УДК 35.077

Ю. М. Дзюрах,
доктор філософії за спеціальністю публічне управління та адміністрування, доцент,
доцент кафедри адміністративного та фінансового менеджменту,
Національний університет "Львівська політехніка"
ORCID ID: https://orcid.org/0000-0001-7131-7468
Р. І. Кукляк,
аспірант кафедри адміністративного та фінансового менеджменту,
Національний університет "Львівська політехніка"
ORCID ID: https://orcid.org/0009-0008-1541-6179

DOI: 10.32702/2306-6814.2026.9.535

ОЦІНЮВАННЯ КІБЕРБЕЗПЕКОВОЇ СПРОМОЖНОСТІ ГРОМАД: ЕМПІРИЧНИЙ АНАЛІЗ ТА УПРАВЛІНСЬКІ ОБМЕЖЕННЯ

Yu. Dziurakh,
Doctor of Philosophy in Public Management and Administration, Associate Professor,
Associate Professor of the Department of Administrative and Financial Management, Lviv Polytechnic National University
R. Kukliak,
PhD Student of the Department of Administrative and Financial Management, Lviv Polytechnic National University

ASSESSMENT OF CYBERSECURITY CAPACITY OF COMMUNITIES: EMPIRICAL ANALYSIS AND MANAGERIAL CONSTRAINTS

У статті досліджено кібербезпекову спроможність органів місцевого самоврядування як ключову інфраструктурну умову забезпечення результативності публічного управління інформаційною безпекою на локальному рівні. Обгрунтовано, що рівень кіберзахисту визначає стабільність інформаційних потоків, безперервність управлінських процесів та здатність громад протидіяти сучасним кіберзагрозам. Встановлено, що кібербезпекова складова виступає системоутворюючим елементом цифрової трансформації публічного управління.

Проаналізовано підходи до оцінювання кібербезпекової спроможності на місцевому рівні та виявлено їх фрагментарний характер, що проявляється у домінуванні окремих технічних показників без урахування управлінських, організаційних та кадрових аспектів. Встановлено, що відсутність комплексного підходу до оцінювання обмежує можливості формування обгрунтованих управлінських рішень у сфері кібербезпеки.

Розроблено методичний підхід до оцінювання кібербезпекової спроможності громад, який передбачає використання системи індикаторів, що охоплюють профілактичні та реактивні компоненти, зокрема управління доступом, резервне копіювання, моніторинг загроз, процедури реагування та підготовку персоналу. Запропоновано розрахунок часткового індексу кібербезпекової спроможності на основі нормування показників та їх агрегування, що забезпечує можливість комплексної оцінки рівня готовності громад до кіберзагроз. Емпіричні результати свідчать про наявність диспропорції між формалізацією політик кібербезпеки та реальною операційною готовністю органів місцевого самоврядування, що зумовлює обмежену ефективність існуючих механізмів захисту. Визначено, що ключовими управлінськими обмеженнями є недостатня інституціоналізація функції кібербезпеки, нечітке розмежування відповідальності та низький рівень інтеграції кібербезпеки у систему стратегічного управління.

Обгрунтовано практичну значущість запропонованого підходу, що полягає у можливості його використання для підвищення рівня кібербезпекової спроможності громад, удосконалення управлінських рішень та формування превентивної моделі управління кіберризиками. Визначено перспективи подальших досліджень, пов'язані з розвитком інтегральних моделей оцінювання та їх впровадженням у систему стратегічного планування діяльності органів місцевого самоврядування.

The article examines the cybersecurity capacity of local self-government bodies as a key infrastructural condition for ensuring the effectiveness of public administration in the field of information security at the local level. It is substantiated that the level of cybersecurity determines the stability of information flows, the continuity of managerial processes, and the ability of communities to withstand modern cyber threats. It is established that the cybersecurity component acts as a system-forming element of the digital transformation of public governance.

Existing approaches to assessing cybersecurity capacity at the local level are analyzed, and their fragmented nature is identified, manifested in the dominance of individual technical indicators without considering managerial, organizational, and human resource aspects. It is determined that the absence of a comprehensive assessment approach limits the ability to develop well-grounded managerial decisions in the field of cybersecurity.

