УДК 35.077.3:004.056.5:316.77
DOI https://doi.org/10.32782/2310-9653-2025-4.8

Р. І. Кукляк, аспірант кафедри адміністративного
та фінансового менеджменту Національного університету
«Львівська політехніка»

КОМУНІКАЦІЙНІ МОДЕЛІ ПУБЛІЧНОГО УПРАВЛІННЯ В КОНТЕКСТІ ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ СТІЙКОСТІ ОРГАНІВ МІСЦЕВОГО САМОВРЯДУВАННЯ

Досліджено особливості функціонування комунікаційних моделей у системі публічного управління інформаційною безпекою на рівні органів місцевого самоврядування України. Розроблено порівняльно-аналітичну модель впливу лінійних, інтерактивних і мережевих комунікаційних моделей на формування інформаційної стійкості органів місцевого самоврядування, що дозволило системно оцінити їхні ризики, управлінські можливості та застосовність у цифровому середовищі.Проаналізовано глобальні й національні статистичні індикатори (зокрема дані Глобального індексу кібербезпеки ITU), які засвідчують нерівномірність розвитку складових кіберстійкості України: високі показники у сфері правових та технічних заходів поєднуються з недостатністю кадрового потенціалу, організаційної спроможності та слабкою інтегрованістю громад у національні механізми інформаційної безпеки. Виявлено, що комунікаційна взаємодія в органах місцевого самоврядування виконує ключову координаційну, превентивну та управлінську функції, визначаючи здатність громад протидіяти інформаційним інцидентам, дезінформаційним кампаніям та кіберзагрозам.

Сформовано концепцію оптимізації комунікаційної безпеки органів місцевого самоврядування, яка інтегрує правові, технічні, організаційні, освітні та кооперацийні механізми, відображаючи їх взаємозв'язок із компонентами індексу GCI. Візуалізовано структуру концепції та деталізовано її ключові елементи: локальні політики комунікаційної безпеки, безпечні канали обміну інформацією, центри комунікаційної координації, систему підготовки кадрів, мережеву міжмуніципальну взаємодію та партнерства з національними структурами кіберзахисту. Показано, що слабкі результати України у сфері розвитку потенціалу (14,61 бали) та організаційних заходів (15,97 бали) безпосередньо впливають на стійкість комунікаційних процесів у громадах та потребують цілеспрямованого управлінського втручання.

Сформульовано практичні рекомендації щодо удосконалення комунікаційної безпеки в органах місцевого самоврядування. Обґрунтовано необхідність інституціоналізації локальних політик інформаційної та комунікаційної безпеки, створення регламентованих процедур кризових комунікацій, впровадження систем раннього сповіщення про інциденти, кадрового підсилення функцій кіберстійкості, а також розвитку горизонтальних мереж взаємодії між громадами. Узагальнено нормативно-правові передумови для підвищення прозорості, довіри та керованості інформаційного простору громад та визначено напрями подальшого удосконалення законодавства.

Результати дослідження можуть бути використані для формування стратегій інформаційної стійкості територіальних громад, розбудови місцевої політики кіберзахисту, комплексного підсилення комунікаційних процесів у публічному управлінні та підвищення здатності органів місцевого самоврядування діяти в умовах гібридної війни та цифрових загроз.

Ключові слова: *публічне управління, комунікаційні моделі, інформаційна безпека, інформаційна стійкість, органи місцевого самоврядування, кіберзагрози, кризові комунікації, кіберстійкість, цифрова трансформація.*

R. I. Kuklyak. Communication models of public administration in the context of forming information resilience of local government bodies

The peculiarities of the functioning of communication models in the system of public information security management at the level of local government bodies of Ukraine were studied. A comparative analytical model of the impact of linear, interactive and network communication models on the formation of information resilience of local governments has been developed, which allowed for a systematic assessment of their risks, management capabilities and applicability in the digital environment. Global and national statistical indicators (in particular, data from the ITU Global Cybersecurity Index) were analyzed, which indicate the uneven development of the components of Ukraine's cyber resilience: high indicators in the field of legal and technical measures are combined with insufficient human resources, organizational capacity and weak integration of communities into national information security mechanisms. It was found that communication interaction in local governments performs a key coordination, preventive and management function, determining the ability of communities to counteract information incidents, disinformation campaigns and cyber threats.

A concept for optimizing communication security in local governments has been developed, which integrates legal, technical, organizational, educational, and cooperation mechanisms, reflecting their interrelationship with the components of the GCI index. The structure of the concept has been visualized and its key elements have been detailed: local communication security policies, secure information exchange channels, communication coordination centers, a personnel training system, networked intermunicipal interaction, and partnerships with national cyber defense structures. It has been shown that Ukraine's weak results in the field

of capacity development (14.61 points) and organizational measures (15.97 points) directly affect the sustainability of communication processes in communities and require targeted management intervention.

Practical recommendations have been formulated for improving communication security in local governments. The need for institutionalization of local information and communication security policies, creation of regulated crisis communication procedures, implementation of early warning systems for incidents, personnel strengthening of cyber resilience functions, as well as development of horizontal networks of interaction between communities is substantiated. The regulatory and legal prerequisites for increasing transparency, trust and manageability of the information space of communities are summarized and directions for further improvement of legislation are identified.

The results of the study can be used to form strategies for information resilience of territorial communities, development of local cyber defense policies, comprehensive strengthening of communication processes in public administration and increase the ability of local governments to act in conditions of hybrid warfare and digital threats.

Key words: *public administration, communication models, information security, information resilience, local governments, cyber threats, crisis communications, cyber resilience, digital transformation.*

Постановка проблеми. Україна перебуває у процесі глибинної цифровізації суспільства та публічного управління, але несинхронність між темпами цифрової інтеграції та рівнем адаптації органів місцевого самоврядування створює суттєві загрози інформаційній стійкості. З одного боку, цифрове середовище стрімко розширюється, охоплюючи всі сфери життєдіяльності громади. Зростає інтенсивність використання соціальних мереж, електронних сервісів, онлайн-платформ комунікації, що формує нову архітектуру інформаційного простору. З іншого боку, органи місцевого самоврядування часто не володіють належними інструментами, компетенціями та інституційною структурою для ефективного управління інформаційними потоками, які стають дедалі складнішими, динамічнішими та потенційно небезпечними.

