УДК: 351:004.056
JEL Classification: H83, H12, L38, O38, D83
DOI: 10.31767/nasoa.3-2026.12

М. МАМЕДОВ,
здобувач третього (освітньо-наукового) рівня вищої освіти,
Навчально-науковий інститут менеджменту та психології
ДЗВО «Університет менеджменту освіти»,
E-mail: mamedov_umo2022@ukr.net,
ORCID: 0009-0002-8079-2871

Механізми реалізації регіональної політики щодо інформаційної безпеки

У статті обґрунтовано механізм реалізації державної політики щодо інформаційної безпеки на місцевому та регіональному рівнях шляхом створення регіональних центрів кіберзахисту. Наголошено, що сучасні умови цифрової трансформації публічного управління, розвиток електронного врядування, поширення цифрових сервісів і зростання кількості кіберзагроз формують потребу у вдосконаленні наявних механізмів захисту інформаційних ресурсів територіальних громад. Особливої актуальності зазначене питання набуло в умовах повномасштабної російської агресії, коли об'єктами кібератак дедалі частіше стають органи державної влади, органи місцевого самоврядування, комунальні підприємства та інші суб'єкти критичної інформаційної інфраструктури.

Доведено, що традиційна централізована модель забезпечення кібербезпеки не завжди здатна гарантувати належний рівень оперативності реагування на локальні інциденти інформаційної безпеки, що зумовлює необхідність формування регіонального рівня координації та управління процесами кіберзахисту. Обґрунтовано, що регіональні центри кіберзахисту можуть виконувати функції моніторингу кіберзагроз, аудиту інформаційної безпеки, координації міжсекторальної взаємодії, підготовки фахівців і консультативного супроводу органів місцевого самоврядування у сфері цифрової безпеки. Найбільш ефективною організаційною основою функціонування таких центрів є механізм державно-приватного партнерства, який забезпечує поєднання управлінського потенціалу держави, технологічних ресурсів приватного сектору, науково-експертного середовища та громадських ініціатив. Запропоновано розглядати регіональні центри кіберзахисту як елемент регіональної цифрової інфраструктури та інституційний механізм реалізації місцевої політики щодо інформаційної безпеки. Зроблено висновок, що створення таких центрів сприятиме підвищенню кіберстійкості територіальних громад, розвитку системи превентивного реагування на кіберзагрози

та зміцненню інформаційної безпеки держави загалом.

Ключові слова: *інформаційна безпека, кібербезпека, регіональна політика щодо інформаційної безпеки, регіональні центри кіберзахисту, державно-приватне партнерство, цифрова трансформація, територіальні громади.*

M. MAMEDOV,
Postgraduate student,
Educational and Scientific Institute of Management and Psychology,
SIHE "University of Educational Management",
E-mail: mamedov_umo2022@ukr.net,
ORCID: 0009-0002-8079-2871

Mechanisms for Implementing the Regional Information Security Policy

The article provides a substantiation of the feasibility of establishing regional cyber defense centers as a mechanism for implementing the public policy on information security at the local and regional level. It is argued that digital transformations in the public administration, the development of e-governance, the expansion of digital services, and the growing number of cyber threats necessitate the improvement of existing mechanisms for protecting the information resources of territorial communities. This issue has become particularly relevant in the context of the full-scale Russian aggression, when public authorities, local self-government bodies, municipal enterprises, and other critical information infrastructures are increasingly becoming targets of cyberattacks.

It is demonstrated that the traditional centralized cybersecurity model is not always capable of ensuring an adequate level of responsiveness to local information security incidents, which necessitates the establishment of a regional level of coordination and control of cyber defense processes. It is substantiated that regional cyber defense centers can perform functions related to cyber threat monitoring, information security auditing, coordination of cross-sectoral cooperation, professional training, and advisory support for local self-government bodies charged with digital security. Public-private partnership is identified as the most effective organizational framework for the operation of such centers, as it enables for integrating the state's administrative capacity, the technological resources of the private sector, research and expertise, and civic initiatives. It is proposed to incorporate regional cyber defense centers in the regional digital infrastructure as an institutional mechanism for implementing the local information security policy. It is concluded that the establishment of such centers will contribute to strengthening the cyber resilience of territorial communities, enhancing preventive cyber threat response mechanisms, and improving the national information security.

Keywords: *information security, cybersecurity, regional information security policy, regional cyber defense centers, public-private partnership, digital transformation, territorial communities.*

Постановка проблеми. Сучасний етап розвитку публічного управління в Україні характеризується стрімким впровадженням цифрових технологій у діяльність органів державної влади та місцевого самоврядування. Розвиток електронного врядування, цифровізація адміністративних послуг, інтеграція інформаційних систем, використання хмарних технологій та розширення мережевої взаємодії між суб'єктами публічного управління створюють нові можливості для підвищення ефективності управлінських процесів. Але зазначені процеси супроводжуються суттєвим зростанням кількості ризиків, пов'язаних із забезпеченням інформаційної безпеки та захистом цифрової інфраструктури.

