

Supreme Court are analyzed in terms of understanding the concept and content of "intrusion into a dwelling, other premises, or storage facility." Problematic issues observed during the consideration of specific cases are highlighted. The positions and emphases made by law enforcement officials when providing a judicial interpretation of the qualifying circumstance of "trespassing into a dwelling, other premises, or storage facility" are presented. The conclusion is that the concept of trespassing should be formed based on its objective and subjective characteristics. Thus, intrusions must occur in a dwelling, other premises, or storage facility to which there is no free access and where the person has no legal right to be. In addition, intrusion is possible only in objects that have the characteristics of a dwelling, other premises, or a storage facility. By committing an intrusion, a person pursues mercenary motives to take possession of someone else's property.

Keywords: theft, intrusion into a dwelling, other premises or storage facility, qualifying feature, mercenary motive, person.

Стаття надійшла до редакції / Received 15.10.2025

Прийнята до друку / Accepted 02.11.2025

Бібліографічний опис статті:

Шинкарьов Ю.В. Щодо розуміння поняття «проникнення у житло, інше приміщення чи сховище» у контексті ч. 3 ст. 185 Кримінального кодексу України. Актуальні проблеми інноваційної економіки та права. 2025. № 6. С. 6-9.

Shinkarov Y.V. On the understanding of "breaking into a dwelling, other premises or storage facility" in the context of Part 3 of Article 185 of the Criminal Code of Ukraine. Actual problems of innovative economy and law. 2025. No. 6, pp. 6-9.

УДК: 351.077:004.9:005.334:352; JEL Classification: R58, H70, H83, D83
DOI: <https://doi.org/10.36887/2524-0455-2025-6-2>

ХАНДОГА Юрій Васильович, аспірант кафедри публічного управління та адміністрування Карпатського національного університету імені Василя Стефаника, <https://orcid.org/0009-0005-5944-7530>
ДРАБЧУК Наталія Юрївна, доктор філософії (PhD) за спеціальністю 051 Економіка, асистент кафедри публічного управління та адміністрування Карпатського національного університету імені Василя Стефаника, <https://orcid.org/0000-0001-5965-9959>

УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕХАНІЗМІВ СТРАТЕГІЧНОГО УПРАВЛІННЯ РИЗИКАМИ В СИСТЕМІ ТЕРИТОРІАЛЬНИХ ГРОМАД

Хандога Ю.В., Драбчук Н.Ю. Удосконалення інформаційно-комунікаційних механізмів стратегічного управління ризиками в системі територіальних громад.

У статті розкрито актуальність удосконалення інформаційно-комунікаційних механізмів стратегічного управління ризиками на рівні територіальних громад в умовах соціальної турбулентності, зовнішньої воєнної загрози та зростання внутрішніх системних ризиків. Обґрунтовано, що ефективність стратегічного управління в громадах безпосередньо залежить від здатності органів місцевого самоврядування забезпечувати безперервний обмін даними, прозору координацію суб'єктів управління, оперативну ідентифікацію загроз і прийняття обґрунтованих рішень. Водночас акцентовано, що цифровізація комунікаційних процесів поряд із можливостями формує нові вразливості, пов'язані з кіберризиками, дезінформацією, недостатньою довірою до офіційних джерел, фрагментарністю цифрової інфраструктури та обмеженими цифровими компетентностями населення і персоналу ОМС. Систематизовано ключові загрози функціонування інформаційно-комунікаційних механізмів у стратегічному управлінні ризиками територіальних громад, зокрема: роз'єднаність інформаційних ресурсів і відсутність інтегрованої системи управління даними; низьку якість, неповноту та невчасність інформації для стратегічного аналізу; уразливість IT-інфраструктури та дефіцит політичк кібербезпеки; недобіру населення та слабкість каналів зворотного зв'язку; цифрову нерівність як бар'єр участі; інформаційні атаки, маніпуляції та поширення фейкових повідомлень у гібридному середовищі. Доведено, що ігнорування зазначених загроз призводить до викривлення ризикового профілю громади, зниження керованості кризовими ситуаціями, дезорганізації дій та зростання соціальної напруги. Окреслено пріоритетні напрями вдосконалення інформаційно-комунікаційних механізмів управління ризиками: інституційне закріплення цифрової інфраструктури та створення єдиної платформи управління ризиками з інтеграцією даних і міжвідомчою взаємодією; формування стійких об'єднаних каналів комунікації з населенням; підвищення компетентностей працівників ОМС у сфері кризових комунікацій і цифрової гігієни; нормативне унормування цифрової взаємодії в умовах ризиків; розвиток міжгромадських комунікаційних альянсів і інтеграція ризик-менеджменту в стратегічне планування.

Ключові слова: стратегічне управління, ризики, публічне управління, територіальні громади, інформаційно-комунікаційні механізми, механізми, цифровізація, органи місцевого самоврядування, сталий розвиток, комунікація.