У такій ситуації інформаційна стійкість громад дедалі більше залежить від якості комунікаційної політики. Проте значна частина місцевих органів влади досі працює за застарілими моделями інформаційної взаємодії, у яких забезпечення прозорості, передбачуваності та достовірності інформації не розглядається як складова безпеки. Невпорядкованість стандартів комунікацій, низький рівень інституційної культури взаємодії з громадянами, фрагментарність практик кризового інформування, неузгодженість внутрішніх процедур і відсутність єдиних підходів до цифрової присутності створюють передумови для підриву довіри та втрати керованості інформаційними процесами на місцевому рівні.

Ситуація ускладнюється стрімким зростанням кіберзагроз, які стають невід'ємним елементом сучасної гібридної війни. Інформаційний простір громад дедалі частіше стає мішенню для деструктивних впливів, спрямованих на порушення сталості інформаційних каналів, дискредитацію органів влади, дестабілізацію соціальної ситуації чи спотворення важливої комунікації між владою та населенням. Поширеним інструментом зовнішнього втручання стають маніпулятивні інформаційні кампанії, спрямовані на розхитування суспільної думки, провокування страху, невизначеності, панічних настроїв або знищення авторитету органів місцевого самоврядування через поширення фейкових повідомлень. У цих умовах громади опиняються у ситуації, коли будь-яка слабкість у комунікаційному ланцюзі може бути використана для створення інформаційних інцидентів, здатних вплинути на життєздатність місцевих інституцій.

Зростання кіберзагроз ставить перед органами місцевого самоврядування низку нових практичних завдань, які раніше були актуальними переважно для центральних органів влади або сектору критичної інфраструктури. Місцеві ради змушені не лише забезпечувати функціонування цифрових сервісів, а й активно протидіяти зовнішнім впливам, захищати персональні дані громадян, забезпечувати неперервність доступу до офіційної інформації та гарантувати її достовірність. При цьому інформаційний простір громади є значно вразливішим, ніж національний: він характеризується фрагментарністю каналів, нерівномірністю цифрової готовності, залежністю від кадрових ресурсів, які часто не мають спеціалізованої підготовки. Вищенаведене посилює ризики появи локальних інформаційних криз, які швидко переростають у масштабні, якщо їх не виявити та не нейтралізувати на ранніх етапах.

Проблема інформаційної стійкості органів місцевого самоврядування набуває особливого значення в контексті наукових і практичних завдань сучасного публічного управління. По-перше, саме комунікаційні моделі стають інструментом, через який формується середовище довіри, забезпечується легітимність рішень, підтримується стабільність місцевої влади та взаємодія з громадянами. По-друге, через ефективні інформаційні моделі ОМС можуть своєчасно реагувати на загрози, мінімізувати ризики дезінформації та формувати спільну інформаційну позицію громади. По-третє, якість комунікацій визначає рівень демократичності управління, оскільки від неї залежить доступ громадян до інформації, можливість впливу на рішення та рівень їх залучення.

Відтак актуальність дослідження зумовлена необхідністю інтеграції сучасних комунікаційних моделей у систему публічного управління органів місцевого самоврядування так, щоб вони сприяли підвищенню інформаційної стійкості, були здатні протистояти зовнішнім та внутрішнім інформаційним загрозам і забезпечували стабільність та ефективність функціонування місцевих владних інституцій у цифрову добу.

Аналіз останніх досліджень і публікацій. У системі публічного управління комунікація є не лише інструментом обміну інформацією, а й ключовим механізмом забезпечення взаємодії між органами влади, суспільством та іншими суб'єктами публічної політики. Сутність публічного управління неможливо зрозуміти поза комунікаційним виміром, адже саме через комунікацію відбувається формування політики, ухвалення управлінських рішень, мобілізація громадської підтримки та легітимація влади. Ефективна комунікація виступає запобіжником управлінських збоїв і водночас – базовою умовою для підтримання інформаційної безпеки.

Комунікаційні процеси в публічному управлінні тривалий час осмислювались на основі класичних моделей, що сформувалися у ХХ столітті в межах загальної теорії комунікації. Їхня цінність полягає в можливості формалізованого опису процесів передачі інформації та виявлення чинників, що впливають на її ефективність. У сфері публічного управління вони стали методологічним підґрунтям для побудови системи взаємодії між державою, суспільством та інституціями громадянського сектору.

Класична лінійна модель комунікації Шеннона-Уівера описує процес передавання повідомлення від джерела через канал до отримувача з урахуванням можливих перешкод («шумів»). У контексті публічного управління ця модель демонструє вразливість інформаційних потоків: повідомлення, що поширюється органами влади, може бути спотворене на рівні каналу або інтерпретації. Саме «шум» у цій моделі інтерпретується сучасними дослідниками як аналог ризику дезінформації, маніпуляцій чи інформаційних атак [1].

Українські вчені відзначають, що цінність моделі Шеннона-Уівера полягає у можливості досліджувати надійність каналів комунікації. Зокрема, М. Головатий у своїх працях з державного управління наголошує, що публічні органи влади мають впроваджувати системи контролю інформаційних потоків, аби знижувати ризики «шуму» в управлінській комунікації [2].

Модель Г. Лассуелла визначає комунікацію як процес, який можна розкласти за формулою: «Хто? – Що? – По якому каналу? – Кому? – З яким ефектом?». На відміну від моделі Шеннона-Уівера, вона акцентує увагу на цілях та результативності комунікації. У публічному управлінні це дозволяє аналізувати вплив владних повідомлень на громадську думку, формування довіри або недовіри до інституцій.Для інформаційної безпеки ця модель актуальна тим, що вона звертає увагу не лише на технічний аспект комунікації, а й на її ефективність у досягненні результату. Якщо ефект не відповідає очікуваному (наприклад, поширення паніки замість мобілізації довіри), то це свідчить про загрозу інформаційній стійкості суспільства.

У 1950-1960-х роках поширення набув системний підхід до комунікації (Д. Берталанфі), де комунікація розглядається як взаємодія елементів у межах цілісної системи. З точки зору публічного управління, це означає, що ефективність інформаційного обміну залежить не лише від технічних характеристик каналів, а й від структурної організації системи управління.Український дослідник В. Бараболя підкреслює, що системний підхід дозволяє розглядати публічне управління як відкриту систему, де комунікація виступає ключовим регулятором обміну між владою та суспільством. У випадку збою цього регулятора система втрачає здатність адекватно реагувати на зовнішні загрози, що безпосередньо створює ризики для інформаційної безпеки. Водночас на якість комунікації впливають низка зовнішніх і внутрішніх чинників,зокрема інформаційна відкритість влади, наявність ресурсів, рівень цифровізації, правовограмотність населення, а також соціальна згуртованість громади [3, с. 72–83].