Особливої актуальності ця проблематика набула в умовах повномасштабної російської агресії проти України. Поряд із воєнними діями відбувались кібератаки на державні інформаційні ресурси, об'єкти критичної інфраструктури, інструменти електронного врядування, інформаційно-комунікаційні мережі та цифрові сервіси, які забезпечують функціонування органів публічної влади. У сучасних умовах кіберпростір став одним із ключових середовищ політичного протиборства, де поряд із традиційними воєнними засобами активно використовуються інструменти інформаційного впливу, дезінформації, OSINT-розвідки та дестабілізації систем управління. Саме тому забезпечення інформаційної безпеки дедалі більше розглядається не лише як технологічне завдання, а як важливий напрям державної безпекової політики та невід'ємна складова національної безпеки держави [1].

Важливою особливістю сучасного етапу цифрової трансформації є те, що значна частина інформаційних ресурсів і цифрових сервісів функціонує безпосередньо на місцевому рівні. Органи місцевого самоврядування, комунальні підприємства, заклади освіти, охорони здоров'я та інші суб'єкти місцевого публічного управління використовують електронний документообіг, інформаційні системи обліку, реєстри, цифрові платформи взаємодії з населенням та інші електронні сервіси. Відповідно зростає потреба у забезпеченні належного рівня їх кіберзахисту та стійкості до зовнішніх і внутрішніх загроз.

Проте практика свідчить про суттєві відмінності в рівні цифрової готовності територіальних громад України. Значна кількість органів місцевого самоврядування не має достатнього кадрового потенціалу для забезпечення належного рівня інформаційної безпеки. Іншими проблемами є дефіцит кваліфікованих фахівців з кібербезпеки, недостатнє фінансування заходів із захисту інформації, відсутність системного моніторингу кіберзагроз та обмежені можливості оперативного реагування на кіберінциденти. У результаті виникає ситуація, коли рівень захищеності цифрової інфраструктури окремих територіальних громад України значною мірою залежить від наявних ресурсів конкретного органу місцевого самоврядування, що створює нерівномірність у забезпеченні інформаційної безпеки на регіональному рівні.

Досвід функціонування сучасних систем кібербезпеки свідчить, що моделі централізованого управління не завжди забезпечують достатній

рівень оперативності реагування на локальні загрози. Сучасні підходи до кібербезпекового врядування дедалі частіше орієнтуються на багаторівневу систему взаємодії, яка передбачає розподіл функцій між національними, регіональними та локальними суб'єктами забезпечення інформаційної безпеки [2]. Такий підхід дає змогу враховувати специфіку окремих територій, особливості функціонування місцевої цифрової інфраструктури та забезпечувати ефективнішу координацію заходів кіберзахисту.

Дослідники також наголошують, що ефективність функціонування систем інформаційної безпеки значною мірою залежить від рівня організації взаємодії між державними структурами, приватним сектором та іншими учасниками цифрового середовища [3]. Це пов'язано з тим, що значна частина технологічних рішень, програмного забезпечення, засобів кіберзахисту та експертного потенціалу зосереджена саме у приватному секторі. Тому забезпечення стійкості цифрової інфраструктури потребує не лише адміністративних механізмів державного регулювання, а й створення ефективних моделей партнерської взаємодії між усіма суб'єктами забезпечення інформаційної безпеки.

Одним із перспективних напрямів вирішення зазначеної проблеми може стати створення регіональних центрів кіберзахисту, діяльність яких буде спрямована на забезпечення координації заходів інформаційної безпеки на місцевому та регіональному рівнях. Такі центри можуть ставати платформами взаємодії органів державної влади, органів місцевого самоврядування, приватних ІТ-компаній, наукових установ і громадських організацій. Їх функціонування здатне забезпечити формування єдиного середовища моніторингу кіберзагроз, проведення аудитів інформаційної безпеки, консультативну підтримку територіальних громад, підготовку профільних спеціалістів і координацію реагування на кіберінциденти.

Практичні передумови для реалізації подібного підходу вже простежуються у діяльності окремих регіональних цифрових інституцій, які поєднують функції цифрового розвитку, координації процесів цифрової трансформації та підтримки інформаційної безпеки [4, 5]. Але сьогодні відсутнє комплексне наукове обґрунтування механізмів інтеграції регіональних центрів кіберзахисту до системи реалізації державної політики щодо інформаційної безпеки, недостатньо дослідженими залишаються питання їхнього інституційного статусу, функціонального наповнення, організаційної структури та взаємодії із суб'єктами публічного управління.

У зв'язку з цим виникає необхідність наукового обґрунтування доцільності створення регіональних центрів кіберзахисту як складника механізму реалізації регіональної політики щодо інформаційної безпеки, яка сприятиме посиленню кіберстійкості територіальних громад, удосконаленню міжсекторальної взаємодії та формуванню ефективної системи реагування на сучасні інформаційні та кіберзагрози.

