ПОЛІТОЛОГІЯ

УДК: 351.342.352/354.1

РОЛЬ ПУБЛІЧНОГО УПРАВЛІННЯ У ФОРМУВАННІ НАЦІОНАЛЬНОЇ КІБЕРБЕЗПЕКИ: МЕХАНІЗМИ КООРДИНАЦІЇ ТА КОНТРОЛЮ

К. Ф. Іщенко, К. А. Швець

Анотація. У статті здійснено дослідження ролі публічного управління у забезпеченні національної кібербезпеки з акцентом на механізми координації та контролю. Проаналізовано основні етапи формування системи кібербезпеки, зокрема розроблення нормативно-правового забезпечення, координацію діяльності державних органів та значення міжнародного співробітництва. Окреслено необхідність інтеграції органів державної влади, безпекових структур та приватного сектору для забезпечення комплексного підходу до протидії кіберзагрозам. Розглянуто ключові інструменти моніторингу та реагування на кіберінциденти, а також аспекти захисту критичної інформаційної інфраструктури. У висновках обґрунтовано доцільність удосконалення нормативно-правових механізмів та посилення міжнародної співпраці задля підвищення ефективності боротьби з кіберзлочинністю та кібертероризмом.

Ключові слова: публічне управління, національна кібербезпека, механізми координації, контроль, кіберзагрози.

Вступ. Із розвитком цифрових технологій і глобалізацією інформаційного простору кібербезпека стає однією з найбільш актуальних проблем для держав на всіх рівнях. Від ефективності управлінських структур у цій сфері залежить безпека державних інтересів, захист економічних, політичних і соціальних структур від кіберзагроз, а також стабільність національної безпеки. Оскільки кіберзагрози мають глобальний характер, у зв'язку з чим можливість їх нейтралізації та запобігання потребує комплексного підходу, у цьому випадку роль публічного управління в забезпеченні національної кібербезпеки є критично важливою. Проте незважаючи на численні розробки в цій галузі, наявність специфічних викликів у сфері координації державних та приватних організацій, а також міждержавного співробітництва, залишається актуальним питанням.

Забезпечення національної кібербезпеки є частиною більш широких завдань національної безпеки, зокрема в аспектах стратегічної оборони, економічної стабільності, захисту критичної інфраструктури, збереження приватності громадян та державних секретів. Це також включає забезпечення безпечної кіберінфраструктури, розробку нормативно-правових актів, взаємодію між державними структурами і приватними компаніями, а також підготовку кадрів.

Протягом останніх десятиліть кібербезпека стала предметом численних наукових і практичних досліджень, які висвітлюють різні аспекти цієї проблеми. Окремі дослідження зосереджені на правових аспектах кібербезпеки, інші – на технічних інноваціях для захисту інформаційних систем. Серед важливих наукових праць можна відзначити роботи з міжнародної співпраці у сфері кібербезпеки, як-от праці міжнародних організацій (НАТО, ЄС), а також національних дослідних інститутів. Прикладом є праці дослідницьких центрів (RAND Corporation, Carnegie Endowment for International Peace, Brookings Institution, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Європейська стратегія кібербезпеки (EU Cybersecurity Strategy)) тощо. Дослідження кіберполітики та нормативного регулювання у галузі кіберзахисту вказують на необхідність зміцнення публічно-приватного партнерства та спільних зусиль для розвитку адаптивних і інноваційних механізмів для боротьби з новими кіберзагрозами.

Один із найбільш невирішених аспектів, якому приділяється мало уваги в наявних дослідженнях, – це саме координація міждержавного співробітництва в області кібербезпеки. Відсутність єдиного підходу до реагування на транснаціональні кіберзагрози часто створює прогалини в міжурядовій взаємодії. Важливою проблемою є також відсутність узгоджених механізмів на рівні публічного управління для забезпечення ефективного контролю та моніторингу в реальному часі. До того ж питання інтеграції нових технологій та управлінських інновацій у стратегії кібербезпеки ще не отримали достатньої уваги.

Метою цієї статті є дослідження ролі публічного управління у формуванні національної кібербезпеки, зокрема механізмів координації та контролю, а також на основі аналізу сучасних наукових досліджень і практичного досвіду розробка рекомендацій щодо удосконалення наявних механізмів для підвищення ефективності державної політики у сфері кібербезпеки.

