

КОМУНІКАЦІЙНА ВЗАЄМОДІЯ В СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ: ВИКЛИКИ ДЛЯ ОРГАНІВ МІСЦЕВОГО САМОВРЯДУВАННЯ

COMMUNICATION INTERACTION IN THE SYSTEM OF PUBLIC GOVERNANCE OF INFORMATION SECURITY: CHALLENGES FOR LOCAL SELF-GOVERNMENT BODIES

Досліджено особливості комунікаційної взаємодії в системі публічного управління інформаційною безпекою в діяльності органів місцевого самоврядування України. Проведено аналіз статистичних та соціологічних джерел, що засвідчують, з одного боку, глибоку інституційну недовіру до основних органів влади (центрального уряду, парламенту, суду, виборчі комісії), а з іншого – стабільну підтримку базових демократичних і національних цінностей (незалежність, демократія, єдність, державна мова, політична участь). Виявлено, що комунікаційна взаємодія у сфері інформаційної безпеки виконує не лише превентивну, а й координаційно-управлінську функцію, виступаючи індикатором адаптивності публічного управління до динаміки сучасних загроз.

Сформовано модель комунікаційної взаємодії суб'єктів публічного управління інформаційною безпекою на місцевому рівні, яка включає центральні органи виконавчої влади, органи місцевого самоврядування, громадян, локальні ЗМІ, IT-сектор, освітні установи, громадські ініціативи та національні структури кіберзахисту. Проведено візуалізацію комунікаційної моделі у форматі структурованої інфографіки та деталізовано ролі кожного суб'єкта взаємодії в умовах інформаційних загроз. Результати опитування 2024 року проілюстровано графічно: встановлено, що попри низьку довіру до інституцій, рівень суспільної підтримки демократичного устрою та політичної участі громадян залишається стабільно високим.

Сформульовано практичні рекомендації щодо підвищення прозорості, довіри та кіберстійкості в публічному управлінні. Зокрема, обґрунтовано доцільність впровадження кризових протоколів комунікації, інституціоналізації функцій кібербезпеки в структурах ОМС, розбудови цифрових механізмів зворотного зв'язку з громадянами та залучення громадських організацій до формування локальних стратегій інформаційної безпеки. Узагальнено нормативно-правові засади та пропозиції щодо вдосконалення комунікаційної взаємодії органів місцевого самоврядування в системі публічного управління інформаційною безпекою. Відображено зв'язок між запропонованими управлінськими заходами, чинною нормативно-правовою базою та конкретними змінами, які необхідно внести до законодавства України.

Результати дослідження можуть бути використані для вдосконалення місцевої інформаційної політики, актуалізації нормативного поля, а також підвищення ефективності публічної комунікації в умовах гібридної війни, суспільної вразливості та цифрової трансформації.

Ключові слова: публічне управління, інформаційна безпека, органи місцевого самоврядування, комунікаційна взаємодія, довіра, прозорість, кіберстійкість, нормативно-

правове регулювання, цифрова трансформація, інституційна відповідальність.

The study explores the features of communication interaction within the system of public governance of information security in the activities of local self-government bodies in Ukraine. An analysis of statistical and sociological sources reveals, on the one hand, deep institutional distrust toward key branches of power (central government, parliament, judiciary, electoral commissions), and on the other, consistent public support for fundamental democratic and national values (independence, democracy, unity, state language, political participation). It is determined that communication interaction in the field of information security performs not only a preventive but also a coordination and management function, serving as an indicator of the adaptability of public governance to the dynamics of modern threats.

A communication interaction model of public information security governance actors at the local level has been developed. It includes central executive authorities, local self-government bodies, citizens, local media, the IT sector, educational institutions, civic initiatives, and national cybersecurity agencies. The communication model is visualized through a structured infographic, and the roles of each interaction subject under conditions of information threats are detailed. Data from the 2024 survey are graphically illustrated, showing that despite low trust in institutions, public support for the democratic order and civic political participation remains consistently high.

Practical recommendations are formulated to enhance transparency, trust, and cyber resilience in public governance. In particular, the implementation of crisis communication protocols, institutionalization of cybersecurity functions within local governments, development of digital feedback mechanisms with citizens, and involvement of civic organizations in shaping local information security strategies are substantiated. The regulatory framework is systematized and accompanied by proposals for improving the communication interaction of local self-government bodies within the public information security governance system. The relationship is outlined between the proposed governance measures, current legal norms, and specific legislative amendments required in Ukrainian law.

The findings of this research can be used to improve local information policies, update the regulatory framework, and enhance the effectiveness of public communication under conditions of hybrid warfare, societal vulnerability, and digital transformation.

Key words: public governance, information security, local self-government bodies, communication interaction, trust, transparency, cyber resilience, regulatory framework, digital transformation, institutional responsibility.

УДК 35.077.3:004.056.5:316.77
DOI <https://doi.org/10.32782/pma2663-5240-2025.45.33>

Кукляк Р.І.