A methodological approach to assessing the cybersecurity capacity of communities is developed, which involves the use of a system of indicators covering both preventive and reactive components, including access management, data backup, threat monitoring, incident response procedures, and staff training. The calculation of a partial cybersecurity capacity index based on the normalization and aggregation of indicators is proposed, ensuring a comprehensive evaluation of communities' preparedness for cyber threats.

It is proven that empirical results indicate a discrepancy between the formalization of cybersecurity policies and the actual operational readiness of local self-government bodies, which leads to limited effectiveness of existing protection mechanisms. It is identified that the key managerial constraints include insufficient institutionalization of the cybersecurity function, unclear distribution of responsibilities, and a low level of integration of cybersecurity into the system of strategic management.

The practical significance of the proposed approach is substantiated by its potential use to enhance the cybersecurity capacity of communities, improve managerial decision-making, and form a preventive model of cyber risk management. Prospects for further research are defined in the development of integrated assessment models and their incorporation into the strategic planning system of local self-government bodies.

Ключові слова: кібербезпека, органи місцевого самоврядування, публічне управління та адміністрування, територіальні громади, координаційний механізм, інституціоналізація, кібербезпекова спроможність, стратегічне управління, цифрова трансформація, кіберризики.

Key words: cybersecurity, local governments, public management and administration, territorial communities, coordination mechanism, institutionalization, cybersecurity capacity, strategic management, digitalization, digital transformation, cyber risks.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Сучасний етап цифрової трансформації публічного управління супроводжується зростанням залежності органів місцевого самоврядування від інформаційно-комунікаційних систем, що актуалізує питання забезпечення належного рівня кібербезпекової спроможності на локальному рівні. Умови гібридних загроз, активізація кібератак та ускладнення цифрової інфраструктури громад формують нові вимоги до організації процесів захисту інформації, безперервності управлінських функцій і стійкості інформаційних потоків. За таких обставин кібербезпека набуває ознак не лише технічної, але й управлінської категорії, інтегрованої у систему публічного управління.

Водночас практика функціонування органів місцевого самоврядування свідчить про наявність системних обмежень, пов'язаних із фрагментарною інституціона-

лізацією функції кібербезпеки, відсутністю комплексних підходів до її оцінювання та недостатньою інтеграцією у стратегічне управління. Наявні механізми кіберзахисту часто мають декларативний характер, не забезпечують належного рівня координації дій, чіткого розмежування відповідальності та своєчасного реагування на кіберінциденти, що знижує загальну результативність публічного управління інформаційною безпекою.

Особливої актуальності набуває проблема формування науково обгрунтованих підходів до оцінювання кібербезпекової спроможності громад, які б враховували не лише технічні параметри, але й управлінські, організаційні та кадрові аспекти. Відсутність інтегрованих методик оцінювання ускладнює ідентифікацію вразливих зон, обмежує можливості порівняльного аналізу та стримує розроблення ефективних управлінських рішень у сфері кібербезпеки.

З огляду на зазначене, наукова проблема полягає у необхідності розроблення комплексного методичного підходу до оцінювання кібербезпекової спроможності органів місцевого самоврядування та виявлення управлінських обмежень, що впливають на її рівень. Практичне значення вирішення цієї проблеми полягає у створенні інструментарію для підвищення ефективності управління інформаційною безпекою на місцевому рівні, формуванні превентивної моделі управління кіберризиками та забезпеченні стійкості функціонування громад в умовах цифровізації та гібридних загроз.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ, В ЯКИХ ЗАПОЧАТКОВАНО РОЗВ'ЯЗАННЯ ДАНОЇ ПРОБЛЕМИ І НА ЯКІ СПИРАЮТЬСЯ АВТОРИ, ВИДІЛЕННЯ НЕ ВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРИМ ПРИСВЯЧУЄТЬСЯ ОЗНАЧЕНА СТАТТЯ

Кібербезпековий вимір проблематики публічного управління інформаційною безпекою на місцевому рівні поступово набуває самостійного значення у сучасному науковому дискурсі. У вітчизняних дослідженнях увага зосереджується переважно на питаннях формування державної політики кібербезпеки, інституційного забезпечення національної системи кіберзахисту, оцінювання цифрових ризиків, а також на визначенні місця кібербезпеки в архітектурі національної безпеки. Саме в такому контексті започатковано теоретико-методологічне підгрунтя для подальшого дослідження кібербезпекової спроможності органів місцевого самоврядування.