Основна частина. Україна часто ставала мішенню кібератак, особливо з боку російських хакерських груп. Яскравим прикладом є кібератака на енергосистему у 2015–2016 рр., коли у грудні 2015 р. хакери атакували три енергетичні компанії: «Прикарпаттяобленерго», «Чернівціобленерго» і «Київобленерго». Внаслідок цього 230 000 людей в Івано-Франківській області залишилися без електропостачання на кілька годин. У 2016 р. подібна атака вивела з ладу підстанцію «Північна» в Києві. Також не менш шкідливим стала атака NotPetya у 2017 р. Ця шкідлива програма поширювалася через українське бухгалтерське ПЗ M.E.Doc. Вона паралізувала роботу урядових органів, банків, компаній, включно з «Укрпоштою» та «Ощадбанком». Загальні збитки оцінюються в мільярди доларів.

Перед вторгненням Російської Федерації (січень 2022 р.) хакери атакували десятки державних сайтів, залишивши повідомлення «Бійтеся і чекайте гіршого». Внаслідок цього була тимчасово порушена робота «Дії» та інших сервісів. У 2022–2023 рр. українські урядові сайти та банки зазнавали масованих DDoS-атак з боку російських хакерських угруповань. 19 грудня 2024 р. відбулася масштабна кібератака на державні реєстри України, зокрема на сайти Національних інформаційних систем (НАІС) та Міністерства юстиції. Ця атака призвела до тимчасового призупинення роботи Єдиних Державних реєстрів, що вплинуло на надання адміністративних послуг громадянам.

За даними Державної служби спеціального зв'язку та захисту інформації України, кількість кіберінцидентів у 2024 р. зросла на 69,8 %, порівняно з 2023 р. За статистикою, у 2023 р. зафіксовано 2 541 кіберінцидент, у 2024 р. – 4 315 випадків.

Основними цілями хакерів стали місцеві органи влади, урядові організації, сектор безпеки та оборони, енергетичний сектор, комерційні організації та телекомунікації. Серед найпоширеніших типів атак було розповсюдження шкідливого програмного забезпечення, фішинг, компрометація облікових записів. Основна мета – викрадення чутливої інформації та знищення даних.

Забезпечення національної кібербезпеки потребує комплексного підходу та взаємодії різних органів державної влади, правоохоронних структур, приватного сектору, а також міжнародної спільноти. Тому роль публічного управління в цій сфері полягає в ефективній організації та координації дій на всіх рівнях управління, що забезпечує максимальний рівень безпеки інформаційної інфраструктури держави [1, с. 248].

Публічне управління відіграє ключову роль у формуванні та реалізації національних стратегій кібербезпеки, забезпечуючи їх ефективне впровадження, моніторинг та адаптацію до динамічних загроз кіберпростору. Важливим аспектом цієї діяльності є координація взаємодії між органами державної влади, приватним сектором та міжнародними партнерами, що сприяє створенню комплексної та стійкої системи кібербезпеки. У цьому контексті механізми координації та контролю є визначальними для ефективного функціонування національної кібербезпекової політики [2, с. 298]. Основні аспекти цієї ролі включають:

1. Публічне управління має створювати та впроваджувати стратегії кібербезпеки, що визначають пріоритети, цілі та механізми захисту критичної інфраструктури та національних інтересів. Важливим завданням цих стратегій є їх адаптація до динамічного технологічного середовища та еволюції кіберзагроз, що забезпечує гнучкість і стійкість національної системи кібербезпеки.

2. Національна кібербезпека потребує тісної співпраці між різними урядовими структурами, як-от Міністерство цифрової трансформації, Міністерство оборони, органи безпеки, правоохоронні органи та інші. Ключовим є створення міжвідомчих робочих груп, комітетів або спеціальних агентств для координації дій у сфері кібербезпеки.

3. Державні органи повинні мати можливості для моніторингу кіберпростору, виявлення загроз і атак у реальному часі, а також оцінки рівня готовності та реагування на інциденти. Це

включає в себе контроль за критичною інфраструктурою та забезпечення її захисту від потенційних кіберзагроз.