Постановка проблеми у загальному вигляді. У сучасних умовах соціальної турбулентності, зовнішньої воєнної загрози та зростання внутрішніх системних ризиків надзвичайно важливо забезпечити ефективне стратегічне управління на рівні територіальних громад. Однією з ключових складових такої системи є налагоджений інформаційно-комунікаційний механізм, що забезпечує безперервний обмін даними, прозору взаємодію всіх суб'єктів управління, оперативну ідентифікацію загроз та прийняття обґрунтованих рішень. Проте на сьогодні у більшості українських громад відсутні чітко регламентовані інструменти комунікації в управлінні ризиками, а також системи збору, обробки та поширення релевантної інформації, що значно знижує якість реагування на критичні виклики.

Впровадження інформаційно-комунікаційних механізмів несе в собі не лише можливості, а й нові вразливості. Розбудова цифрової інфраструктури, інтеграція сучасних IT-рішень, формування каналів зворотного зв'язку – усе це створює складне середовище, яке вимагає високого рівня безпеки, довіри, технічної грамотності та політичної зрілості. Без належного аналізу потенційних загроз ці механізми можуть стати джерелом дезорганізації, паніки або навіть об'єктами цілеспрямованих атак.

Аналіз останніх досліджень і публікацій. Питаннями стратегічного управління ризиками та розвитком територіальними громадами займаються низка науковців, зокрема: О. Бортнік [1], В. Баранова,

К. Дворник [2], В. Дикань, І. Посохов [3], С. Богуславська, Ю. Бондар, С. Фесун [4], Н. Пилипів [5] О. Жук та ін. [6–8], Н. Керецман та ін. [9], Г. Олексюк, Н. Попадонець [10], Л. Захаркіна та ін. [11] та ін. Однак на сьогодні залишається відкритим питання рівня розкриття інформаційно-комунікаційних механізмів стратегічного управління ризиками в системі територіальних громад.

Формулювання цілей статті (постановка завдання). Метою статті є теоретико-методичне обґрунтування напрямів удосконалення інформаційно-комунікаційних механізмів стратегічного управління ризиками в системі територіальних громад.

Виклад основного матеріалу дослідження. Вивчення загроз, що супроводжують функціонування інформаційно-комунікаційних механізмів стратегічного управління ризиками в системі територіальних громад, є вкрай важливим і своєчасним. Визначення таких загроз (рис. 1) дозволить не лише посилити безпеку громад, а й розробити превентивні інструменти адаптації та реагування, які базуються на реаліях українського сьогодення.

Однією з головних загроз для ефективного функціонування інформаційно-комунікаційних механізмів у стратегічному управлінні ризиками є фрагментарність інформаційних ресурсів та відсутність єдиної інтегрованої цифрової системи управління даними в межах територіальної громади. Часто різні підрозділи місцевого самоврядування, комунальні підприємства та партнери (освітні, медичні, соціальні установи) користуються різними платформами, неузгодженими базами даних,

архівними таблицями або паперовими звітами. Така роз'єднаність призводить до дублювання інформації, втрати актуальності, невідповідності форматів, а головне – унеможлиблює системну оцінку ризиків та прийняття оперативних рішень. Відсутність автоматизованого обміну даними між основними службами знижує ефективність управлінських дій, особливо в умовах надзвичайних ситуацій або непередбачуваних викликів.

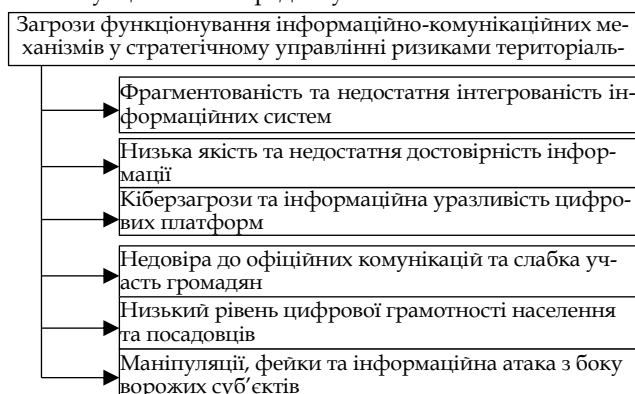


Рис. 1. Загрози функціонування інформаційно-комунікаційних механізмів у стратегічному управлінні ризиками територіальних громад.