Значний внесок у розроблення проблематики публічного управління кібербезпекою здійснено у працях А. Вовк [1], де акцентовано увагу на інституційних та управлінських засадах формування системи кібербезпеки, ролі держави у координації відповідних процесів та необхідності інтеграції кібербезпекових механізмів у систему публічного управління. Зазначений підхід має принципове значення для обгрунтування того, що кібербезпека не обмежується суто технічним захистом інформаційних систем, а виступає комплексною функцією управління, що охоплює організаційні, нормативні, кадрові та координаційні аспекти.

У працях О. Заріцького та Л. Гальчинського [2] кібербезпекова проблематика розглядається крізь призму управління ризиками, оцінювання загроз та вироблення механізмів реагування в умовах цифрової трансформації. Цінність таких напрацювань полягає у посиленні аналітичного підходу до кібербезпеки, зокрема через акцент на необхідності ідентифікації вразливостей, прогнозування ризиків та побудови системи превентивного реагування. Для дослідження кібербезпекової спроможності громад цей підхід є важливим, оскільки дозволяє інтерпретувати кібербезпеку не лише як наявність окремих технічних засобів, а як здатність органу публічної влади своєчасно виявляти, оцінювати та мінімізувати кіберризики.

Роботи О. Жеребця [3] мають значення для осмислення кібербезпеки як складової інформаційної безпеки у ширшій системі державного управління. У них простежується прагнення до систематизації суб'єктів, функцій і механізмів забезпечення безпеки у цифровому середовищі, що створює концептуальну основу для подальшої деталізації ролі органів місцевого самоврядування у цій сфері. Наукова цінність відповідних підходів полягає у переході від загального розуміння кібербезпеки до її інституційного впорядкування як складової управлінської діяльності.

У свою чергу, С. Красніков [4] приділяє увагу розвитку національної системи кіберзахисту, механізмам координації та взаємодії між суб'єктами кібербезпеки. Такі дослідження мають важливе значення для обгрунтування необхідності включення локального рівня у загальнодержавну систему реагування на кіберзагрози. Вони підтверджують, що ефективність національної моделі кібербезпеки визначається не лише наявністю центральних координаційних інституцій, а й спроможністю локальних суб'єктів діяти узгоджено, вчасно передавати інформацію про інциденти та реалізовувати стандартизовані процедури реагування.

Поряд із вітчизняними науковими розробками, суттєве значення для дослідження мають міжнародні стандарти, аналітичні звіти та практичні рамки забезпечення кібербезпеки. Рамка NIST Cybersecurity Framework орієнтує на побудову цілісної системи управління кіберризиками через взаємопов'язані функції ідентифікації, захисту, виявлення, реагування та відновлення. Стандарт ISO/IEC 27001:2022 закріплює вимоги до системи управління інформаційною безпекою та акцентує увагу на формалізації політик, розподілі відповідальності, постійному моніторингу та вдосконаленні процедур. Практики ENISA спрямовані на зміцнення інституційної стійкості та формування організаційної культури кібербезпеки в органах публічної влади. Вимоги NIS2 закладають новий рівень відповідальності суб'єктів публічного сектору за кіберстійкість, управління ризиками, звітування про інциденти та забезпечення безперервності функціонування цифрової інфраструктури. Зазначені підходи створюють важливу нормативно-аналітичну базу для порівняльного аналізу та визначення тих орієнтирів, до яких має наближатися українська практика на місцевому рівні.

Окремий блок становлять зарубіжні дослідження, присвячені кібербезпеці у секторі місцевого самоврядування. Вони демонструють, що основними

викликами для муніципального рівня є обмеженість ресурсів, недостатня кадрова забезпеченість, слабка формалізація процедур реагування, фрагментарна інституціоналізація відповідальності та недостатня інтегрованість у національні системи кіберкоординації. Такі напрацювання є особливо цінними для українського контексту, оскільки дозволяють розглядати проблематику кібербезпеки громад не як ізольований технічний виклик, а як комплексну управлінську проблему, пов'язану з організаційною структурою, стратегічним плануванням, внутрішнім контролем і координаційними механізмами.