Аналіз досліджень і публікацій. Тематика, пов'язана із забезпеченням інформаційної безпеки та кібербезпеки в сучасних умовах перебуває у центрі уваги як вітчизняних, так і зарубіжних науковців.

Особливої актуальності вона набула в умовах цифрової трансформації публічного управління, розвитку електронного врядування та зростання кількості кіберзагроз для державних інформаційних ресурсів і критичної інфраструктури.

Теоретико-методологічні основи інформаційної безпеки держави досліджує В. Шемчук, який підкреслює її зростаюче значення як одного з ключових чинників забезпечення стійкості держави до сучасних воєнних та гібридних загроз [1]. Аналогічної позиції дотримуються S. Flowerday та T. Tuyikeze, які обґрунтовують необхідність переходу від традиційного розуміння інформаційної безпеки до комплексної системи кібербезпеки, здатної забезпечити захист цифрового середовища загалом [2]. Окремі аспекти взаємозв'язку інформаційної та національної безпеки висвітлено Т. Перун [3]. Питання управління кібербезпекою в умовах розвитку цифрових екосистем розкриті M. Kamariotou, F. Kitsios, які акцентують увагу на необхідності інтеграції організаційних, технологічних та управлінських механізмів захисту цифрової інфраструктури [4]. Теоретичні засади цифрового врядування у сфері забезпечення кібербезпеки на засадах державно-приватного партнерства розробляли M. J. G. van Eeten, J. A. de Bruijn, M. Kars, H. G. van der Voort, Van J. Till, які запропонували концептуальний підхід до багаторівневого управління кібербезпекою із залученням державних органів, приватного сектору та інших зацікавлених сторін [5].

Однак проведений аналіз наукових джерел свідчить, що питання формування регіональних центрів кіберзахисту як окремого механізму реалізації регіональної політики щодо інформаційної безпеки досліджено недостатньо. Особливо це стосується проблематики організаційного забезпечення їхньої діяльності, використання механізмів державно-приватного партнерства та інтеграції таких центрів до системи публічного управління на місцевому та регіональному рівнях.

Мета статті – обґрунтувати механізми реалізації регіональної політики щодо інформаційної безпеки шляхом створення регіональних центрів кіберзахисту як інституційного інструменту координації діяльності суб'єктів публічного управління, приватного сектору, наукових установ та громадянського суспільства; розкрити функціональне призначення та організаційні засади діяльності регіональних центрів кіберзахисту, а також їхню роль у формуванні стійкої системи кіберзахисту на місцевому та регіональному рівнях.

Результати дослідження. У сучасних умовах інформаційна безпека перестає бути суто технічним напрямом діяльності, пов'язаним із комплексним захистом інформаційних систем або окремих інформаційних ресурсів. Вона поступово перетворюється на важливий елемент державної політики, що безпосередньо впливає на стійкість функціонування органів влади, захист національних інтересів і здатність держави забезпечувати належний рівень управлінської ефективності в умовах зовнішніх і внутрішніх загроз.

Розвиток місцевого самоврядування та розширення повноважень

територіальних громад в Україні суттєво змінили характер реалізації державної політики щодо інформаційної безпеки. Значна частина інформаційних ресурсів, цифрових сервісів та управлінських процесів сьогодні функціонує саме на місцевому рівні. Це зумовлює необхідність формування нових організаційних механізмів, здатних забезпечити належний рівень захисту інформаційного середовища не лише на загальнодержавному, а й на регіональному рівні. У зв'язку з цим виникає потреба у створенні інституцій, які поєднуватимуть функції моніторингу кіберзагроз, інформаційно-аналітичного супроводу, координації взаємодії між суб'єктами кібербезпеки та практичної підтримки органів місцевого самоврядування [6].

На нашу думку, саме регіональний рівень є найбільш придатним для реалізації таких функцій. З одного боку, він забезпечує достатню близькість до територіальних громад і дає змогу враховувати специфіку функціонування місцевої цифрової інфраструктури, з іншого – створює можливість для концентрації фінансових, кадрових і технологічних ресурсів, які часто є недоступними для окремих громад. Саме тому доцільним видається формування регіональних центрів кіберзахисту (РЦКЗ) як спеціалізованих інституцій, покликаних забезпечити реалізацію регіональної політики щодо інформаційної безпеки [7].

Необхідність розвитку подібних механізмів підтверджується сучасними науковими дослідженнями державно-приватного партнерства та інформаційної безпеки. С. Воробйов і К. Гамкрелідзе наголошують, що забезпечення інформаційної безпеки сучасних цифрових платформ потребує поєднання організаційних, управлінських і технологічних інструментів, а також активного залучення приватного сектору до процесів створення та підтримки безпечного цифрового середовища [8]. Цей висновок має особливе значення для місцевого рівня управління, оскільки більшість територіальних громад не володіє достатніми ресурсами для самостійного формування комплексної системи кіберзахисту.