аспірант кафедри адміністративного та фінансового менеджменту
Національного університету
«Львівська політехніка»

Постановка проблеми та її зв'язок із важливими науковими або практичними завданнями. В умовах гібридної війни, посилення інформаційних загроз та цифрової трансформації суспільства питання забезпечення інформаційної безпеки набуває особливої ваги не лише на національному, а й на місцевому рівні. Органи місцевого самоврядування дедалі частіше стають об'єктами цілеспрямованих інформаційних атак, фейкових кампаній, кібератак на інформаційні ресурси, що загрожує не лише функціонуванню муніципального управління, а й довірі громадян до влади.

У цьому контексті важливого значення набуває ефективна комунікаційна взаємодія як механізм оперативного інформування, спростування дезінформації, залучення громадськості до формування стійкого інформаційного середовища. Проте в практиці місцевого врядування комунікаційні аспекти публічного управління інформаційною безпекою залишаються недостатньо інституціалізованими, що вимагає глибокого наукового аналізу, концептуального осмислення та вдосконалення. Незважаючи на наявність державних стратегічних документів у сфері інформаційної безпеки, на місцевому рівні відсутні чіткі стандарти, моделі та механізми комунікаційної взаємодії, що дозволяють ефективно реагувати на інформаційні загрози, будувати довірливі відносини з громадянами та забезпечувати відкритість управління в умовах кіберризиків.

Проблема полягає в тому, що система публічного управління інформаційною безпекою на місцевому рівні залишається фрагментарною, мало координованою та недостатньо гнучкою до сучасних викликів, що унеможливує реалізацію ефективної комунікаційної політики в кризових інформаційних умовах. Вищенаведене зумовлює потребу у формуванні сучасних науково обґрунтованих підходів до комунікаційної взаємодії в системі публічного управління інформаційною безпекою, орієнтованих на прозорість, кіберстійкість, своєчасне реагування та залучення громадян.

Аналіз останніх досліджень і публікацій щодо проблем прийняття управлінських рішень у державному управлінні. Питання комунікаційної взаємодії в системі публічного управління інформаційною безпекою досліджуються у працях вітчизняних науковців, які висвітлюють окремі аспекти зазначеної проблеми, зокрема в контексті діяльності органів місцевого самоврядування. Так, у статті Л.М. Васильєвої та М.М. Іжболдіна увагу зосереджено на механізмах інформаційної безпеки в економічній сфері, які розглядаються як важливий елемент загальної стратегії інформаційного захисту

в державному управлінні. Автори підкреслюють, що належна організація комунікаційних процесів в інформаційному середовищі здатна суттєво впливати на рівень стійкості до інформаційних загроз та зміцнення інформаційної безпеки в державному секторі загалом [1]. І.В. Шпекторенко розкриває специфіку комунікативної діяльності органів виконавчої влади та місцевого самоврядування. Автор аналізує засоби, методи та форми комунікації, а також структури, відповідальні за внутрішні та зовнішні комунікації, що є важливими для забезпечення інформаційної безпеки на місцевому рівні [2]. Іншими науковцями досліджено теоретичні та практичні питання правового регулювання інформаційної взаємодії у місцевому самоврядуванні. Основна увага приділена аналізу інформаційних правовідносин, специфічних принципів інформаційної взаємодії та удосконаленню національного законодавства в цій сфері [3]. Дослідження Т. Амро присвячене впливу комунікативних технологій на ефективність публічного управління в Україні в умовах воєнного стану. Автор обґрунтовує необхідність удосконалення комунікаційного процесу та прийняття рішень у кризових ситуаціях, встановлення партнерських відносин між органами державної влади та громадянським суспільством для забезпечення інформаційної безпеки [4]. В. Терехов досліджує особливості нормативно-правового регулювання забезпечення інформаційної безпеки в органах місцевого самоврядування та виокремлює фактори, що впливають на стан захищеності інформації, та пропонує розробити концепцію інформаційної безпеки органів місцевого самоврядування [5]. В.І. Малімона описує роль та особливості сучасної комунікації для системи публічного управління. Посібник спрямований на формування у студентів знань щодо комунікацій в публічному управлінні та підвищення ефективності інформаційної взаємодії між органами влади та громадськістю [6].

Проведений аналіз свідчить про те, що науковці активно досліджують певні аспекти публічного управління інформаційною безпекою та комунікаційної взаємодії. Проте, у сучасних реаліях низка ключових питань залишається невирешеною. Зокрема, недостатньо вивченими є комплексні механізми інтеграції комунікаційної взаємодії та інформаційної безпеки на рівні місцевого самоврядування. Відсутні уніфіковані моделі ризик-орієнтованої комунікації в умовах цифрових загроз, обмежено аналізуються сучасні цифрові практики адаптивної комунікації в кризових ситуаціях, не систематизовано підходи до взаємодії органів влади з громадськістю

в умовах інформаційної нестабільності, що обумовлює необхідність подальшого комплексного дослідження даної проблематики.

Метою статті є дослідження особливостей, проблем та напрямів вдосконалення комунікаційної взаємодії в системі публічного управління інформаційною безпекою на рівні органів місцевого самоврядування в умовах цифрової трансформації та загроз кіберпростору.