Подальший розвиток отримали інтерактивні моделі комунікації (Ч. Осгуд, У. Шрамм), які враховують зворотний зв'язок і циклічний характер обміну інформацією. Вони відображають реальність публічного управління більш адекватно, оскільки органи влади не лише транслюють інформацію, а й отримують відгуки від суспільства.У сфері інформаційної безпеки наявність зворотного зв'язку критично важлива: вона дозволяє виявляти недовіру, фейки, інформаційні атаки на ранніх стадіях. Відсутність інтерактивності створює умови для накопичення ризиків і загострення кризових ситуацій.

Вітчизняні дослідники наголошують, що комунікація у публічному управлінні має системний характер. Так, О.Д. Бакуменко визначає її як «сукупність процесів взаємодії, спрямованих на узгодження позицій учасників управлінських відносин і забезпечення стійкості політичної системи» [4, с. 21–28.]. Науковець акцентує, що ігнорування принципів комунікації веде до інформаційних розривів, які знижують ефективність управління та підвищують ризики інформаційних атак.

С. В. Серьогін [6] трактує комунікацію як «інституційне посередництво», що пов'язує різні рівні публічного управління. На його думку, інформаційні прогалини та викривлення комунікацій створюють додаткові ризики, адже стають каналами для поширення недостовірної інформації або маніпулятивних впливів.

Особливий акцент у сучасній літературі робиться на ролі комунікації у цифровому середовищі. Як зазначає І. Руденко, цифрові канали трансформують класичні моделі, створюючи умови для багатоспрямованої комунікації та формування мережевих спільнот, здатних як зміцнювати, так і підривати інформаційну безпеку [7 с. 59–69]. Автори В. Євдокимов, та С. Коломієць у працях про комунікативні технології пропонують інноваційну модель комунікації, де особливу роль відіграють цифрові інструменти візуалізації та аналітики, що дозволяють відслідковувати інформаційні ризики у реальному часі [8]. О.В. Кравченко наголошує на важливості системно-синергетичної моделі, де комунікація розглядається як процес самоорганізації, що здатен або підвищити стійкість держави,

або, навпаки, спричинити інформаційні кризи в умовах зовнішнього тиску [9]. Узагальнення підходів українських учених показує, що вітчизняна наука пропонує багатовимірне бачення комунікаційних моделей у публічному управлінні (табл. 1).

Таким чином, аналіз вітчизняної наукової літератури свідчить, що комунікація у публічному управлінні є складним багаторівневим явищем, яке одночасно виконує функції інформування, узгодження, легітимації, формування довіри та стратегічного управління ризиками. Її ефективність прямо корелює з рівнем інформаційної безпеки, адже неналагоджені канали комунікації стають джерелом вразливостей і підвищують ймовірність деструктивного інформаційного впливу.

Метою дослідження є обґрунтування ролі комунікаційних моделей публічного управління у формуванні інформаційної стійкості органів місцевого самоврядування, з'ясуванні їхнього впливу на спроможність громад протидіяти інформаційним загрозам та визначенні управлінських підходів щодо удосконалення комунікаційної політики в умовах цифрової трансформації.

Виклад основного матеріалу. Цифрова комунікація – реальний і поширений феномен в Україні, але структурна та інституційна підготовка систем публічного управління для роботи в таких умовах – часто недостатня, що породжує серйозні загрози інформаційній стійкості, особливо на рівні місцевого самоврядування. За останніми даними, 82% населення України користуються інтернетом, на початок 2024 року близько 29,64 млн українців були інтернет-користувачами; рівень інтернет-penetrації становив ~79,2% [10]. При цьому значна частина населення (понад 60%) користується соціальними мережами, що підсилює роль цифрових комунікацій у повсякденному інформаційному середовищі [11]. Проте попри високий рівень цифрового охоплення, аналіз розвитку ІКТ-сфери в Україні свідчить про наявність значних прогалин у інфраструктурі, стандартизації цифрових комунікацій та захисті інформації.

Водночас Україна перебуває у стані гібридних загроз, де інформаційна сфера є об'єктом системного впливу. Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA, яка діє при Держспецзв'язку, в 2024 році опрацювала 4315 кіберінцидентів, що на 69,8% більше, ніж роком раніше, коли кіберзлочинці атакували український кіберпростір 2541 раз. Кіберзловмисники найчастіше націлюються на органи місцевої влади, центральні урядові структури, сектор безпеки й оборони, енергетику, телекомунікації та комерційні організації. Основні інциденти пов'язані з фішингом, поширенням шкідливого ПЗ, несанкціонованими підключеннями та компрометацією облікових записів чи систем, а головними цілями атак є викрадення конфіденційних даних і виведення з ладу інформаційних ресурсів [12]. У міжнародному рейтингу з кібербезпеки Global Cybersecurity Index [13] Україна має свої слабкі місця, що вказує на необхідність підвищення готовності до кіберзагроз (рис. 1).

Одна з найсильніших позицій України – рівень технічних заходів (17,35 бали), що свідчить про достатній рівень технічної готовності, оскільки Україна має активний національний CERT-UA, функціонуючі сектори кіберзахисту в органах державної влади, впроваджені технічні стандарти, а також налагоджену взаємодію з міжнародними кіберцентрами. У цьому напрямі Україна перевищує середньорегіональний рівень і демонструє високу адаптивність у відповідь на безпрецедентну кількість атак. Саме технічні спроможності дозволили забезпечити неперервність роботи ключових державних платформ (Дія, реєстри Мін'юсту, Кабміну тощо). Однак проблема полягає в тому, що технічні спроможності залишаються зосередженими на центральному рівні. Натомість місцеві громади не мають власних CISO або технічних команд, не проводять системні сканування вразливостей, користуються застарілими серверами та програмами, часто мають неконтрольований доступ до критичних даних, що створює "точки входу" для атак через слабкі інституції.