Одним із базових принципів функціонування регіональних центрів кіберзахисту має стати державно-приватне партнерство. У межах такої моделі органи державної влади та місцевого самоврядування забезпечують нормативно-правову, організаційну та координаційну складову діяльності центру, а приватний сектор бере участь у впровадженні технологічних рішень, проведенні аудитів інформаційної безпеки, розробленні програмних продуктів і підготовці спеціалістів [9]. До цієї взаємодії можна залучати заклади вищої освіти, наукові установи та громадські організації, що сприятиме формуванню комплексної екосистеми регіональної кіберстійкості.

Слід зазначити, що ефективність функціонування РЦКЗ значною мірою залежатиме від правильного визначення їхнього місця у структурі публічного управління. РЦКЗ не повинні дублювати повноваження національних суб'єктів забезпечення кібербезпеки або підміняти діяльність спеціально уповноважених державних органів. Натомість їхню діяльність доцільно спрямовувати на виконання координаційних, консультаційних, аналітичних і сервісних функцій, які забезпечуватимуть реалізацію державної

політики безпосередньо на регіональному рівні [10]. За такого підходу РЦКЗ може ставати своєрідним посередником між загальнодержавною системою кібербезпеки та місцевими суб'єктами цифрової взаємодії.

Особливого значення у цьому контексті набуває формування єдиного регіонального середовища обміну інформацією про кіберзагрози та кіберінциденти. Практика свідчить, що однією з основних проблем забезпечення інформаційної безпеки є фрагментарність інформації про потенційні загрози та відсутність оперативного механізму її поширення серед суб'єктів, які потребують відповідних даних. Наявність РЦКЗ забезпечить постійний моніторинг кіберпростору, накопичення інформації про загрози та своєчасне інформування органів місцевого самоврядування щодо необхідних заходів реагування.

Крім того, важливим напрямом діяльності РЦКЗ має стати оцінювання рівня інформаційної безпеки територіальних громад. Йдеться про проведення регулярних аудитів інформаційних систем, аналіз вразливостей цифрової інфраструктури, оцінювання ризиків і підготовку рекомендацій щодо підвищення рівня кіберзахисту. Реалізація зазначених функцій дасть змогу перейти від переважно реактивної моделі реагування на кіберінциденти до превентивної моделі управління інформаційною безпекою, що відповідає сучасним підходам до забезпечення кіберстійкості публічного сектору. Саме формування такої системи превентивного управління ризиками створює підґрунтя для подальшого розвитку регіональної політики щодо інформаційної безпеки та потребує більш детального розгляду організаційних і функціональних механізмів діяльності РЦКЗ.

Подальший розвиток концепції РЦКЗ потребує визначення їх функціонального наповнення та місця у системі реалізації регіональної політики щодо інформаційної безпеки. У сучасних умовах регіональна політика дедалі більше орієнтується на створення стійких механізмів управління ризиками, пов'язаними з цифровою трансформацією суспільства. Відповідно до цього забезпечення інформаційної безпеки слід розглядати не як окремий напрям діяльності спеціалізованих підрозділів, а як комплексну управлінську функцію, інтегровану до процесів стратегічного планування, цифрового розвитку та організації публічного управління на місцевому і регіональному рівнях.

У цьому контексті РЦКЗ можуть виконувати роль постійних координаційних платформ, діяльність яких спрямовується на забезпечення взаємодії між усіма суб'єктами регіональної системи інформаційної безпеки. Йдеться про формування механізму, який дасть змогу об'єднати органи місцевого самоврядування, місцеві органи виконавчої влади, комунальні підприємства, операторів цифрової інфраструктури, освітні та наукові установи, а також представників бізнесу в межах єдиного безпекового середовища. Такий підхід створює можливість для своєчасного обміну інформацією про кіберзагрози, координації заходів реагування та вироблення узгоджених управлінських рішень.

Важливо враховувати, що забезпечення інформаційної безпеки на регіональному рівні має здійснюватися відповідно до загальнодержавних

пріоритетів національної безпеки. Саме тому діяльність РЦКЗ повинна бути інтегрована до загальної архітектури державної системи кібербезпеки. У цьому аспекті особливого значення набувають напрями діяльності, визначені Радою національної безпеки і оборони України, яка розглядає захист інформаційного простору, критичної інформаційної інфраструктури та державних інформаційних ресурсів як один із ключових компонентів забезпечення національної безпеки [11]. З огляду на це РЦКЗ можуть стати інструментом практичної реалізації державних безпекових пріоритетів безпосередньо на рівні регіонів і територіальних громад.

Одним із ключових напрямів діяльності РЦКЗ має бути створення системи безперервного моніторингу кіберризиків. На відміну від традиційного підходу, який передбачає реагування вже після виникнення кіберінциденту, сучасна модель управління інформаційною безпекою орієнтується на своєчасне виявлення потенційних загроз та їх попередження. Саме тому РЦКЗ повинні забезпечувати збирання, аналіз та узагальнення інформації щодо стану захищеності цифрової інфраструктури територіальних громад, виявляти типові вразливості та формувати рекомендації щодо їх усунення. Наявність єдиного аналітичного середовища підвищить ефективність управління ризиками та рівень кіберстійкості регіону загалом.