Виклад основного матеріалу. У сучасних умовах гібридних загроз, цифрової трансформації та поширення дезінформаційних кампаній особливого значення набуває комунікаційна взаємодія в системі публічного управління. Вона виступає не лише як технічний або організаційний інструмент інформаційного обміну, а як системоутворюючий фактор забезпечення інформаційної безпеки держави, регіонів та громад. Комунікаційна взаємодія у сфері публічного управління інформаційною безпекою – це цілеспрямований, організований процес обміну інформацією між органами публічної влади (центральною та місцевими), громадськістю, інституціями безпекового сектору та суб'єктами інформаційного простору, що включає системи зворотного зв'язку, кризові комунікації, інформаційні кампанії, цифрові платформи взаємодії та офіційну комунікацію в межах державної політики. Сутність такої комунікаційної взаємодії полягає у забезпеченні своєчасного, достовірного та захищеного обміну інформацією між ключовими стейкхолдерами публічного управління, підвищенні обізнаності громадян щодо інформаційних загроз, включаючи фейки, пропаганду, витоки персональних даних, підтримці довіри до інституцій державної влади в умовах криз, соціальних потрясінь або кібератак, формуванні інформаційного імунітету територіальних громад до зовнішніх впливів через прозору, відкриту та проактивну публічну комунікацію (рис. 1).

У системі органів місцевого самоврядування комунікаційна взаємодія відіграє подвійну роль: з одного боку, як інструмент реалізації локальної політики інформаційної безпеки, з іншого – як канал оперативного реагування на загрози в інформаційному середовищі. Комунікаційна взаємодія забезпечує координацію між владою, підприємствами критичної інфраструктури, засобами масової інформації, громадськими ініціативами, освітніми установами, а ключовими інструментами такої взаємодії є офіційні вебресурси органів влади, соціальні мережі та цифрові платформи зворотного зв'язку, кризові інформаційні центри, стратегічні комунікації під час надзвичайних ситуацій, протоколи реагування на інформаційні атаки.

Таким чином, комунікаційна взаємодія в публічному управлінні інформаційною безпекою виконує як превентивну, так і управлінсько-координаційну функцію, стаючи індикатором адаптивності системи управління до динаміки сучасних викликів.

Аналіз міжнародних статистичних показників дозволяє сформулювати обґрунтовані висновки щодо ефективності комунікаційної взаємодії в системі публічного управління інформаційною безпекою України. Одним із ключових підтверджень високого рівня організаційної спроможності держави в цьому напрямі є позиція України в Індексі національної кібербезпеки (NCSI), де вона займає 19 місце серед 160 країн із загальним показником 80.83 балів (табл. 1).

Вищезазначене свідчить про сформовану політику у сфері кібербезпеки, яка включає інституційно оформлені комунікаційні механізми, налагоджені процедури реагування на загрози та міжвідомчу координацію. Додатковим емпіричним аргументом є офіційна статистика кіберінцидентів: упродовж

Таблиця 1

Індикатори ефективності комунікаційної взаємодії в управлінні інформаційною безпекою

Показник	Статистичне значення	Джерело
Місце України у NCSI (світовий рейтинг)	19 з 160 (80.83 балів)	Governance Academy Foundation [7]
Кількість кіберінцидентів (2024)	4,315 інцидентів на рік	InfoSec Ukraine [8]
Рівень важливості комунікації у публічній політиці (2024)	83.3% опитаних вважають важливою	VoxUkraine [9]
Довіра до стратегічних комунікацій в кіберзахисті (GMF, 2023)	Висока (перехід до проактивної моделі)	German Marshall Fund [10]
Інтероперабельність публічного управління (Європейська комісія, 2023)	Високий рівень відповідності Європейській рамці	European Commission [11]

Примітка: систематизовано автором за даними [7–11]