Разом із тим, аналіз наукових джерел дає підстави стверджувати, що попри наявність значної кількості праць з питань державної політики кібербезпеки, управління цифровими ризиками та розвитку національної системи кіберзахисту, низка аспектів залишається недостатньо опрацьованою. Насамперед, у більшості досліджень домінує макрорівневий підхід, у межах якого основна увага приділяється державним інституціям, загальнонаціональним стратегіям та нормативно-правовим механізмам. Локальний рівень при цьому висвітлюється фрагментарно, без належного аналізу реальної організаційної спроможності органів місцевого самоврядування забезпечувати кіберзахист у повсякденній управлінській практиці.

Недостатньо розробленим залишається і питання методичного оцінювання кібербезпекової спроможності громад. Наявні підходи або зосереджуються на технічних параметрах захисту, або розглядають кібербезпеку у загальному контексті цифровізації, не виокремлюючи її як самостійний об'єкт емпіричного аналізу. У науковій літературі бракує інтегрованих моделей оцінювання, які б поєднували профілактичні та реактивні компоненти, враховували рівень формалізації процедур, стан кадрового забезпечення, моніторингові можливості, наявність резервування, алгоритми реагування та управлінську інтегрованість кібербезпеки у систему стратегічних рішень громади.

Не вирішеною раніше частиною загальної проблеми залишається також виявлення управлінських обмежень, що знижують результативність функціонування локальних механізмів кіберзахисту. Передусім ідеться про недостатню інституціоналізацію відповідальності, нечіткість розмежування функцій між посадовими особами, відсутність формалізованих координаційних механізмів, обмежений зв'язок між технічним супроводом і стратегічним управлінням, а також слабку інтеграцію кібербезпеки в систему публічного управління інформаційною безпекою на місцевому рівні.

Отже, наявні дослідження сформували важливу теоретичну й нормативно-аналітичну основу для вивчення кібербезпекової проблематики, однак не забезпечили цілісного емпіричного бачення кібербезпекової спроможності громад як окремого об'єкта оцінювання. Саме тому означена стаття присвячується розробленню підходу до оцінювання кібербезпекової спроможності органів місцевого самоврядування, виявленню структурних і управлінських обмежень її розвитку, а також обгрунтуванню напрямів удосконалення локальних механізмів кібербезпеки у системі публічного управління інформаційною безпекою.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є обгрунтування методичного підходу до оцінювання кібербезпекової спроможності органів місцевого самоврядування та виявлення управлінських обмежень, що впливають на ефективність функціонування локальних механізмів кіберзахисту.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ З ПОВНИМ ОБГРУНТУВАННЯМ ОТРИМАНИХ НАУКОВИХ РЕЗУЛЬТАТІВ

Зростання кіберзагроз та ускладнення цифрової інфраструктури на місцевому рівні актуалізують необхідність ефективної координації кібербезпеки між органами місцевого самоврядування та національними структурами, оскільки саме від узгодженості організаційних, технологічних і кадрових компонентів залежить здатність громад протидіяти кіберризикам [5].

У межах емпіричного дослідження кібербезпековий компонент запропоновано оцінювати через п'ять ключових показників, які відображають баланс профілактики та готовності до реагування. Прешим показником пропонується оцінювати двофакторну автентифікація та контроль доступів. Наявність 2FA для службових електронних систем (електронна пошта, внутрішні портали, документообіг, адміністрування сайтів) є базовим індикатором профілактичного захисту. Показник враховує впровадження 2FA для ключових облікових записів, централізований облік доступів, періодичний перегляд прав користувачів, розмежування доступів за принципом "мінімально необхідних повноважень". Відсутність системного контролю доступів свідчить про вразливість цифрових каналів, що прямо впливає на якість комунікацій та ризик викривлення офіційної інформації.