4. Публічне управління повинно забезпечувати належне законодавче забезпечення кібербезпеки, створюючи правові норми для захисту персональних даних, боротьби з кіберзлочинністю, а також для регулювання діяльності у сфері кібербезпеки. Закони та нормативно-правові акти повинні регулярно оновлюватися з урахуванням нових кіберзагроз та тенденцій.

5. З огляду на глобальний характер кіберзагроз, публічне управління повинно забезпечувати активну взаємодію з міжнародними партнерами, зокрема Європейським Союзом, НАТО, ООН та урядами інших держав. Ця взаємодія охоплює участь у міжнародних ініціативах, спрямованих на обмін інформацією, координацію зусиль у сфері протидії кіберзлочинності та розроблення спільних механізмів реагування на транснаціональні кіберзагрози, що сприяє зміцненню глобальної кіберстійкості.

6. Публічне управління також повинно стимулювати партнерство з приватним сектором, оскільки значна частина критичної інфраструктури знаходиться у приватній власності. Механізми координації між державою та бізнесом повинні включати в себе надання рекомендацій щодо стандартів кібербезпеки, а також взаємодію в разі кіберінцидентів.

7. Державні органи повинні інвестувати в освіту та підвищення кваліфікації кадрів у сфері кібербезпеки. Це включає підготовку фахівців для державних структур, а також для приватного сектору. Залучення освітніх установ до розвитку спеціалізованих програм і курсів має сприяти підвищенню загального рівня кіберграмотності в суспільстві.

8. У разі кіберінцидентів публічне управління повинно мати чіткі плани реагування, в тому числі щодо відновлення функціонування критичної інфраструктури, розслідування кіберзлочинів і мінімізації збитків. Створення спеціалізованих центрів реагування на кіберінциденти (CERT) є важливим елементом національної стратегії [3, с. 218].

Законодавчі та нормативні основи кібербезпеки є одним з основних механізмів формування національної кібербезпеки. Публічне управління повинно створювати чітку правову основу для функціонування системи кібербезпеки, що включає розробку та впровадження законів, стандартів і процедур для захисту інформаційних систем [1, с. 248; 4, с. 176]. В Україні такими документами є Закон України «Про основні засади забезпечення кібербезпеки України» (2017), який визначає правові та організаційні основи захисту життєво важливих інтересів людини, суспільства та держави у кіберпросторі, а також встановлює основні цілі, напрями та принципи державної політики у сфері кібербезпеки. Постанова КМУ № 518 від 19 червня 2019 р. «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» встановлює загальні вимоги до кіберзахисту об'єктів критичної інфраструктури [15]. Також Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» встановлює правові засади захисту інформації в інформаційно-телекомунікаційних системах та визначає обов'язки суб'єктів у цій сфері [16]. Також Стратегія кібербезпеки України 2021–2025 роки окреслює напрями розвитку та модернізації кіберзахисту в Україні [3, с. 201; 5, с. 208].

У 2025 р. Україна продовжила вдосконалювати нормативно-правову базу у цій сфері. Наприклад, 25 лютого 2025 р. були офіційно прийняті зміни Постановою № 24 «Про затвердження Змін до деяких нормативно-правових актів Національного банку України з питань інформаційної безпеки та кіберзахисту». Основні нововведення включали інформування про зміни в організації інформаційної безпеки. Тобто банки зобов'язані повідомляти НБУ про істотні зміни в організації інформаційної безпеки та кіберзахисту, як-от призначення або звільнення керівника інформаційної безпеки (CISO), зміни в структурі підрозділів, відповідальних за кіберзахист, або впровадження нових продуктів, що впливають на інформаційну безпеку. Таке інформування має здійснюватися протягом п'яти робочих днів з моменту впровадження змін. Ще однією зміною є вдосконалення процедури звітування. Ці заходи спрямовані на підвищення стійкості банківської системи України до кіберзагроз та забезпечення надійного захисту інформаційних ресурсів фінансових установ.