Середній рівень організаційних заходів, оцінений у 15,97 бали, підкреслює наявність стратегічних документів, але слабку інституційну реалізацію. Україна має національну стратегію кібербезпеки, урядові центри

Таблиця 1

Порівняння підходів українських авторів до комунікації у публічному управлінні

Автор	Модель / підхід	Ключові риси	Вплив на інформаційну безпеку	Ризики
Бакуменко О. Д. [4, с. 21–28]	Системна комунікація	Узгодження інтересів, горизонтальні зв'язки	Забезпечує цілісність системи	Монополізація потоків
Серьогін С. В. [6]	Інституціональна модель	Інституалізація каналів, роль ОМС	Стабільність комунікаційної інфраструктури	Інформаційні вакууми
Руденко І. [7, с. 59–69]	Мережева цифрова модель	Відкритість, інтерактивність	Оперативність, зворотний зв'язок	Кібератаки, фейки
Євдокимов В., Коломієць С. [8]	Інноваційна модель	Використання цифрових технологій	Аналітика ризиків у реальному часі	Технічні збої, вразливість
Кравченко О. В. [9]	Системно-синергетичний підхід	Самоорганізація, стійкість	Підвищує здатність протистояти зовнішньому тиску	Ефект «каскаду криз»

 ISSN 2310-9653 (Print), 2664-6145 (Online)

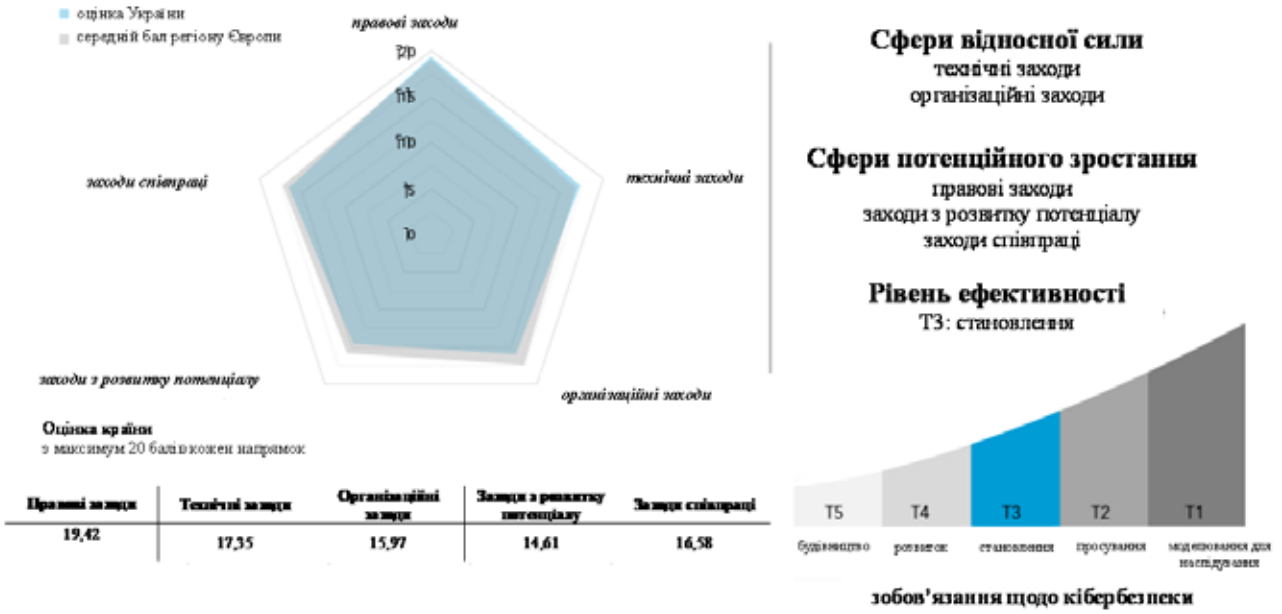

Рис. 1. Аналітика Глобального індексу кібербезпеки (Global Cybersecurity Index, GCI)

Джерело: створено автором за даними [13].

та профільні агентства, що працюють ефективно. Проте організаційна вертикаль залишається недостатньо розвиненою: немає офіційних відповідальних за кібербезпеку на рівні громад; не існує стандартизованої структури інформаційної політики ОМС; система підзвітності та управління ризиками відсутня на більшості локальних рівнів; міжмуніципальна взаємодія є фрагментарною. Таким чином, організаційна спроможність зосереджена на центральному рівні, що суперечить принципам децентралізації та сучасної концепції інформаційної стійкості.

Найнижчий показник серед усіх стовпів – заходи з розвитку потенціалу (14,61 бали), що вказує на ключову структурну вразливість: дефіцит людського капіталу у сфері цифрової та кібербезпеки. Причинами цього є відсутність спеціалізованих навчальних програм для працівників органів місцевого самоврядування, низький рівень цифрової культури, відсутність регулярних тренінгів з комунікаційної безпеки, кризових комунікацій, протидії дезінформації, брак фахівців, особливо в громадах до 50 тисяч населення. Описаний компонент є основною перешкодою для нарощування стійкості, оскільки навіть найсучасніші технічні системи втрачають ефективність без компетентних користувачів.

Середній рівень показника – заходи співпраці (16,58 бали) – свідчить про помірну, але неповну інтегрованість у міжнародні та внутрішні мережі співробітництва. Загалом Україна демонструє високий рівень міжнародної взаємодії (НАТО, ЄС, ITU, FIRST), однак на внутрішньому рівні: міжвідомча координація є нерівномірною, місцеві органи влади часто не залучаються до національних програм кібербезпеки, державно-приватне партнерство у сфері кіберзахисту розвинене обмежено, горизонтальні мережі співпраці між громадами практично відсутні. Таким чином, Україна добре інтегрована в глобальну екосистему кібербезпеки, але слабко – у власну національну.

За результатами аналізу індексу, можна констатувати: сильні сторони України – правові та технічні механізми; слабкі сторони – кадровий потенціал, локальна організаційна спроможність і співпраця на рівні громад. Вищенаведене чітко визначає головний стратегічний виклик: підвищення інформаційної стійкості органів місцевого самоврядування через нарощування людського капіталу, інституційну структуризацію і розвиток партнерств. Саме на цьому слід концентрувати реформі, якщо метою є стійке управління інформаційною безпекою в умовах гібридних загроз.

З 2022 року кількість кіберінцидентів проти українських органів державної влади зросла у понад четверо, а щомісячно фіксується понад 3 000 кібератак на державні сайти та критичну інфраструктуру. Водночас інституційна спроможність місцевих органів влади у сфері інформаційної безпеки залишається низькою: лише 43% громад мають фахівців із цифрової безпеки, а 60% сайтів органів місцевого самоврядування не мають сертифікатів SSL [12]. Проблема загострюється на фоні глобального цифрового розриву: за індексом кібербезпеки ITU (2024) Україна посідає 46-те місце серед 194 країн, тоді як Польща – 28-те, Естонія – 10-те, а США – 5-те.