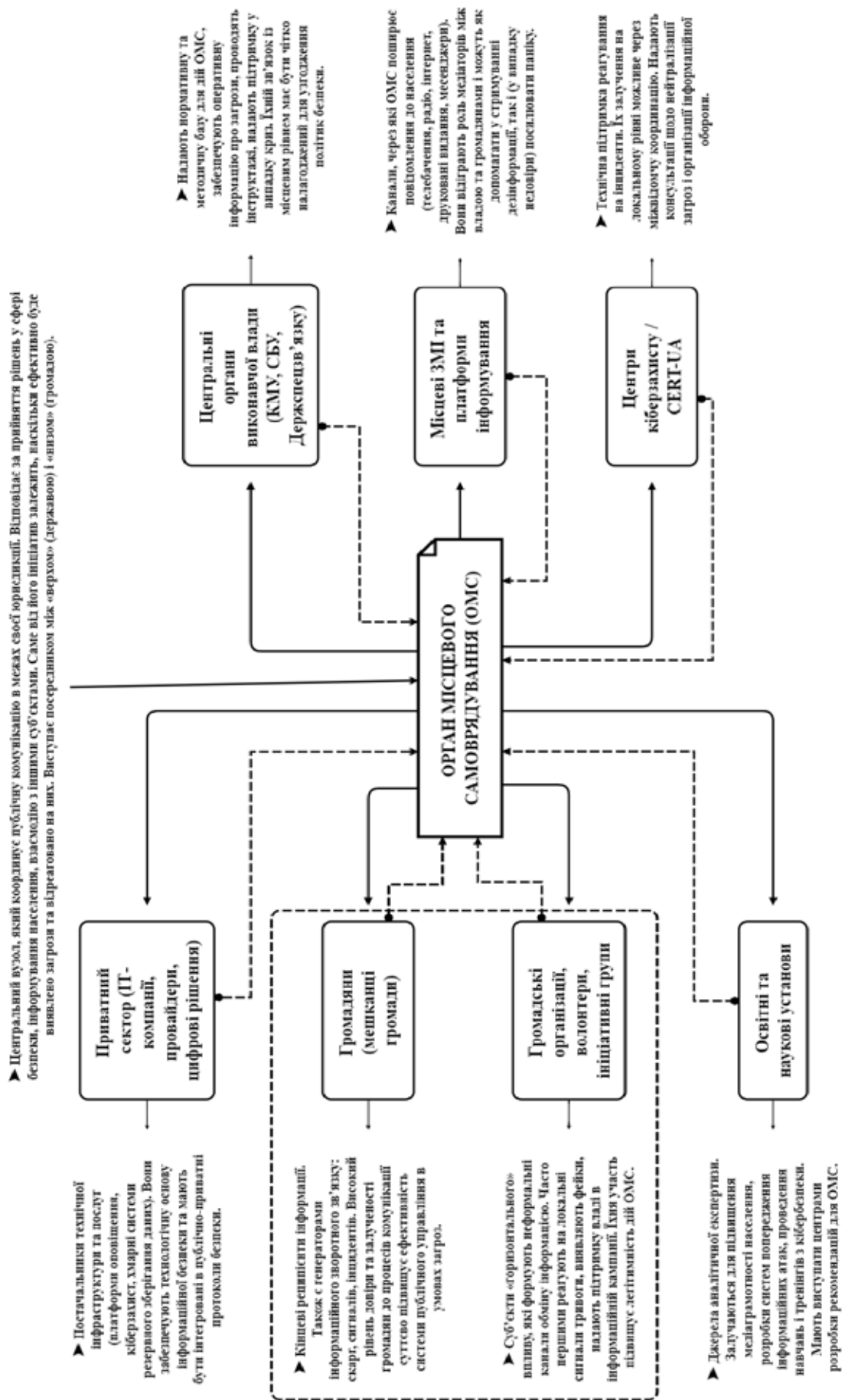


Рис. 1. Системно-організаційна модель комунікаційної взаємодії суб'єктів публічного управління в інформаційній безпеці на місцевому рівні

Примітка: систематизовано автором на основі проведеного дослідження

2024 року на території України зафіксовано 4315 інформаційних атак. Зазначене підтверджує як масштаб загроз, так і результативність механізмів сповіщення, оперативного моніторингу та поширення інформації серед стейкхолдерів. У цьому контексті особливого значення набуває комунікація між органами місцевого самоврядування, службами безпеки та населенням.

Підтвердженням важливості взаємодії влади й громадян слугує результат соціологічного дослідження VoxUkraine, згідно з яким 83.3% респондентів вважають необхідним здійснювати вплив на державну політику через доступні канали комунікації. Така статистика демонструє не лише високий рівень запиту на участь, а й зростаючу довіру до стратегічних механізмів комунікаційного управління. У дослідженні German Marshall Fund наголошено, що перехід України до проактивної моделі публічного інформування дозволив зміцнити кіберстійкість, підвищити

швидкість реагування на загрози та забезпечити сталість інформаційного середовища. Водночас, відповідно до звіту Європейської комісії, зафіксовано високий рівень інтероперабельності цифрового управління в Україні, що свідчить про ефективну інтеграцію інформаційно-комунікаційних технологій у практику прийняття рішень. Узагальнення зазначених фактів дозволяє дійти висновку, що комунікаційна взаємодія в межах публічного управління інформаційною безпекою відіграє не лише превентивну, а й управлінсько-координаційну роль, виступаючи достовірним індикатором адаптивності адміністративної системи до динаміки сучасних загроз.

На основі соціологічного дослідження, проведеного компанією Research.ua LLC у листопаді 2024 року, результати якого зведено на рисунку 2, можна сформулювати цілісну аналітичну картину щодо стану політичної довіри, пріоритетів громадян, а також перспектив публічного управління в умовах війни.