Для забезпечення ефективної роботи системи кібербезпеки необхідна координація діяльності різних органів державної влади. В Україні таким органом є Національний координацій-

ний центр кібербезпеки, який об'єднує зусилля державних установ, силових відомств і приватних компаній для оперативного реагування на кіберзагрози [2, с. 289; 6, с. 178]. Важливою частиною цієї роботи є інтеграція з міжнародними організаціями, зокрема з Європейським Союзом і НАТО, для обміну інформацією та кращими практиками в галузі кібербезпеки [4, с. 167; 7, с. 187].

Часті кібернапади, зокрема на енергетичну мережу, стали основою для вдосконалення механізмів кіберзахисту та посилення координації між органами державної влади та приватним сектором. 5 жовтня 2015 р. в межах Міністерства внутрішніх справ було створено підрозділ Кіберполіції України (МВС). Цей підрозділ розслідує кіберзлочини, зокрема фішинг, шахрайство та DDoS-атаки, та взаємодіє з міжнародними партнерами для боротьби з кіберзагрозами [12; 13].

Одним з основних завдань публічного управління є впровадження механізмів моніторингу та контролю за виконанням заходів з кібербезпеки. Це включає регулярні аудити безпеки інформаційних систем, перевірки дотримання вимог щодо захисту персональних даних, проведення тестів на вразливість критичної інфраструктури. Також важливим є створення CERT-UA (Команди реагування на комп'ютерні надзвичайні події), яка входить до складу Держспецзв'язку. Команда здійснює моніторинг і аналіз кібератак, реагує на кіберінциденти та координує їх розслідування, а також працює з міжнародними партнерами для захисту державних ресурсів.

Також важливо згадати про стратегічне управління Ради національної безпеки і оборони України (РНБО), яка визначає державну політику у сфері кібербезпеки, координує взаємодію між державними органами та приватним сектором та розробляє і впроваджує Стратегію кібербезпеки України. Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку) відповідає за технічний кіберзахист державних інформаційних ресурсів, розробляє стандарти та політики у сфері кіберзахисту, а також контролює дотримання норм безпеки в державному секторі. Служба безпеки України (СБУ) виявляє та запобігає кіберзагрозам, пов'язаним із національною безпекою, протидіє кібератакам з боку іноземних спецслужб і хакерських угруповань. Міністерство цифрової трансформації України (Мінцифра) розвиває цифрову інфраструктуру та стандарти кібербезпеки, відповідає за проєкт «Дія» та захист персональних даних громадян.

Критична інформаційна інфраструктура є основою функціонування держави, економіки та безпеки [9]. Публічне управління забезпечує її захист через встановлення вимог до захисту інформаційних систем, розробку стандартів безпеки, сертифікацію та впровадження заходів щодо забезпечення стійкості цих систем до кібератак [10].

У відповідь на зростання кіберзагроз український ринок кібербезпеки зріс у 4 рази за останні 8 років, досягнувши $138 млн у 2024 р. Очікується, що протягом наступних п'яти років ринок зросте ще на 50 %, досягнувши $209 млн. Україна впровадила низку механізмів для координації та контролю кібербезпеки, що охоплюють державний, військовий і приватний сектори.

Кіберзагрози не мають кордонів, тому важливим аспектом є міжнародна співпраця у цій сфері. Публічне управління повинно активно співпрацювати з міжнародними організаціями, зокрема з ЄС, НАТО, Інтерполом та іншими, для обміну інформацією, розробки спільних стандартів безпеки та координації дій у боротьбі з кіберзлочинністю [14, с. 870].

Україна співпрацює з ЄС, НАТО, США, Великою Британією та іншими країнами для посилення кібербезпеки, отримує технічну та фінансову підтримку для зміцнення кіберзахисту критичної інфраструктури.

Висновки. Публічне управління відіграє центральну роль у забезпеченні національної кібербезпеки, сприяючи ефективній реалізації комплексних заходів, спрямованих на захист державних та приватних інтересів у цифровому середовищі. Важливими складниками цього процесу є впровадження механізмів координації між державними органами, моніторинг і контроль кіберпростору, розроблення та вдосконалення нормативно-правової бази, міжнародна співпраця, а також налагодження партнерства з приватним сектором. Узгоджене функціонування цих

механізмів є необхідною умовою для забезпечення стійкості та безпеки національної інформаційної інфраструктури, що сприяє зміцненню державної стабільності, сталому розвитку та оперативному реагуванню на новітні кіберзагрози.