Україна значно поступається європейським державам у питаннях системного управління інформаційною безпекою, зокрема на муніципальному рівні. Вразливість місцевих систем посилює ризики втручання у дані населення, підміни інформації та деструктивних інформаційних впливів на громади.Проблема інформаційної безпеки

в органах місцевого самоврядування України має системний і стратегічний характер. Наявність високого рівня загроз при низькій цифровій спроможності органів влади створює ризик підриву довіри громадян до держави.

Розв'язання потребує не лише технологічного, а й управлінського підходу: формування комунікаційної культури безпеки, інтеграції систем кіберзахисту на місцевому рівні та розвитку людського потенціалу, що відображено в структурно-аналітичній моделі впливу лінійних, інтерактивних і мережевих комунікаційних моделей на інформаційну стійкість ОМС (рис. 2).

Представлена аналітична модель демонструє необхідність інтеграції сучасних комунікаційних моделей у систему публічного управління органів місцевого самоврядування так, щоб вони сприяли підвищенню інформаційної стійкості, були здатні протистояти зовнішнім та внутрішнім інформаційним загрозам і забезпечували стабільність та ефективність функціонування місцевих владних інституцій у цифрову добу, що потребує гібридної комунікаційної системи з надійними каналами, інтерактивністю, адаптацією до аудиторії та власними фільтрами достовірності.

На основі аналізу складових індексу GCI ідентифіковано, що інформаційна стійкість українських громад може бути суттєво посилена через перебудову комунікаційних моделей, які мають статиформалізованими (правові механізми),технологічно захищеними (технічні механізми), інституційно закріпленими (організаційні механізми), кадрово-забезпеченими (розвиток потенціалу), та мережевими (співпраця).Таким чином, саме комунікація – не технології й не правові норми – є центральним елементом, що перетворює окремі заходи на цілісну систему інформаційної стійкості громад, важливим при цьому є формування потужної системи комунікаційної безпеки для забезпечення інформаційної стійкості органів місцевого самоврядування (рис. 3).

Концепція підвищення інформаційної стійкості ОМС через удосконалення комунікаційних моделей демонструє комплексний і системний характер, оскільки поєднує правові, технічні, організаційні та кадрові механізми в єдину логічну структуру.

Такий підхід дозволяє уникнути фрагментарності у впровадженні рішень і створює цілісне інформаційне середовище громади, що підвищує її здатність реагувати на загрози. Орієнтація моделі на комунікаційні процеси та їхню безпеку робить її сучасним інструментом розвитку інформаційної стійкості, оскільки акценти зміщено з технологій на управління інформаційними потоками, регламентацію взаємодії та контроль за достовірністю поширюваних даних. Значною перевагою виступає інституціоналізація комунікаційної діяльності на рівні громад.

Формалізація ролей, процедур і політик забезпечує передбачувану та керовану поведінку органів влади під час інформаційних інцидентів. Чіткий нормативний каркас усуває хаотичність дій, підвищує відповідальність посадових осіб і сприяє впровадженню єдиних стандартів роботи з інформацією. У поєднанні з технічною компонентною модель створює захищену комунікаційну інфраструктуру, що мінімізує ризики атак через вразливі канали, підвищує контроль за доступами та забезпечує безпечний обмін даними між підрозділами ОМС, центральними структурами та громадянами.

Організаційна складова формує нову вертикаль управління комунікаційною безпекою. Налагоджена внутрішня координація, визначеність відповідальних осіб, створення комунікаційних центрів та уніфікація каналів дозволяють громадам працювати узгоджено і швидко реагувати на загрози будь-якого масштабу. Така інституційна структурованість формує "єдиний голос громади", що зменшує ризики суперечливих повідомлень, інформаційного хаосу та втрати довіри.

Особливу увагу приділено людському фактору, який традиційно є найбільш вразливим елементом системи безпеки. Завдяки навчальним програмам, тренінгам, симуляціям кризових ситуацій і підвищенню кваліфікації працівників підсилюється кадрова спроможність громад діяти у складних інформаційних умовах.

Підготовлений персонал володіє навичками безпечної комунікації, здатністю розпізнавати інформаційні загрози та застосовувати ефективні моделі взаємодії з громадянами, медіа та міжвідомчими партнерами.

Важливою перевагою є розвиток горизонтальної співпраці між громадами, яка створює передумови для формування мережевої системи колективної інформаційної оборони. Обмін досвідом, спільна реакція на інциденти, використання єдиних стандартів і взаємний моніторинг забезпечують синергію, якої неможливо досягти окремими зусиллями. Такий мережевий підхід посилює здатність громад ефективно протистояти дезінформаційним кампаніям і координувати власні дії у кризових умовах.

Практична орієнтація концепції створює умови для її безпосереднього впровадження в діяльність ОМС. Конкретизовані дії, визначені виконавці, чіткі процедури й інституційні механізми дозволяють громадам керуватися не загальними рекомендаціями, а практичними інструментами, здатними забезпечити швидкий і вимірюваний результат. Така прикладна спрямованість значно підвищує керованість інформаційного простору громади, зменшує хаотичність у комунікаціях та дозволяє своєчасно нейтралізувати загрози.