Не менш важливою функцією РЦКЗ є організація методичної та консультаційної підтримки суб'єктів місцевого самоврядування. Практика свідчить, що значна частина територіальних громад не має достатнього досвіду у сфері організації систем інформаційної безпеки, управління ризиками та реагування на кіберінциденти. У багатьох випадках відсутні профільні структурні підрозділи або фахівці, здатні забезпечити належний рівень кіберзахисту. За таких умов РЦКЗ може стати джерелом експертної підтримки, забезпечуючи підготовку рекомендацій, проведення консультацій, організацію навчань і супровід реалізації заходів з інформаційної безпеки.

Окремого значення набуває освітня складова діяльності РЦКЗ. Сучасні кіберзагрози значною мірою пов'язані з людським фактором, помилками користувачів і недостатнім рівнем цифрової грамотності. Саме тому формування культури інформаційної безпеки повинно стати одним із пріоритетних напрямів регіональної політики кіберзахисту. Відповідні програми можуть охоплювати підвищення кваліфікації посадових осіб органів місцевого самоврядування, проведення тренінгів із цифрової гігієни, організацію тематичних навчальних заходів для працівників комунальних підприємств та інформаційно-просвітницьку роботу серед населення.

Але ефективне функціонування РЦКЗ неможливе без належного нормативно-правового забезпечення. Зараз питання інформаційної безпеки регулюються в Україні значною кількістю нормативно-правових актів, проте значна їх частина стосується загальнодержавного рівня управління. У зв'язку з цим виникає необхідність удосконалення правових механізмів, які визначатимуть статус регіональних центрів кіберзахисту, їхні повноваження, порядок взаємодії із суб'єктами забезпечення кібербезпеки та особливості функціонування в системі публічного управління. Важливе

значення у цьому процесі мають наукові напрацювання щодо правових засад забезпечення кібербезпеки та інформаційної безпеки в Україні, де акцентовано увагу на необхідності розвитку інституційних механізмів координації діяльності суб'єктів безпекової політики та вдосконалення нормативного регулювання кіберзахисту [12].

Необхідно також ураховувати, що результативність діяльності РЦКЗ значною мірою залежатиме від їхньої здатності забезпечувати міжсекторальну взаємодію. Сучасна практика свідчить, що жоден із суб'єктів інформаційної безпеки не може самостійно гарантувати повний захист цифрового середовища. Ефективна протидія кіберзагрозам потребує консолідації ресурсів, знань і компетенцій різних учасників безпекового процесу. Саме тому РЦКЗ доцільно розглядати не лише як окрему організаційну структуру, а й як інтеграційний механізм, який забезпечує узгодження інтересів і координацію дій державного сектору, бізнесу, наукової спільноти та громадянського суспільства.

Отже, функціонування РЦКЗ має ґрунтуватися на поєднанні організаційних, аналітичних, освітніх, консультативних і координаційних механізмів. Реалізація зазначених функцій створює передумови для формування цілісної регіональної системи інформаційної безпеки, здатної забезпечити належний рівень захисту цифрової інфраструктури територіальних громад. Але практична реалізація такої моделі потребує більш детального визначення інституційних умов її впровадження та оцінювання потенційних переваг створення РЦКЗ як складника сучасної системи публічного управління.

Подальше обґрунтування доцільності створення РЦКЗ потребує оцінювання їхнього потенційного впливу на забезпечення стійкості територіальних громад до сучасних інформаційних і кібернетичних загроз. У сучасних умовах інформаційна безпека дедалі більше визначає спроможність органів публічного управління забезпечувати безперервність виконання їхніх функцій, підтримувати стабільність суспільних процесів і гарантувати належний рівень захисту інформаційних ресурсів. Особливого значення це набуває в умовах воєнного стану, коли інформаційний простір стає об'єктом системного впливу з боку держави-агресора, а кібератаки використовуються як інструмент дестабілізації функціонування державних інституцій та місцевих систем управління.

Дослідження сучасних безпекових викликів свідчать, що інформаційна безпека сьогодні виходить далеко за межі суто технічного захисту інформаційних систем. Вона охоплює широкий комплекс організаційних, правових, управлінських і соціальних заходів, спрямованих на забезпечення захищеності інформаційного середовища держави та суспільства. Зазначений підхід дає змогу розглядати РЦКЗ не лише як технічні структури, орієнтовані на реагування на кіберінциденти, а й як повноцінні елементи регіональної безпекової політики.

У цьому контексті важливим завданням РЦКЗ має стати формування механізмів забезпечення цифрової стійкості територіальних громад. На відміну від традиційного підходу, який орієнтується переважно на

усунення наслідків кібератак, сучасна концепція кіберстійкості передбачає здатність системи функціонувати навіть за умов виникнення безпекових інцидентів, швидко адаптуватися до нових загроз та відновлювати працездатність після кризових ситуацій. Саме тому діяльність РЦКЗ доцільно спрямовувати на створення комплексної системи управління ризиками, що включатиме моніторинг загроз, оцінювання вразливостей, планування заходів реагування та розроблення механізмів відновлення функціонування цифрових сервісів.