Наступним для оцінки слід дослідити резервне копіювання та відновлюваність даних, зокрема у частині регулярного резервного копіювання (локального/віддаленого), зберігання копій поза основною інфраструктурою, періодичного тестування відновлення, формалізованої політики backup. Резервування є ключовою умовою збереження безперервності управлінських процесів у разі кібератак або технічних збоїв. За відсутності таких процедур навіть незначний інцидент може призвести до паралічу інформаційних потоків.

Іншим важливим на наш погляд показником є процедури реагування на кіберінциденти. Показник відображає не лише технічний, а й управлінський контур кібербезпеки та спрямований на оцінку наявності затвердженого алгоритму дій у разі інциденту, визначення відповідальних осіб, фіксацію та документування випадків, а також механізми інформування керівництва та взаємодії з національними структурами.

Моніторинг інцидентів та вразливостей спрямований на аналіз наявності системного журналювання подій, періодичного аудиту інформаційно-комунікаційних систем, співпраці з провайдерами безпеки, використання засобів виявлення вторгнень. Мо-

ніторинг визначає здатність органу місцевого самоврядування не лише реагувати, а й виявляти загрози на ранніх етапах. Співвіднесення з міжнародними індикаторами, отримані на локальному рівні — співставляються з міжнародними показниками кібербезпеки держави, зокрема National Cyber Security Index (NCSI), Global Cybersecurity Index (GCI) та іншими міжнародними рейтингами спроможності. Таке співвіднесення дозволяє оцінити, наскільки локальні практики узгоджуються із загальнонаціональними та міжнародними стандартами. Якщо на рівні держави декларується високий рівень кіберготовності, але на муніципальному рівні показники залишаються низькими, виникає дисбаланс між стратегічними орієнтирами та фактичною інфраструктурною спроможністю громад.

Кібербезпекова спроможність у межах дослідження трактується як інфраструктурна умова забезпечення результативності публічного управління інформаційною безпекою та формує технічний фундамент, без якого неможливо забезпечити стабільність інформаційних потоків, достовірність офіційних повідомлень, захист від зовнішнього втручання, безперервність управлінських функцій у кризових ситуаціях. Кібербезпековий модуль завершує трикомпонентну модель оцінювання, забезпечуючи повноту аналізу результативності публічного управління інформаційною безпекою на місцевому рівні.

Зібрані емпіричні дані дають можливість визначити рівень профілактичного захисту, оцінити готовність до кризових кіберситуацій і встановити, наскільки кібербезпекове середовище підтримує або обмежує здатність органів місцевого самоврядування забезпечувати інформаційну безпеку в цифровому середовищі.

Отримані результати підтверджують значущість кібербезпекового компонента як інфраструктурної умови функціонування механізмів інформаційної безпеки та формують підгрунтя для подальшого узагальнення результатів у межах інтегральної оцінки результативності публічного управління інформаційною безпекою на місцевому рівні.

Розрахунок часткового індексу кібербезпекової спроможності потребує нормування, в межах якого застосовано шкалу нормування 0-1 із трирівневою градацією відповідей (аналогічно як і для інших часткових індексів):

1 — повна наявність / системність (регулярність, формалізованість, автоматизація);

0,5 — часткова наявність / нерегулярність;

0 — відсутність або не здійснюється.

Показники агрегуються на основі зведених часток відповідей за кожною позицією (табл. 1).

На рисунку 1 представлено радарну візуалізацію розподілу відповідей громад за трирівневою шкалою нормування (1 — повна реалізація, 0,5 — часткова, 0 — відсутність) щодо семи показників кібербезпекової спроможності.

Рисунок 1 підтверджує середній рівень кібербезпекової спроможності із вираженим розривом між

Таблиця 1. Емпіричний розподіл нормованих показників кібербезпекової спроможності

Показник	Діапазон зведених даних опитування			
	1	0.5	0	середній зважений показник
1. Двофакторна автентифікація 2FA	0,29	0,44	0,27	0,510
2. Регулярність резервного копіювання	0,35	0,39	0,26	0,545
3. Політика управління доступами	0,34	0,42	0,24	0,550
4. Перегляд прав доступу	0,31	0,40	0,29	0,510
5. Технічний моніторинг загроз	0,26	0,47	0,27	0,495
6. Процедура реагування на інциденти	0,32	0,29	0,39	0,465
7. Навчання з кіберреагування	0,18	0,34	0,48	0,350

Джерело: розраховано авторами за підсумками анкетування (n = 62).