Глибока інтеграція моделі в контекст гібридних загроз забезпечує її адаптованість до сучасних українських реалій. Реагування на інформаційні атаки, зміцнення стійкості комунікаційних каналів та мінімізація ризиків маніпуляцій формують основу інформаційної оборони на місцевому рівні. У результаті підвищується рівень

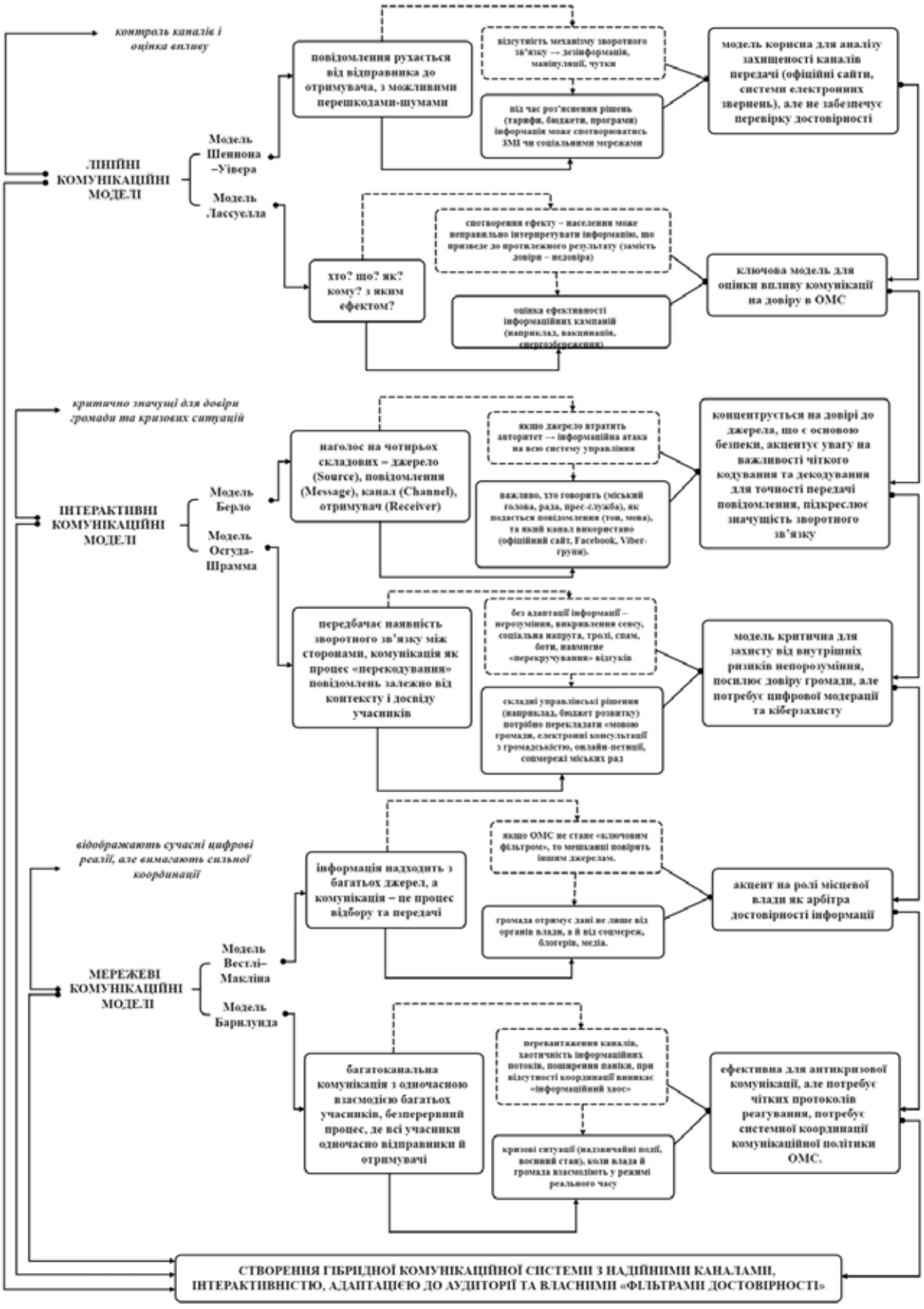

Рис. 2. Структурно-аналітична модель впливу лінійних, інтерактивних і мережевих комунікаційних моделей на інформаційну стійкість ОМС

Джерело: розроблено автором на основі проведеного дослідження.