Важливою перевагою запропонованої моделі є можливість концентрації експертного потенціалу на регіональному рівні. Практика функціонування органів місцевого самоврядування свідчить, що далеко не кожна територіальна громада має можливість утримувати власний підрозділ кібербезпеки або залучати висококваліфікованих спеціалістів у цій сфері. Але РЦКЗ може забезпечувати відповідну підтримку одразу для значної кількості громад, формуючи спільний кадровий, аналітичний та технологічний ресурс. Це підвищить ефективність використання фінансових ресурсів і рівень захищеності інформаційних систем незалежно від економічних можливостей окремої громади.

Окрему увагу доцільно приділити питанню інтеграції РЦКЗ до процесів цифрового врядування. Цифрова трансформація публічного сектору супроводжується постійним розширенням кількості електронних сервісів, інформаційних платформ та автоматизованих систем управління. Відповідно зростає потреба у формуванні єдиних підходів до забезпечення інформаційної безпеки таких систем. Наявність РЦКЗ створює можливість для впровадження стандартизованих процедур оцінювання ризиків, проведення аудитів інформаційної безпеки та координації заходів із захисту цифрової інфраструктури на території відповідного регіону.

Крім того, важливим напрямом діяльності РЦКЗ може стати забезпечення взаємодії між різними рівнями публічного управління. Сучасна система забезпечення інформаційної безпеки характеризується значною кількістю суб'єктів, повноваження яких часто перетинаються або потребують додаткової координації. За таких умов РЦКЗ може виконувати функцію координаційного вузла, який забезпечуватиме обмін інформацією між державними органами, місцевим самоврядуванням, спеціалізованими безпековими структурами та іншими учасниками цифрового середовища. Це сприятиме підвищенню оперативності реагування на кіберзагрози та формуванню єдиного безпекового простору.

Перспективність запропонованого підходу підтверджується і сучасними науковими дослідженнями, де кібербезпека розглядається як невід'ємна складова системи національної безпеки. У [13] наголошено, що розвиток сучасних цифрових технологій зумовлює необхідність постійного вдосконалення механізмів захисту інформаційного простору та створення нових інституційних форм забезпечення кібербезпеки, здатних адаптуватися до динамічного характеру сучасних загроз. У цьому контексті РЦКЗ можна розглядати як один із перспективних напрямів модернізації системи забезпечення інформаційної безпеки.

Отже, створення РЦКЗ відповідає сучасним тенденціям розвитку публічного управління, цифрового врядування та безпекової політики держави. Їх функціонування здатне забезпечити підвищення рівня координації суб'єктів інформаційної безпеки, посилення кіберстійкості територіальних громад, розвиток механізмів державно-приватного партнерства та формування ефективної системи управління кіберризиками на місцевому і регіональному рівнях. Запропонована модель створює передумови для переходу від переважно реактивного реагування на кіберзагрози до системного та превентивного управління інформаційною безпекою, що є необхідною умовою забезпечення стійкого функціонування цифрової держави в умовах сучасних викликів і загроз.

Висновки. Цифровізація публічного сектору супроводжується суттєвим розширенням кількості інформаційних ресурсів, електронних сервісів та інформаційно-комунікаційних систем, які використовуються органами державної влади, органами місцевого самоврядування, комунальними підприємствами та іншими суб'єктами публічного управління. За таких умов питання забезпечення інформаційної безпеки набуває комплексного характеру та виходить за межі суто технічного захисту інформаційних систем. Інформаційна безпека стає важливим елементом державної політики, безпосередньо пов'язаним із забезпеченням стійкості управлінських процесів, безперервності функціонування цифрової інфраструктури та захистом національних інтересів держави.

Однією з ключових проблем сучасної системи забезпечення інформаційної безпеки залишається обмежена спроможність окремих територіальних громад самостійно організовувати комплексний кіберзахист власних інформаційних ресурсів. Нерівномірний рівень цифрової готовності громад, дефіцит кваліфікованих кадрів і фінансових ресурсів, відсутність спеціалізованих організаційних структур суттєво ускладнюють реалізацію ефективної політики інформаційної безпеки на місцевому рівні. За таких умов виникає потреба у створенні проміжної координаційної ланки між загальнодержавною системою кібербезпеки та місцевими суб'єктами цифрової взаємодії.

Регіональні центри кіберзахисту (РЦКЗ) можуть виконувати функцію такої координаційної ланки, забезпечуючи інтеграцію організаційних, аналітичних, технологічних, освітніх і консультативних механізмів реалізації політики інформаційної безпеки. Запропонований підхід дає змогу сформувати єдине регіональне середовище управління ризиками, у межах якого здійснюватиметься моніторинг кіберзагроз, проведення аудитів інформаційної безпеки, оцінювання вразливостей цифрової інфраструктури, інформаційно-аналітичний супровід діяльності органів місцевого самоврядування та координація реагування на кіберінциденти.