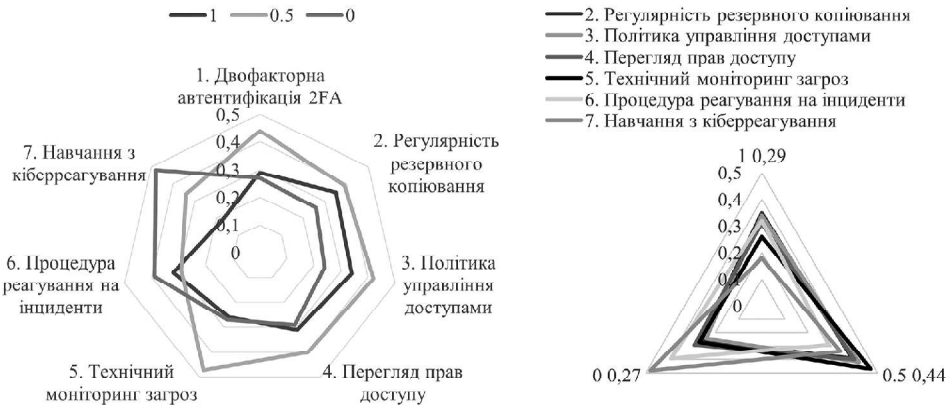

Рис. 1. Результати дослідження рівня кібербезпекової спроможності громад Львівської області

Джерело: розраховано авторами за підсумками анкетування.

формалізацією правил та реальною операційною готовністю. Саме ця диспропорція обмежує вплив кіберкомпонента на загальну результативність публічного управління інформаційною безпекою на місцевому рівні.

Частковий індекс кібербезпекової спроможності пропоновано визначати як середнє нормованих показників:

$$I_{cyber} = \frac{1}{k}\sum_{i=1}^{k} \bar{x}_i \qquad (3),$$

де $k = 7$ — кількість показників, $\bar{x}_i$ — середнє нормоване значення кожного індикатора.

Формалізована модель для розрахунку часткового індексу кібербезпекової спроможності матиме вигляд:

$$I_{cyber} = \frac{1}{k}\sum_{i=1}^{k}\left(\frac{\sum_{j=1}^{n} x_{ij}}{n}\right) \qquad (1),$$

де $x_{ij} \in \{1; 0{,}5; 0\}$, $n = 62$ — кількість громад.

$$I_{cyber} =$$

$$= \frac{0.510 + 0.545 + 0.550 + 0.510 + 0.495 + 0.465 + 0.350}{7}$$

$$I_{cyber} = \frac{3.425}{7} = 0.489$$

Отримане значення відповідає нижній межі середнього рівня спроможності, при цьому сильніші позиції відслідковуються в частині формалізації політики доступів (0.550) та регулярності резервного копіювання (0.545). Водночас вразливі зони: навчання з кіберреагування (0.350); процедура реагування (0.465); технічний моніторинг загроз (0.495).

Спостерігається характерна диспропорція: наявність регламентів управління доступами — відносно високий показник, водночас реальна готовність до інцидентів (навчання, відпрацьовані сценарії) — значно нижча, що свідчить про переважання декларативного рівня регламентації над практичним відпрацюванням, недостатню інтеграцію людського фактору в систему кіберзахисту, а також низьку культуру кіберпрофілактики.

Таким чином, кібербезпекова спроможність функціонує переважно як формально-організаційна конструкція, а не як повноцінна інфраструктурна система захисту. Кібербезпекова складова демонструє помірний рівень зрілості, однак є найбільш уразливою серед трьох модулів результативності. Саме вона створює потенційний обмежувач загального індексу результативності публічного управління інформаційною безпекою на місцевому рівні.