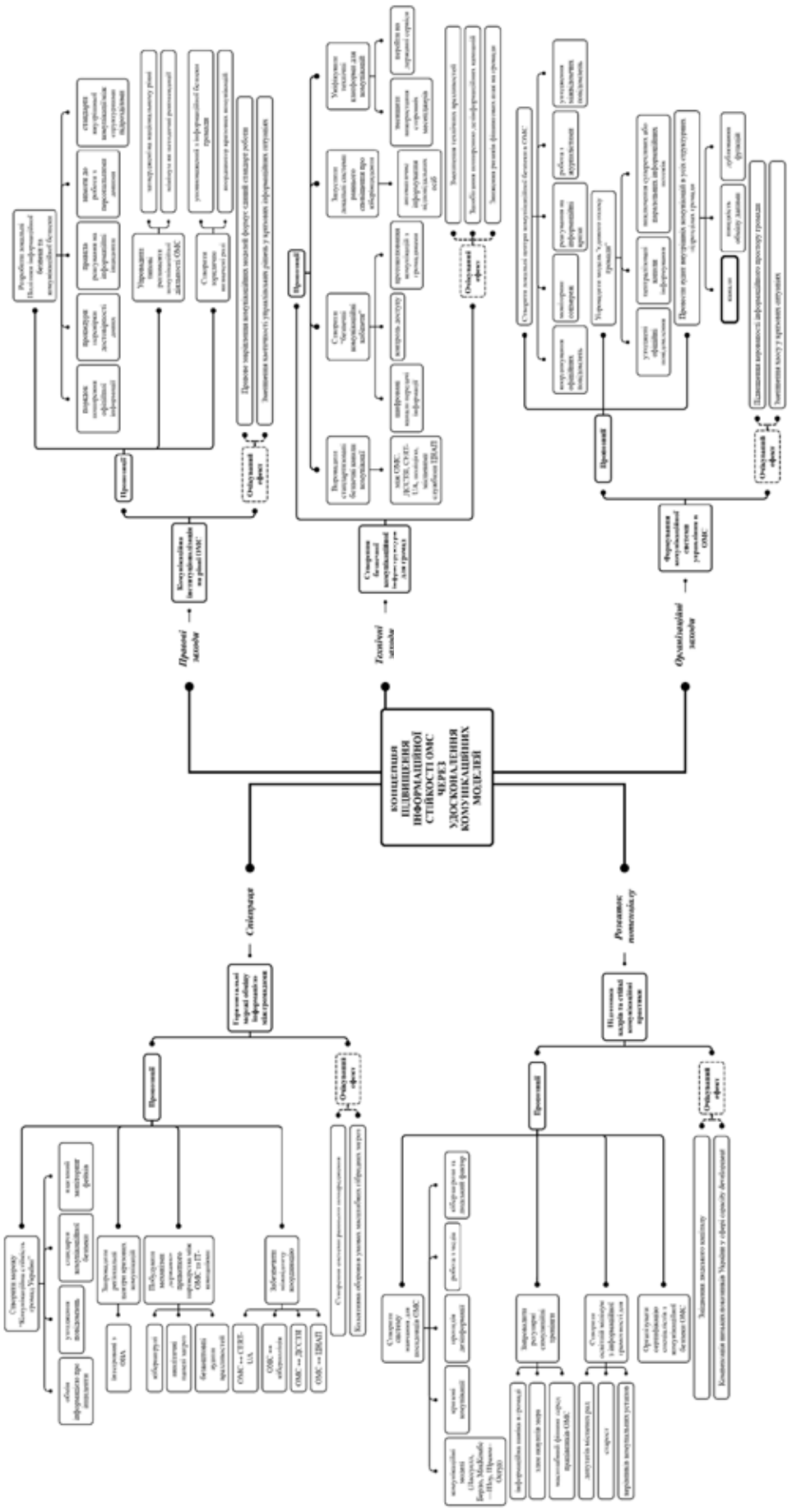

Рис. 3. Концепція підвищення інформаційної стійкості ОМС через удосконалення комунікаційних моделей

Джерело: авторська розробка.

ISSN 2310-9653 (Print), 2664-6145 (Online)

довіри громадян до місцевої влади, скорочується час реагування на кризові ситуації, зміцнюється цифрова зрілість і зростає загальна інформаційна стійкість громади.

Висновки з дослідження і перспективи подальших розвідок у цьому напрямі. Проведене дослідження засвідчило, що комунікаційні моделі відіграють визначальну роль у формуванні інформаційної стійкості органів місцевого самоврядування, оскільки саме вони забезпечують керованість інформаційних потоків, своєчасність реагування, достовірність повідомлень і зворотний зв'язок із громадою. Аналіз лінійних, інтерактивних і мережевих моделей показав, що кожна з них має власні сильні сторони та обмеження, а відтак потребує інтегрованого використання. Лінійні моделі є ефективними для офіційного повідомлення та кризового інформування, проте недостатні для перевірки достовірності інформації. Інтерактивні моделі забезпечують взаємодію та довіру, але залежать від авторитету джерела та цифрової компетентності отримувачів. Мережеві моделі найбільш відповідають цифровому середовищу громад, однак потребують сильної модерації та системної координації для запобігання поширенню недостовірних даних.

Порівняльний аналіз національних та міжнародних статистичних індикаторів, зокрема складових Глобального індексу кібербезпеки, виявив дисбаланс між технічними та правовими заходами України, що перебувають на високому рівні, і недостатніми показниками розвитку кадрового потенціалу, організаційної спроможності й міжмуніципальної співпраці. Така нерівномірність безпосередньо впливає на стійкість комунікаційних процесів в ОМС, ускладнюючи захист інформаційних каналів, кризове реагування та управління довірою під час інформаційних атак. Запропонована аналітична модель дозволила системно оцінити можливості й ризики кожної групи комунікаційних моделей та визначити оптимальну конфігурацію для гібридного застосування в громадах. Для підвищення інформаційної стійкості органів місцевого самоврядування доцільно зосередити управлінські зусилля на розбудові цілісної комунікаційної політики, яка включає стандарти кризового інформування, протоколи взаємодії між підрозділами, впровадження фільтрів достовірності та інформаційної модерації, посилення цифрової інфраструктури, розвиток компетентностей працівників та інституціоналізацію функцій комунікаційної безпеки. Поглиблення міжмуніципальної співпраці, створення локальних центрів комунікаційної координації та системна інтеграція громад у національну екосистему кіберзахисту сприятимуть зміцненню довіри, підвищенню керованості інформаційного простору та стійкості місцевого самоврядування до гібридних і цифрових загроз.

Список використаних джерел:

1. Shannon C., Weaver W. The Mathematical Theory of Communication. Urbana: University of Illinois Press, 1949. URL: https://people.math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf

2. Головатий М. Ф., Романенко Є. О. Політика: Реальність і гра: монографія. Київ: Міжрегіональна Академія управління персоналом, 2021. 288 с. UPL: https://vadnd.org.ua/app/uploads/2021/04/mono.pdf

3. Бараболя В. Комунікація між владою та громадою в територіальних громадах України: виклики війни, децентралізації та шляхи інституційної реалізації. *Науковий часопис Українського державного університету імені Михайла Драгоманова. Серія 22: Політичні науки та методика викладання соціально-політичних дисциплін*: збірник наукових праць / відп. ред. О. В. Бабкіна. Київ: Вид-во УДУ імені Михайла Драгоманова, 2025. Вип. 37. С. 72–83. URL: https://doi.org/10.31392/UDU-nc.series22.2025.37.07

4. Бакуменко В. Д., Попов С. А. Парадигма інноваційного розвитку суспільства: сучасні концепції реформування публічного управління. *Ефективність державного управління*. 2015. Вип. 43. С. 21–28. URL: http://nbuv.gov.ua/UJRN/efdu_2015_43_4.

5. Шпекторенко І. В. Комунікації в публічному управлінні : навч. посіб. / Нац. техн. ун-т «Дніпровська політехніка». Дніпро: НТУ «ДП», 2024. 85 с. URL: https://surl.li/tkuexz

6. Серьогін С. Професіоналізм керівників органів влади. *Публічне адміністрування: теорія та практика*. 2014. Вип. 2. URL: http://nbuv.gov.ua/UJRN/Patp_2014_2_21

7. Руденко І. С. Цифрова трансформація публічного управління: комунікаційні механізми, етичні виклики та нормативне регулювання. *Сучасний науковий журнал.* 2025. (7(1). С. 59–69. URL: https://doi.org/10.36994/2786-9008-2025-7-7

8. Євдокимов В., Коломієць С. Цифрова трансформація публічного управління: виклики та перспективи. *Актуальні питання у сучасній науці. Серія Державне управління. 2*024. № 9 (27) URL: https://elibrary.ru/item.asp?id=74102870

9. Кравченко О. В. Інноваційні механізми публічного управління інформаційними потоками на засадах реформування територіальної організації влади. Дис., спец. 281 «Публічне управління та адміністрування». Маріуполь. 2021. URL: https://mu.edu.ua/storage/MSU/pages/specrady/%D0%94%D0%A4% 2011.107.005%20%D0%9A%D1%80%D0%B0%D0%B2%D1%87%D0%B5%D0%BD%D0%BA%D0%BE/%D0%94%D0%B8%D1%81%D0%B5%D1%80%D1%82%D0%B0%D1%86%D1%96%D1%8F.pdf

10. Стан цифрових технологій в Україні у 2024 році. *Цифровий 2024: Україна.* URL: https://datareportal.com/reports/digital-2024-ukraine?utm_source=chatgpt.com

11. Як повномасштабна війна відобразилася на кількості інтернет-користувачів в Україні. *Слово і діло.* 2024. 15 квітня. URL: https://www.slovoidilo.ua/2024/04/15/infografika/suspilstvo/yak-povnomasshtabna-vijna-vidobrazylasya-kilkosti-internet-korystuvachiv-ukrayini?utm_source=chatgpt.com

12. CERT-UA минулого року опрацювала 4315 кіберінцидентів / Державна служби спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv.