Організаційною основою функціонування РЦКЗ може стати механізм державно-приватного партнерства. Поєднання управлінського потенціалу державних інституцій, технологічних можливостей приватного сектору, науково-експертного середовища та громадських ініціатив створює передумови для формування більш гнучкої та ефективної системи

забезпечення інформаційної безпеки. Така модель дає змогу не лише залучати додаткові фінансові та технологічні ресурси, а й забезпечувати постійне оновлення інструментів кіберзахисту відповідно до динамічного характеру сучасних загроз.

Основними функціональними напрямами діяльності РЦКЗ мають стати організація системи моніторингу кіберзагроз, забезпечення інформаційного обміну між суб'єктами кібербезпеки, оцінювання ризиків інформаційної безпеки, консультативний супровід органів місцевого самоврядування, організація навчальних заходів у сфері цифрової грамотності та кібергігієни, а також координація міжсекторальної взаємодіїу захисті інформаційного простору. Реалізація зазначених функцій сприятиме формуванню регіональної системи кіберстійкості, орієнтованої не лише на реагування на інциденти, а й на їх попередження.

Створення РЦКЗ уможливлює перехід від переважно реактивної моделі забезпечення інформаційної безпеки до превентивної моделі управління ризиками. Такий підхід передбачає систематичне виявлення потенційних загроз, оцінювання рівня захищеності цифрової інфраструктури, прогнозування можливих ризиків і завчасне впровадження заходів з їх мінімізації. Він сприятиме посиленню стійкості територіальних громад до зовнішніх і внутрішніх кіберзагроз, забезпеченню безперервності функціонування цифрових сервісів і зниженню ймовірності виникнення критичних інцидентів інформаційної безпеки.

Отже, створення РЦКЗ доцільно розглядати як перспективний напрям удосконалення механізмів реалізації регіональної політики щодо інформаційної безпеки. Запропонована модель забезпечує поєднання управлінських, організаційних, технологічних та освітніх інструментів у межах єдиної системи регіональної цифрової стійкості, сприяє підвищенню ефективності міжсекторальної взаємодії та формує додаткові можливості для зміцнення кібербезпеки територіальних громад. Напрямом подальших наукових досліджень є розроблення організаційно-правового механізму функціонування РЦКЗ, визначення моделей їх фінансування, а також формування єдиних стандартів їх взаємодії із загальнодержавною системою забезпечення інформаційної безпеки та цифрового врядування.

Список використаних джерел

1. Шемчук В. Механізм забезпечення інформаційної безпеки держави: теоретично-методологічні основи. *Філософські та методологічні проблеми права*. 2019. № 1 (17). С. 51–59. DOI: 10.33270/01191702.51
2. Flowerday S. V., Tuyikeze T. Information security policy development and implementation: The what, how and who. *Computers &Security*. 2016. No. 61. P. 169–183. DOI: 10.1016/j.cose.2016.06.002
3. Перун Т. С. Структурні чинники механізму інформаційної безпеки держави. *Юридичний вісник*. 2020. № 4. С. 117–124. DOI: 10.32837/yuv.v0i4.1980
4. Kamariotou M., Kitsios F. Information Systems Strategy and Security Policy: A Conceptual Framework. *Electronics*. 2023. Vol. 12. No. 2. Article number 382. DOI: 10.3390/electronics12020382
5. Van Eeten M. J. G., de Bruijn J. A., Kars M., van der Voort H. G., Van J. Till. The governance of cybersecurity: A framework for policy. *International Journal of Critical Infrastructures*. 2006. Vol. 2. No. 4. P. 357–378.
6. Central Ukrainian Digital Office. URL: https://digitaloffice.kr.ua
7. Центральноукраїнський центр кіберзахисту. URL: https://cyber.digitaloffice.kr.ua

8. Воробйов С. В., Гамкрелідзе К.Ю. Безпековий аспект державно-приватного партнерства у сфері охорони довкілля: забезпечення інформаційної безпеки ГІС та мобільних застосунків. *Стратегія економічного розвитку України*. 2025. № 57. С. 197–213. DOI: 10.33111/sedu.2025.57.197.213
9. Streltsov L. The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments. *European Journal for Security Research*. 2017. No. 2. P. 147–184. DOI: 10.1007/s41125-017-0020-x
10. Melaku H. M. A Dynamic and Adaptive Cybersecurity Governance Framework. *Journal of Cybersecurity and Privacy*. 2023. Vol. 3. No. 3. P. 327–350. DOI: 10.3390/jcp3030017
11. Україна зміцнює регіональну кіберстійкість. Рада національної безпеки і оборони України. 15.05.2026. URL: https://www.rnbo.gov.ua/ua/Diialnist/7566.html
12. Крушеніцький В. С. Органи публічної влади як суб'єкти формування та реалізації політики національної безпеки в інформаційному просторі. *Наукові записки. Серія: Право*. 2024. № 17. С. 252–256. DOI: 10.36550/2522-9230-2024-17-252-256
13. Антюхов Р. В. Державна політика у сфері інформаційної безпеки України. Національний університет «Києво-Могилянська академія». Київ, 2021. 89 с. URL: https://ekmair.ukma.edu.ua/server/api/core/bitstreams/5992e656-6ee1-4074-9bff-645ebc6f77a5/content

