983. 872 с.

177. Critical infrastructure resilience at EU-level. URL: https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en.

178. Monastyretskyi V. Definition of the administrative and legal status of the security service of Ukraine with regard to the protection of critical infrastructure facilities. *Entrepreneurship, Economy and Law*. 2024. № 4. P. 33–37.

179. UNESCO Thesaurus: Social status in UNESDOC. *ЮНЕСКО.* URL: https://vocabularies.unesco.org/browser/thesaurus/en/page/?uri=http://vocabularies.unesco.org/thesaurus/concept6181.

180. Weber M. Politik als Beruf. Stuttgart : Philipp Reclam, 1992. 96 p.

ДОДАТКИ

Додаток А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Монастирецький В. Л. Поняття адміністративно-правового механізму захисту об’єктів критичної інфраструктури Службою безпеки України. *Право та державне управління*. 2022. № 3. С. 505–510.

2. Монастирецький В. Л. Місце служби безпеки України в системі суб’єктів забезпечення безпеки та стійкості функціонування об’єктів критичної інфраструктури. *KELM*. 2023. № 7 (59). С. 477–480 (Республіка Польща).

3. Монастирецький В. Л. Адміністративно-правові інструменти захисту об’єктів критичної інфраструктури службою безпеки України. *Право і суспільство*. 2024. № 4. С. 865–870.

4. Monastyretskyi V. Definition of the administrative and legal status of the security service of Ukraine with regard to the protection of critical infrastructure facilities. *Entrepreneurship, Economy and Law*. 2024. № 4. P. 33–37.

5. Монастирецький В. Л. До проблеми визначення поняття критичної інфраструктури та її захисту. *Науковий вісник публічного та приватного права*. 2025. Вип. 4. С. 246–250.

які засвідчують апробацію матеріалів дисертації:

6. Монастирецький В. Л. Принципи забезпечення безпеки та стійкості функціонування об’єктів критичної інфраструктури Службою безпеки України. *Виклики сучасності та наукові підходи до їх вирішення*: матеріали Міжнар. наук.-практ. конф. (Київ, 12–13 серп. 2020 р.). Київ: Наук.-дослід. ін-т публіч. права, 2020. С. 132–134.

7. Монастирецький В. Л. Структура адміністративно-правового статусу Служби безпеки України щодо захисту об’єктів критичної інфраструктури.

Інноваційні підходи до реформування сучасного законодавства: матеріали Міжнар. наук.-практ. конф. (Київ, 20–21 квіт. 2023 р.). Київ: Наук.-дослід. ін-т публіч. права, 2023. С. 144–146.

8. Монастирецький В. Л. Завдання забезпечення безпеки та стійкості функціонування об’єктів критичної інфраструктури Службою безпеки України. *Актуальні проблеми імплементації наукових досягнень у практичну діяльність*: матеріали Міжнар. наук.-практ. конф. (Київ, 4–5 черв. 2024 р.). Київ: Наук.-дослід. ін-т публіч. права, 2024. С. 98–100.