13. Global Cybersecurity Index (GCI). International Telecommunication Union 2025. URL: https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

References:

1. Shannon, C., Weaver, W. (1949). The Mathematical Theory of Communication, University of Illinois Press, Urbana. Available at: https://people.math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf

2. Holovatyi, M. F., Romanenko, Ye. O. (2021). Polityka: real′nist′ i hra: monohrafiya [Politics: reality and game: monograph], Mizhrrehional′na akademiya upravlinnya personalom, Kyiv, 276 p. Retrieved from: https://vadnd.org.ua/app/uploads/2021/04/mono.pdf [in Ukrainian].

3. Barabolia, V. (2025). Komunikatsiya mizh vladoyu ta hromadoyu v terytorial′nykh hromadakh Ukrayiny: vyklyky viyny, detsentralizatsiyi ta shlyakhy instytutsiynoyi realizatsiyi [Communication between authorities and communities in territorial communities of Ukraine: challenges of war, decentralization and ways of institutional implementation], *Naukovyi chasopys Ukrayins'koho derzhavnoho universytetu imeni Mykhayla Drahomanova. Seriya 22: Politychni nauky ta metodyka vykladannya sotsial'no-politychnykh dystsyplin*, Vol. 37, pp. 72–83. https://doi.org/10.31392/UDU-nc.series22.2025.37.07 [in Ukrainian].

4. Bakumenko, V. D., Popov, S. A. (2015). Paradyhma innovatsiynoho rozvytku suspil′stva:suchasni kontseptsiyi reformuvannya publichnoho upravlinnya [Paradigm of innovative development of society: modern concepts of public administration reform], *Efektyvnist' derzhavnoho upravlinnya,* Vol. 43, pp. 21–28. Retrieved from: http://nbuv.gov.ua/UJRN/efdu_2015_43_4 [in Ukrainian].

5. Shpektorenko, I. V. (2024). Komunikatsiyi v publichnomu upravlinni : navch. posib [Communications in public administration: teaching aids]. National Technical University "Dnipro Polytechnic". NTU "DP". Dnipro. 85 p. Retrieved from: https://surl.li/tkuexz. [in Ukrainian].

6. Ser′ohin, S. (2014), Profesionalizm kerivnykiv orhaniv vlady [Professionalism of heads of public authorities], *Publichne administruvannya: teoriya ta praktyka,* Vol. 2. Retrieved from: http://nbuv.gov.ua/UJRN/Patp_2014_2_21 [in Ukrainian].

7. Rudenko, I. S. (2025). Tsyfrova transformatsiya publichnoho upravlinnya: komunikatsiyni mekhanizmy, etychni vyklyky ta normatyvne rehulyuvannya [Digital transformation of public administration: communication mechanisms, ethical challenges and regulatory framework], *Suchasnyi naukovy zhurnal*, Vol. 7(1), pp. 59–69. https://doi.org/10.36994/2786-9008-2025-7-7 [in Ukrainian].

8. Yevdokymov, V., Kolomiyets, S. (2024). Tsyfrova transformatsiya publichnoho upravlinnya: vyklyky ta perspektyvy [Digital transformation of public administration: challenges and prospects], *Aktual'ni pytannya u suchasniy nautsi. Seriya «Derzhavne upravlinnya»*, No. 9(27). Retrieved from: https://elibrary.ru/item.asp?id=74102870 [in Ukrainian].

9. Kravchenko, O. V. (2021). Innovatsiyni mekhanizmy publichnoho upravlinnya informatsiynymy potokamy na zasadakh reformuvannya terytorial′noyi orhanizatsiyi vlady [Innovative mechanisms of public management of information flows on the basis of reforming the territorial organization of power], Dissertation, Speciality 281 «Publichne upravlinnya ta administruvannya», Mariupol′, 2021. Retrieved from: https://mu.edu.ua/storage/MSU/pages/specrady/%D0%94%D0%A4%2011.107.005%20%D0%9A%D1%80%D0%B0%D0%B2%D1%87%D0%B5%D0%BD%D0%BA%D0%BE/%D0%94%D0%B8%D1%81%D0%B5%D1%80%D1%82%D0%B0%D1%86%D1%96%D1%8F.pdf [Ukraine]

10. DataReportal (2024). Tsyfrovyi 2024: Ukrayina. Stan tsyfrovykh tekhnolohiy v Ukrayini u 2024 rotsi [Digital 2024: Ukraine. The state of digital technologies in Ukraine in 2024]. Retrieved from: https://datareportal.com/reports/digital-2024-ukraine?utm_source=chatgpt.com [in Ukrainian].

11. Slovo i dilo (2024). Yak povnomasshtabna viyna vidobrazylasya na kil′kosti internet-korystuvachiv v Ukrayini [How the full-scale war affected the number of Internet users in Ukraine], 15 April. Retrieved from: https://www.slovoidilo.ua/2024/04/15/infografika/suspilstvo/yak-povnomasshtabna-vijna-vidobrazylasya-kilkosti-internet-korystuvachiv-ukrayini?utm_source=chatgpt.com [in Ukrainian].

12. Derzhavna sluzhba spetsial′noho zv′yazku ta zakhystu informatsiyi Ukrayiny (2024), CERT-UA mynuloho roku opratsyuvala 4315 kiberintsydentiv [CERT-UA processed 4315 cyber incidents last year]. Retrieved from: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv [in Ukrainian].

13. International Telecommunication Union (2025). Global Cybersecurity Index (GCI), ITU, Geneva. Retrieved from: https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

Дата надходження статті: 08.11.2025
Дата прийняття статті: 10.12.2025
Опубліковано: 30.12.2025