Результати емпіричного дослідження, проведеного серед органів місцевого самоврядування Львівської області, засвідчили, що одним із ключових чинників забезпечення кібербезпекової спроможності на локальному рівні виступає наявність локального координаційного механізму, який забезпечує організацію, управління та контроль процесів захисту інформаційних ресурсів громади. Саме організаційне закріплення функції кібербезпеки визначає ступінь керованості відповідних процесів, швидкість реагування на кіберінциденти та узгодженість управлінських дій у сфері інформаційної безпеки.

Аналіз отриманих анкетних даних показав, що в більшості досліджених громад Львівської області функція кібербезпеки вже частково інституціоналізована, однак її реалізація має фрагментарний характер. Зокрема, у значній частині органів місцевого самоврядування функції технічного адміністрування інформаційних систем покладені на спеціалістів із інформаційних технологій або працівників відповідних відділів цифрового розвитку, інформаційних технологій чи електронного врядування. Наявність таких посад створює базові передумови для формування локального координаційного механізму кібербезпеки, оскільки забезпечує відповідальну особу, яка здійснює управління інформаційною інфраструктурою.

Водночас проведене дослідження засвідчило, що у більшості громад зазначені функції не закріплені формально як функція забезпечення кібербезпеки, а реалізуються в межах загальних обов'язків із технічного супроводу інформаційних систем. Така ситуація створює управлінську невизначеність, оскільки відповідальність за кіберзахист не виділена як самостійна управлінська функція, що ускладнює координацію дій, обмежує можливості стратегічного планування та знижує рівень пріоритетності кібербезпеки у системі управлінських рішень.

Окремі органи місцевого самоврядування Львівської області вже здійснили кроки у напрямі формування більш структурованого підходу до координації кібербезпеки. У громадах із вищим рівнем цифрової спроможності функції захисту інформаційних ресурсів інтегровані у діяльність структурних підрозділів, відповідальних за цифрову трансформацію або інформаційні технології, що забезпечує централізоване управління доступом до інформаційних систем, організацію резервного копіювання, контроль інформаційних потоків та реагування на технічні інциденти. Наявність такого підходу свідчить про формування первинних елементів координаційного механізму, який забезпечує базовий рівень кібербезпекової спроможності.

Разом із тим, результати дослідження виявили низку системних недоліків, які обмежують ефективність існуючих механізмів. Насамперед, у більшості громад відсутнє чітке нормативне закріплення функції координації кібербезпеки на рівні посадових інструкцій, положень про структурні підрозділи або внутрішніх регламентів. Вищенаведене доводить, що відповідальність за кіберзахист не має формалізованого характеру, що ускладнює визначення відповідальних осіб у разі виникнення кіберінцидентів та знижує рівень управлінської відповідальності.

Другим важливим аспектом є відсутність чітко визначених зон відповідальності за окремі компоненти кібербезпеки. У багатьох випадках функції адміністрування, управління доступом, резервного копіювання та реагування на інциденти виконуються без чіткої диференціації відповідальності, що створює ризики неузгодженості управлінських дій та ускладнює реаліза-

цію системного підходу до кіберзахисту. Відсутність такого розмежування також ускладнює здійснення контролю та оцінювання ефективності відповідних заходів.

Крім того, у більшості досліджених органів місцевого самоврядування функція кібербезпеки не інтегрована у систему стратегічного управління., а розглядається переважно як технічне питання, а не як складова управлінської функції, що має стратегічне значення для забезпечення інформаційної безпеки громади. Такий підхід обмежує можливості системного управління кіберризиками та знижує здатність органів місцевого самоврядування ефективно протидіяти сучасним кіберзагрозам.

У цьому контексті ключовим напрямом удосконалення є формування повноцінного локального координаційного механізму кібербезпеки, який має передбачати формальне закріплення відповідальної посадової особи або структурного підрозділу, наділеного повноваженнями щодо організації та координації заходів кіберзахисту. Така особа повинна забезпечувати координацію дій між структурними підрозділами, здійснювати моніторинг стану інформаційної безпеки, організовувати реагування на кіберінциденти та забезпечувати впровадження відповідних процедур захисту інформації.

Важливим елементом такого механізму є чітке визначення зон відповідальності, що передбачає закріплення функцій управління доступом, резервного копіювання, адміністрування інформаційних систем, моніторингу кіберінцидентів та реагування на них за конкретними посадовими особами або структурними підрозділами. Запропоноване забезпечить підвищення керованості процесів кібербезпеки, зменшення ризику управлінських викривлень та підвищення ефективності реагування на загрози.