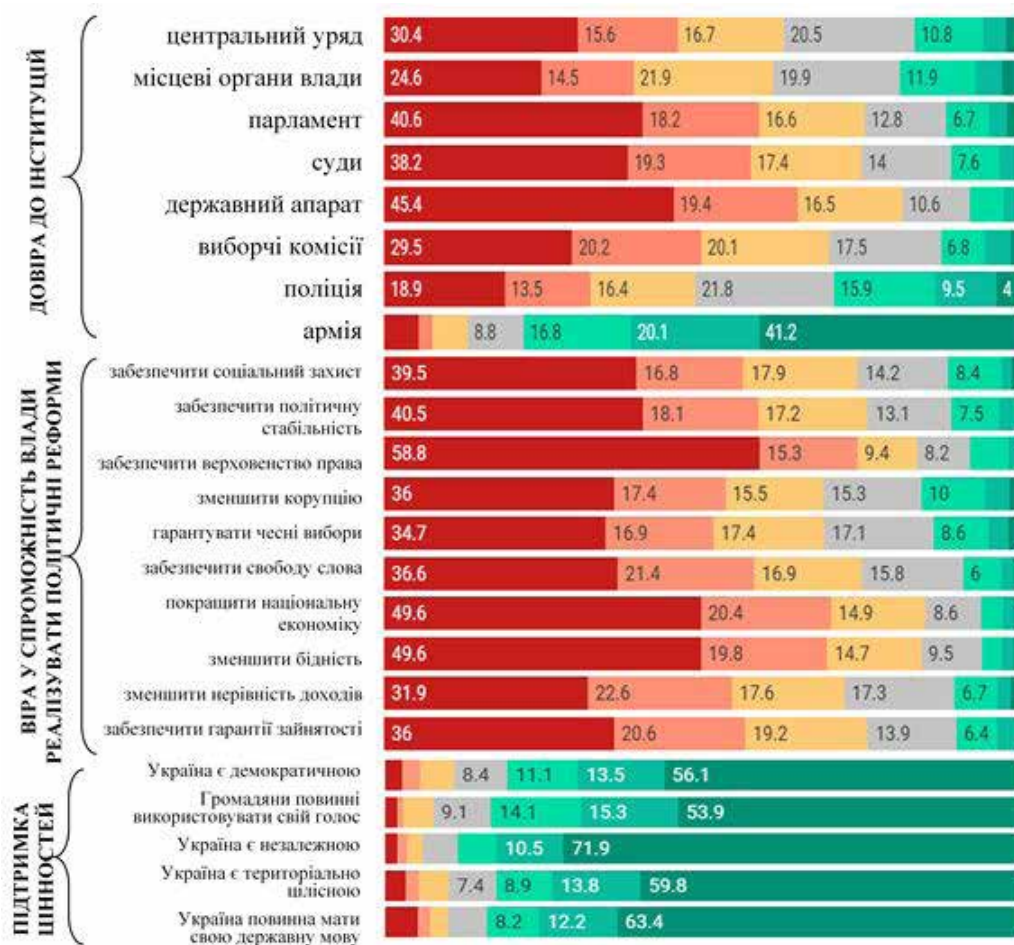


Рис. 2. Стан політичної довіри, очікувань від влади та підтримки ключових цінностей серед українців: систематизовані результати опитування

Примітка: сформовано автором за даними [9]

Репрезентативна вибірка охопила 850 респондентів віком 16–55 років з урахуванням регіональної, статевої та освітньої структури, що забезпечує високу валідність висновків [9].

Результати свідчать про наявність парадоксального поєднання: з одного боку, зафіксовано високий рівень ціннісної підтримки основоположних принципів державності, зокрема демократії, незалежності, територіальної цілісності та права громадян на політичну участь. Зокрема, 88,6% респондентів повністю визнають важливість незалежності України, 83,3% – необхідність активного голосу громадян, а 80,7% – демократичного устрою. З іншого боку, рівень довіри до ключових політичних інституцій є вкрай низьким. Державний апарат не довіряють 81,3% опитаних, парламенту – 75,4%, судам – 74,9%, а виборчим комісіям – 69,8%. Навіть органи місцевого самоврядування мають рівень недовіри на рівні 61%, що свідчить про загальну кризу інституційної легітимності. Єдиним винятком є армія, якій довіряє переважна більшість – понад 60% повністю або переважно підтримують її діяльність.

Аналіз розділу щодо очікувань від політики держави свідчить про домінування соціально-економічного порядку денного. Близько 83,5% респондентів не вірять, що влада зможе подолати корупцію; 84,9% не очікують реального зменшення бідності; 84,1% – зменшення нерівності доходів; 75,8% – забезпечення соціального захисту. Подібний скепсис стосується й правової та політичної сфери: 75,6% не вірять у реалізацію верховенства права, а 74,2% – у досягнення політичної стабільності.

Виявлений системний скептицизм не знищує віру в саму демократичну модель – натомість він концентрується не на ідеології, а на виконавцях – політиках та управлінських структурах. Дослідження виявило слабкий зв'язок (кореляція 0,02–0,20) між вірою в базові демократичні цінності й довірою до інституцій, що підтверджує гіпотезу про стратегічний характер української довіри: громадяни схильні підтримувати інституції, які демонструють щирі зусилля навіть за відсутності швидких результатів. Прикладом виступає ЗСУ, які попри надзвичайно складні умови зберігають високий рівень підтримки саме завдяки відчутній мобілізації та ефективній публічній комунікації.

На цій основі можна зробити кілька стратегічних висновків. По-перше, інституційна довіра в Україні не є незмінно низькою – вона варіативна і піддається відновленню за умов ефективної комунікації, підзвітності та видимої роботи. По-друге, комунікаційна взаємодія між державою і громадянами має розгля-

датися як самостійний інструмент управління довірою, який не лише передає інформацію, а й сигналізує про готовність до змін, намагання діяти та спільність інтересів. По-третє, місцеве самоврядування зберігає потенціал стати осередком відновлення легітимності, з огляду на дещо вищі показники довіри та меншу дистанцію до потреб громад. Таким чином, оприлюднені результати дозволяють інтерпретувати кризу довіри не як фіксований стан, а як реакцію на якість взаємодії між громадянами та інституціями. За наявності прозорості, стратегічної та орієнтованої на участь публічної комунікації існує реальна можливість поступового відновлення довіри до демократичного управління навіть у період глибокої соціальної напруги та війни. З метою удосконалення комунікаційної взаємодії органів місцевого самоврядування в системі публічного управління інформаційною безпекою розроблено рекомендації, що представлено на рис. 3.