З огляду на зростаючі кіберзагрози Україна активно розвиває механізми координації та контролю у сфері кібербезпеки, впроваджуючи міжнародні стандарти та сучасні технології для захисту інформаційного простору. Водночас зберігається нагальна потреба у вдосконаленні законодавчих і нормативних механізмів, підвищенні рівня підготовки фахівців, а також у посиленні міжнародної співпраці задля підвищення ефективності протидії кіберзлочинності та кібертероризму.

Abstract. The article examines the role of public governance in ensuring national cybersecurity, with a focus on coordination and control mechanisms. The key stages of cybersecurity system development are analyzed, including the establishment of a regulatory framework, interagency coordination, and the significance of international cooperation. The necessity of integrating governmental institutions, security agencies, and the private sector to ensure a comprehensive approach to countering cyber threats is emphasized. Key monitoring and incident response tools, as well as aspects of critical information infrastructure protection, are considered. The conclusions substantiate the need for continuous improvement of regulatory mechanisms and the strengthening of international cooperation to enhance the effectiveness of combating cybercrime and cyberterrorism.

Keywords: public administration, national cybersecurity, coordination mechanisms, control, cyber threats.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кузьмін В. В. Кібербезпека України: виклики, загрози та шляхи. Київ: Національний університет оборони України, 2017. 250 с.

2. Мельник О. В. Публічне управління в сфері кібербезпеки: теоретичні засади та практичні аспекти. Київ: Інститут публічного управління, 2019. 300 с.

3. Радченко О. І. Захист критичної інформаційної інфраструктури: міжнародний досвід та українські реалії. Київ: Юрінком Інтер, 2020. 220 с.

4. Бондаренко М. І. Кіберзагрози в національній безпеці та роль державних органів у їх нейтралізації. Харків: ХНУВС, 2018. 180 с.

5. Григор'єв С. М. Аналіз сучасних підходів до організації національної кібербезпеки в умовах цифрової трансформації. Львів: ЛНУ ім. Івана Франка, 2021. 210 с.

6. Ковальчук В. С. Механізми управління кібербезпекою на національному рівні: інституційний підхід. Київ: Наукова думка, 2016. 280 с.

7. Смірнов О. А. Роль міжнародних організацій у забезпеченні кібербезпеки. Київ: Видавничий дім «Київська Русь», 2020. 190 с.

8. Міністерство цифрової трансформації України. Стратегії кібербезпеки України: національний план дій. Київ, 2020. URL: https://www.cyber.gov.ua (дата звернення: 08.03.2025).

9. World Economic Forum. Global Risks Report 2021. URL: https://www.weforum.org/reports/the-global-risks-report-2021

10. Закон України «Про основні засади забезпечення кібербезпеки України»: Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 08.03.2025).

11. Стратегія кібербезпеки України: Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 року № 96/2016. URL: https://www.president.gov.ua/documents/962016-19974 (дата звернення: 08.03.2025).

12. Закон України «Про захист персональних даних»: Закон України від 1 червня 2010 року № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 08.03.2025).

13. Постанова Кабінету Міністрів України «Про затвердження положення про систему управління кібербезпекою в Україні»: Постанова Кабінету Міністрів України від 28 вересня 2017 року № 1084. URL: https://zakon.rada.gov.ua/laws/show/1084-2017-%D0%BF (дата звернення: 08.03.2025).

14. Kankanhalli M. S., Xu Y. Cybersecurity and the Role of Governments: A Global Perspective. *Information Systems Research.* 2018. Vol. 29, № 4. P. 867–879.

15. Постанова Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»: Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518. Київ, 2019. URL: https://www.kmu.gov.ua/ua/npas/pro-zatverdzhennya-zagalnih-vimog-do-kibershahishtu-ob-yektiv-kritichnoyi-infrastrukturi (дата звернення: 08.03.2025).

16. Закон України «Про основні засади забезпечення кібербезпеки України»: Закон України від 5 жовтня 2017 р. № 2163-VIII. Київ, 2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 08.03.2025).