Не менш важливим напрямом удосконалення є інтеграція функції кібербезпеки у систему управлінських рішень органів місцевого самоврядування, що передбачає включення питань кібербезпеки до стратегічних і програмних документів громади, врахування кіберризиків при плануванні розвитку інформаційної інфраструктури, а також забезпечення системного контролю за станом інформаційної безпеки. Такий підхід дозволяє перейти від реактивної моделі реагування на кіберінциденти до превентивної моделі управління кіберризиками.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Результати дослідження засвідчили, що у органах місцевого самоврядування Львівської області вже сформовано базові передумови для створення локального координаційного механізму кібербезпеки, зокрема через наявність відповідних посад і функціональних елементів. Водночас відсутність їх формалізації, чіткого розмежування відповідальності та інтеграції функції кібербезпеки у систему управлінських рішень обмежує ефективність існуючих механізмів. Удосконалення зазначених аспектів дозволить забезпечити формування повноцінного координаційного механізму, що підвищить рівень кібербезпекової спроможності органів місцевого самоврядування та сприятиме підвищенню результативності публічного управління інформаційною безпекою на локальному рівні.

Література:

1. Вовк, А. (2024). Сучасні проблеми публічного управління забезпеченням кібербезпеки в Україні. Публічне управління: концепції, парадигма, розвиток, удосконалення, (8), 28—35. https://pa.journal.in.ua/index.php/pa/article/view/136

2. Заріцький, О., & Гальчинський, Л. (2024). Оцінка ризику кіберзагроз для об'єктів державного сектору України з метою подальшого планування інвестицій в інформаційну безпеку. Universum, (9), 349—355. https://archive.liga.science/index.php/universum/article/view/1124

3. Жеребець, О. (2025). Правове забезпечення методики ідентифікації та оцінки кіберризиків на національному рівні: сучасний досвід Словаччини та Латвії. Інформація і право, (2 (53)), 164—175. http://il.ippi.org.ua/article/view/334163

4. Красніков, С. (2025). Розвиток національної системи кібербезпеки України. Інформація і право, (4 (55)), 191-198. http://il.ippi.org.ua/article/view/346414

5. Bada M., Nurse J. R. C. Developing cybersecurity education and awareness programmes for small— and medium-sized enterprises (SMEs) // Cybersecurity. 2019. Vol. 2, № 1. URL: https://www.mdpi.com/2624-800X/5/2/19

References:

1. Vovk, A. (2024), "Modern problems of public management of cybersecurity in Ukraine", Publichne upravlinnia: kontseptsii, paradyhma, rozvytok, udoskonalennia, vol. (8), pp. 28—35, available at: https://pa.journal.in.ua/index.php/pa/article/view/136 (Accessed 10 April 2026).

2. Zaritskyi, O., & Halchynskyi, L. (2024), "Assessment of cyber threat risk for public sector facilities of Ukraine for the purpose of further planning of investments in information security", Universum, vol. (9), pp. 349—355, available at: https://archive.liga.science/index.php/universum/article/view/1124 (Accessed 10 April 2026).

3. Zherebets, O. (2025), "Legal support for the methodology for identification and assessment of cyber risks at the national level: modern experience of Slovakia and Latvia", Informatsiia i pravo, vol. 2 (53), pp. 164—175, available at: http://il.ippi.org.ua/article/view/334163 (Accessed 10 April 2026).

4. Krasnikov, S. (2025), "Development of the national cybersecurity system of Ukraine", Informatsiia i pravo, vol. 4 (55), pp. 191—198, available at: http://il.ippi.org.ua/article/view/346414 (Accessed 10 April 2026).

5. Bada, M., & Nurse, J. R. C. (2019), "Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs)", Cybersecurity, vol. 2 (1), available at: https://www.mdpi.com/2624-800X/5/2/19 (Accessed 10 April 2026).

Отримано редакцією журналу / Received: 10.04.26
Прорецензовано / Revised: 22. 04.26
Дата публікації / Published: 12.05.26