Запропоновані напрями представляють системний підхід до вдосконалення комунікаційної взаємодії органів місцевого самоврядування в контексті публічного управління інформаційною безпекою та враховують критично важливі принципи прозорості, довіри та кіберстійкості як фундаментальні умови для формування надійного інформаційного середовища в умовах гібридних загроз та цифрових викликів.

Питання прозорості постає як основа легітимності рішень, ухвалених у сфері інформаційної безпеки. У цьому контексті особливого значення набуває впровадження стандартизованих кризових протоколів інформування, що передбачають чітко регламентовані терміни, канали та способи передачі даних населенню у разі виникнення інформаційних інцидентів – таких як кібератаки, дезінформаційні кампанії або порушення роботи інформаційної інфраструктури. Регулярна публікація статистичних звітів щодо стану інформаційної безпеки в громаді, зокрема даних про інциденти, вжиті заходи та потенційні ризики, дозволяє посилити відкритість місцевої влади. Додатково, важливим є забезпечення публічного доступу до алгоритмів прийняття управлінських рішень під час надзвичайних ситуацій – через офіційні вебресурси ОМС, мобільні додатки чи публічні брифінги (рис. 3).

Усвідомлення довіри як ключового індикатора ефективності комунікацій передбачає створення механізмів постійного зворотного зв'язку з мешканцями. Йдеться про доступні гарячі лінії, цифрові чат-боти, модулі для звернень громадян, які мають бути інтегровані у платформу електронного врядування для

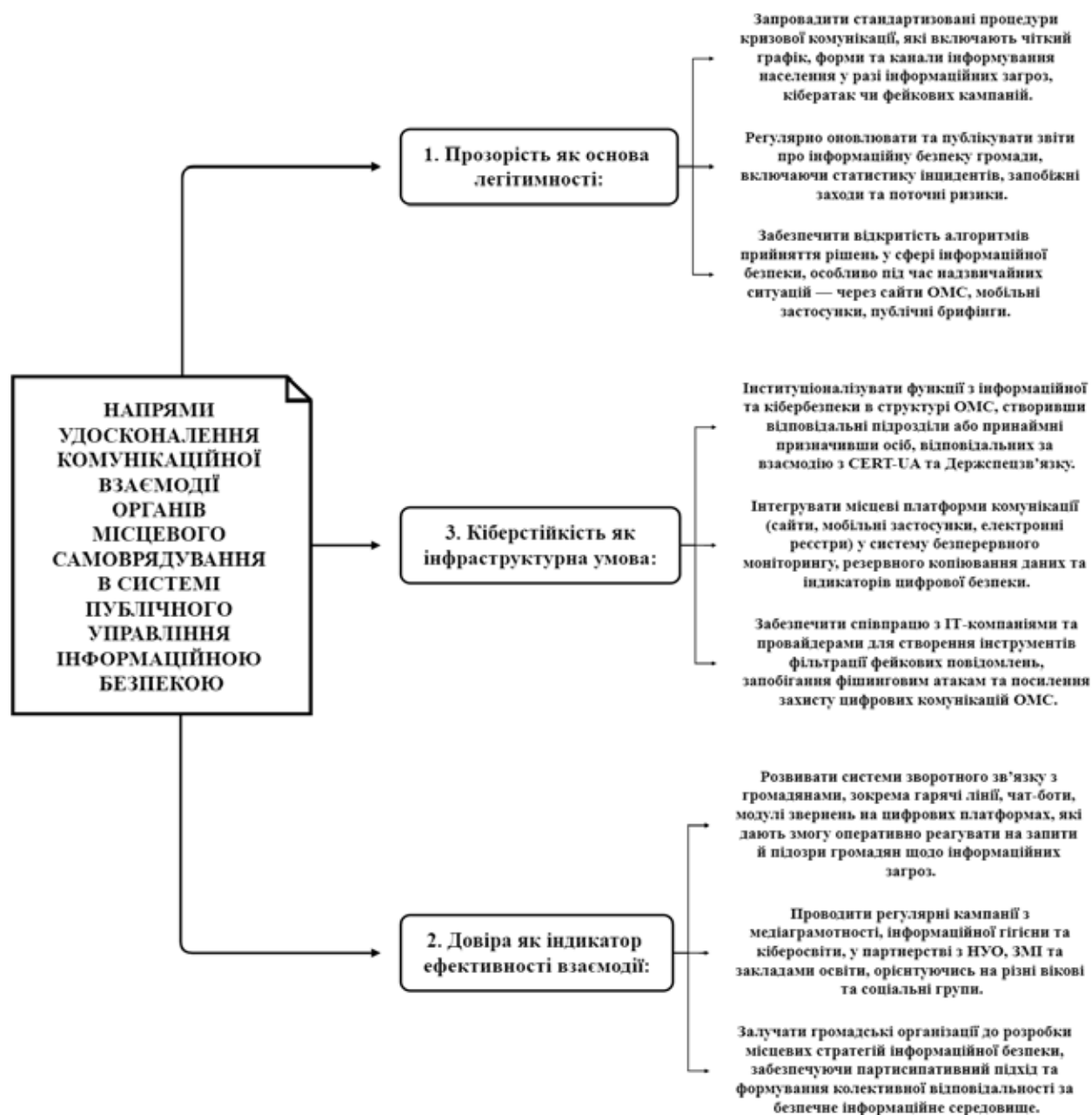


Рис. 3. Напрями удосконалення комунікаційної взаємодії органів місцевого самоврядування в системі публічного управління інформаційною безпекою