References

1. Shemchuk, V. (2019). Osoblyvosti zabezpechennia informatsiinoi bezpeky v umovakh rosiisko-ukrainskoi viiny [Mechanism of Providing Information Security of the State: Theoretical-Methodological Basis]. *Filosofski ta metodolohichni problemy prava – Philosophical and Methodological Problems of Law*, *1 (17)*, 51–59. DOI: 10.33270/01191702.51 [in Ukrainian].
2. Flowerday, S. V., &Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security*, *61*, 169–183. DOI: 10.1016/j.cose.2016.06.002
3. Perun, T. S. (2020). Strukturni chynnyky mekhanizmu informatsiinoi bezpeky derzhavy [Structural factors of the state information security mechanism]. *Yurydychnyi visnyk – Law Herald*, *4*, 117–124. DOI: 10.32837/yuv.v0i4.1980 [in Ukrainian].
4. Kamariotou, M., & Kitsios, F. (2023). Information Systems Strategy and Security Policy: A Conceptual Framework. *Electronics*, *12 (2)*, 382. DOI: 10.3390/electronics12020382
5. Van Eeten, M. J. G., de Bruijn, J. A., Kars, M., van der Voort, H. G., &Van J. Till (2006). The governance of cybersecurity: A framework for policy. *International Journal of Critical Infrastructures*, *2 (4)*, 357–378.
6. Central Ukrainian Digital Office. Retrieved from https://digitaloffice.kr.ua [in Ukrainian].
7. Tsentralnoukrainskyi tsentr kiberzakhystu [The Central Ukrainian Center for Cyber Protection]. Retrieved from https://cyber.digitaloffice.kr.ua [in Ukrainian].
8. Vorobiov, S. V., & Hamkrelidze, K. Yu. (2025). Bezpekovyi aspekt derzhavno-pryvatnoho partnerstva u sferi okhorony dovkillia: zabezpechennia informatsiinoi bezpeky HIS ta mobilnykh zastosunkiv [Security aspects of public-private partnerships in the field of environmental protection: Ensuring the information security of GIS and mobile APP]. *Stratehiia ekonomichnoho rozvytku Ukrainy – Strategy of Economic Development of Ukraine*, *57*, 197–213. DOI: 10.33111/sedu.2025.57.197.213 [in Ukrainian].
9. Streltsov, L. (2017). The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments. *European Journal for Security Research*, *2*, 147–184. DOI 10.1007/s41125-017-0020-x
10. Melaku, H. M. (2023). A Dynamic and Adaptive Cybersecurity Governance Framework. *Journal of Cybersecurity and Privacy*, *3 (3)*, 327–350. DOI: 10.3390/jcp3030017
11. National Security and Defense Council of Ukraine (2026). Ukraina zmitsniuie rehionalnu kiberstiikist [Ukraine is enhancing the regional cyber resilience]. Retrieved from https://www.rnbo.gov.ua/ua/Diialnist/7566.html [in Ukrainian].
12. Krushenitskyi, V. S. (2024). Orhany publichnoi vlady yak subiekty formuvannia ta realizatsii polityky natsionalnoi bezpeky v informatsiinomu prostori [Public authority bodies as entities of forming and implementing national security policy in the information space]. *Naukovi zapysky. Seriia: Pravo – Scientific Notes. Series: Law*, *17*, 252–256. DOI: 10.36550/2522-9230-2024-17-252-256 [in Ukrainian].
13. Antiukhov, R. V. (2021). *Derzhavna polityka u sferi informatsiinoi bezpeky Ukrainy [The Public policy on information security in Ukraine]*. National University of Kyiv Mohyla Academy. Kyiv [in Ukrainian].

Надійшла до редакції / Received on: 30.06.2026
Прорецензована / Reviewed on: 08.07.2026
Підписана до друку / Signed for printing on: 28.08.2026
Оприлюднена / Published on: 31.08.2026

Цитування:

Мамедов М. Механізми реалізації регіональної політики щодо інформаційної безпеки. *Науковий вісник Національної академії статистики, обліку та аудиту: зб. наук. праць.* 2026. № 3. С. 146–159. DOI: 10.31767/nasoa.3-2026.12

Cite this article:

Mamedov, M. (2026). Mekhanizmy realizatsii rehionalnoi polityky shchodo informatsiinoi bezpeky [Mechanisms for Implementing the Regional Information Security Policy]. *Naukovyi visnyk Natsionalnoi akademii statystyky, obliku ta audytu – Scientific Bulletin of the National Academy of Statistics, Accounting and Audit*, 3, 146–159. DOI: 10.31767/nasoa.3-2026.12[in Ukrainian].