Примітка: розроблено автором на основі проведеного дослідження

оперативного реагування на підозри щодо інформаційних загроз. Паралельно слід проводити інформаційно-просвітницькі кампанії з підвищення рівня медіаграмотності, цифрової обізнаності та кібергієни, орієнтовані на різні вікові категорії. Важливо, щоб ці заходи реалізовувалися у партнерстві з закладами освіти, громадськими організаціями та ЗМІ. Не менш значущим є залучення інститутів громадянського суспільства до формування місцевих стратегій інформаційної безпеки – через консультації, круглі столи та спільну розробку політик, що дозволяє забезпечити спільну від-

повідальність та більш високу суспільну легітимність прийнятих рішень.

У межах компонента кіберстійкості варто наголосити на необхідності інституціоналізації функцій з інформаційної безпеки в структурі місцевої влади. Створення профільних підрозділів або призначення відповідальних осіб за координацію з національними центрами кібербезпеки (CERT-UA, Держспецзв'язок) дозволить забезпечити належний рівень реагування на інформаційні загрози. Необхідно також інтегрувати цифрову інфраструктуру місцевих громад (вебсайти, застосунки, електронні

послуги) у системи резервного копіювання та моніторингу індикаторів безпеки. Нарешті, співпраця з ІТ-компаніями, телекомунікаційними провайдерами та технічними партнерами має стати регулярною практикою – для впровадження інструментів фільтрації фейкових повідомлень, запобігання фішинговим атакам і посилення захисту каналів офіційної цифрової комунікації.

Запропоновані заходи повинні перейти зі стадії ситуативного реагування до рівня постійно функціонуючих управлінських процедур, закріплених у локальних нормативно-правових актах і підкріплених цифровою інфраструктурою (табл. 2). Регулярна оцінка ефективності та адаптація політик до нових ризиків є необхідною умовою їх успішності.

Тільки системна, послідовна і прозора комунікаційна політика на рівні місцевого самоврядування здатна зберігати довіру громадян та ефективно протидіяти сучасним загрозам в інформаційному просторі.

Вищенаведена таблиця узагальнює ключові рекомендації щодо вдосконалення комунікаційної взаємодії органів місцевого самоврядування в системі публічного управління інформаційною безпекою та містить відповідне нормативно-правове підґрунтя для їх реалізації. Для кожної пропозиції визначено чинний акт законодавства або нормативний документ, що регламентує відповідну сферу, а також конкретизовано зміни, яких потребує його зміст. Такий підхід дозволяє не лише систематизувати заходи з урахуванням принципів прозо-

Таблиця 2

**Узагальнення нормативно-правових засад та пропозицій
щодо вдосконалення комунікаційної взаємодії органів місцевого самоврядування
в системі публічного управління інформаційною безпекою**

№	Рекомендація	Нормативно-правове забезпечення	Запропоновані зміни
1	Запровадження стандартів кризової комунікації та звітності про інформаційну безпеку	Закон України «Про інформацію»	Додати розділ про комунікаційну безпеку; встановити вимогу регулярної звітності органів місцевого самоврядування щодо інформаційної безпеки
2	Регулярне інформування громадськості через цифрові платформи	Закон України «Про інформацію»	Регламентувати графік, формат і канали офіційної кризової комунікації
3	Формування локальних стратегій інформаційної безпеки	Закон України «Про національну безпеку України»	Закріпити обов'язкову роль місцевих органів у реалізації стратегії національної безпеки; включити вимогу до розробки локальних стратегій
4	Призначення відповідальних осіб або створення підрозділів з кібербезпеки в ОМС	Закон України «Про місцеве самоврядування в Україні»	Передбачити обов'язок створення посади або функціонального підрозділу з питань кібербезпеки в структурі місцевого самоврядування
5	Підключення ОМС до CERT-UA та інших національних систем реагування на інциденти	Закон України «Про основні засади забезпечення кібербезпеки України»	Розширити перелік суб'єктів національної системи кібербезпеки, включивши органи місцевого самоврядування
6	Проведення кампаній з медіаграмотності та кібергігієни	Закон України «Про інформацію»; державні програми освіти	Запровадити обов'язкове інформування населення через навчальні заходи; передбачити співпрацю з ГО та ЗВО
7	Залучення громадськості до розробки політики інформаційної безпеки	Закон України «Про місцеве самоврядування в Україні»	Уточнити механізми громадського обговорення інформаційної політики, зокрема цифрової безпеки
8	Розширення функцій ЦНАП як інформаційних хабів у кризових ситуаціях	Типове положення про ЦНАП	Визначити функцію кризової комунікації ЦНАП у випадку загроз інформаційній безпеці
9	Інтеграція індикаторів інформаційної стійкості в стратегії цифрової трансформації	Концепція розвитку електронного урядування та цифрової трансформації	Передбачити моніторинг та оцінку інформаційної стійкості як елемент управління ризиками в цифровому середовищі

Примітка: розроблено автором на основі проведеного дослідження [12]

рості, довіри та кіберстійкості, але й створити практичний інструмент для адаптації на рівні місцевої політики. Узагальнення нормативно-правових засад та пропозицій є водночас ініціативним планом дій для органів місцевого самоврядування і дороговказом для національних інституцій щодо вдосконалення законодавчої бази у сфері інформаційної безпеки.

Висновки і пропозиції. Комунікаційна взаємодія в системі публічного управління інформаційною безпекою на локальному рівні є критичним чинником формування суспільної довіри, забезпечення стійкості до інформаційних атак та адаптивності владних структур до сучасних викликів. Проведений аналіз статистичних і соціологічних даних підтвердив наявність глибокої недовіри громадян до більшості інституцій. Водночас зафіксовано високу підтримку демократичних цінностей та громадянської участі. Візуалізована модель взаємодії суб'єктів публічного управління в інформаційній сфері окреслила ключові точки комунікації, де необхідне посилення прозорості, кіберстійкості та зворотного зв'язку. Доведено, що ефективна комунікаційна політика виконує не лише превентивну, а й координаційно-управлінську функцію в умовах гібридної війни.

Рекомендовано інституціоналізувати функції з кібер- та інформаційної безпеки в структурах органів місцевого самоврядування, запровадити стандартизовані протоколи кризової комунікації, посилити механізми зворотного зв'язку з громадянами, а також залучити громадські організації до формування локальних стратегій безпеки. Необхідно внести зміни до чинних нормативно-правових актів з метою закріплення прозорих процедур комунікації, визначення відповідальних осіб та інтеграції цифрових платформ у систему управління інформаційними ризиками. Системне впровадження таких підходів дозволить органам місцевого самоврядування ефективніше реагувати на інформаційні загрози та посилити суспільну стійкість.

ЛІТЕРАТУРА:

1. Васильєва, Л. М., & Іжболдін, М. М. (2023). Механізми та підходи щодо забезпечення інформа-

ційної безпеки підприємницької діяльності як елемента інформаційної безпеки держави. *Публічне управління і адміністрування в Україні*, (36). URL: <https://pag-journal.iei.od.ua/archives/2023/36-2023/36-2023.pdf>

2. Шпекторенко І. В. (2024). Комунікації у публічному управлінні : навчальний посібник. НТУ «Дніпровська політехніка». URL: https://palsg.nmu.org.ua/ua/literature/Шпекторенко_І.В._Комунікації_у_публічному_управлінні_Навч_посіб_2024.pdf

3. Інформаційна взаємодія у місцевому самоврядуванні: перспективи правового регулювання. (n.d.). Інститут проблем інформаційного суспільства. URL: <https://ippi.org.ua/informatsiina-vza%D1%94modiya-umistsevomu-samovryaduvanni-perspektivi-pravovogo-regulyuvannya>

4. Амро Т. А. (2023). Вплив комунікативних технологій на ефективність публічного управління в Україні в умовах воєнного стану (Дисертація доктора наук з державного управління). МАУП. URL: <https://maup.com.ua/assets/files/dis/25-00-05/tajer-disertaciya.pdf>

5. Терехов В. (2017). Удосконалення адміністративно-правового регулювання реалізації політики інформаційної безпеки в органах місцевого самоврядування. *Актуальні проблеми правознавства*, (1), 43–47. URL: <https://appj.wunu.edu.ua/index.php/appj/article/view/116/116>

6. Малімон В. І. (2021). Комунікаційна політика в діяльності державного службовця : навчальний посібник. Івано-Франківськ : НУНГ. URL: <https://surli.cc/zrcrkNational Cyber Security Index. e-Governance Academy. URL: https://ncsi.ega.ee/country/ua/>

7. About past, present and future of Ukraine. *InfoSec Ukraine*. URL: <https://surl.li/jqbipd>

8. Tamilina L. Do Ukrainians Trust Democratic Institutions? Institutional Confidence and Democracy Amid the War in Ukraine. *Society. VoxUkraine*. URL: <https://voxukraine.org/en/do-ukrainians-trust-democratic-institutions-institutional-confidence-and-democracy-amid-the-war-in-ukraine>

9. Kvartsiana Kh.. Ukraine's Cyber Defense. URL: <https://www.gmfus.org/sites/default/files/2023-12/Kvartsiana%20-%20Ukraine%20Cyber%20-%20Report.pdf>

10. Digital Public Administration factsheet. 2023. Ukraine. *European Commission*. URL: https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/DPA_Factsheets_2023_Ukraine_vFINAL_rev.pdf

11. Законодавство України. *Офіційний вебпортал парламенту України*. URL: <https://zakon.rada.gov.ua/laws/main/a#Find>