Джерело: розробка автора

Ще однією критичною загрозою є низька якість інформації, яка використовується для стратегічного аналізу ризиків. У багатьох територіальних громадах відсутні чіткі стандарти збору, перевірки та оновлення даних. У результаті дані можуть бути застарілими, неповними, суперечливими або суб'єктивно інтерпретованими. Часто не проводиться належна верифікація джерел інформації, що підвищує ймовірність помилок, маніпуляцій або навмисного викривлення ситуації. Застарілі способи обліку (наприклад, ведення звітності у паперовому форматі або у невідключених Excel-файлах) ускладнюють цифрову трансформацію та створюють прогалини у системі. Така ситуація призводить до викривлення ризикового профілю громади, а отже – до неправильних стратегічних пріоритетів, непродуктивних бюджетних витрат або неефективного реагування у кризових ситуаціях.

У сучасних умовах зростає роль кібербезпеки як ключового елементу стабільності інформаційно-комунікаційної системи управління ризиками. Територіальні громади, особливо в умовах воєнного стану чи гібридної агресії, стають об'єктами кібератак, спроб викрадення інформації, дезінформаційних кампаній та знищення даних. Низький рівень захищеності IT-інфраструктури, відсутність фахових IT-кадрів, відкладене впровадження політик кібербезпеки та слабка інтеграція з державними системами безпеки створюють вразливе цифрове середовище [4]. Крім того, збої в роботі платформ, віруси, втрати даних через недотримання правил резервного копіювання – усе це підвищує ризик «паралічу» інформаційної системи в критичний момент. Тому громади, які активно диджиталізуються, мають одночасно інвестувати у захист своїх інформаційних активів, підготовку персоналу та побудову алгоритмів дій на випадок кіберінцидентів.

Інформаційно-комунікаційна складова управління ризиками може зазнати серйозних втрат у результаті низького рівня довіри населення до органів місцевого самоврядування та офіційної інформації. У разі, коли мешканці вважають, що влада приховує проблеми, маніпулює даними або діє не в інтересах громади – ефективність будь-яких комунікаційних заходів суттєво знижується. Люди не реагують на повідомлення, не беруть участі в опитуваннях, ігнорують громадські обговорення, відмовляються ділитися даними чи вносити свої пропозиції до стратегій. До цього призводять непрозорість управління, відсутність системи зворотного зв'язку,

формальний характер участі громадськості у прийнятті рішень. Особливо це критично в умовах швидкозмінних загроз, де колективна відповідальність та оперативна реакція населення можуть суттєво знизити рівень збитків або навіть врятувати життя. Таким чином, будь-яка недовіра перетворюється на комунікаційний бар'єр, який шкодить загальній стійкості громади.

Цифрова нерівність – ще один фактор, що становить серйозну загрозу для функціонування інформаційно-комунікаційних механізмів. Значна частина мешканців територіальних громад, особливо людей старшого віку, представників соціально вразливих груп або жителів сільської місцевості, не має навичок роботи з цифровими сервісами, не користується електронними формами участі або просто не довіряє їм [6]. Водночас деякі посадовці в органах місцевого самоврядування, попри наявність доступу до IT-рішень, не використовують їх ефективно або бояться відповідальності за дії в цифровому просторі. Це уповільнює процеси цифровізації управління ризиками, обмежує потенціал аналітики та обміну даними. Поширення інформації у цифровому форматі не досягає своєї цільової аудиторії, а механізми реагування втрачають актуальність через брак розуміння серед мешканців, як саме вони мають діяти у кризовій ситуації.

У ситуації гібридної війни або політичної нестабільності загрозою є поширення фейкової, викривленої або навмисно маніпулятивної інформації про події, ризики, діяльність органів влади. Ворог може використовувати місцеві інформаційні канали для дестабілізації ситуації в громадах, посіву паніки або недовіри, дискредитації рішень влади, провокування міжгромадських конфліктів. Особливо небезпечними є атаки на офіційні сайти, сторінки в соцмережах, підміна повідомлень системи оповіщення або фішингові кампанії проти посадовців [11]. Такі явища потребують оперативної реакції та готовності до стратегічної інформаційної протидії – чітко розроблених протоколів публічного спростування, прозорих звітів, співпраці з журналістами та лідерами думок, використання інструментів моніторингу інформаційного простору.

Інформаційно-комунікаційні механізми, попри їхній потенціал як потужного інструменту управління ризиками, є вразливими до низки загроз, що можуть нівелювати їхню ефективність. Ігнорування цих загроз з боку місцевої влади призводить до втрати контролю над кризовими ситуаціями, дезорганізації дій, зниження соціальної згуртованості та недовіри до органів влади. Тому їх своєчасне виявлення, аналіз і системна робота над їхнім подоланням повинні стати пріоритетом у формуванні стратегій ризик-менеджменту в кожній територіальній громаді України.

Визначивши основні загрози для інформаційно-комунікаційних механізмів стратегічного управління ризиками, варто акцентувати увагу на необхідності впровадження структурованої та стійкої інфраструктури, здатної забезпечити безпечний і ефективний обіг критично важливої інформації. Слабкість комунікацій, фрагментарність цифрової інфраструктури та недостатній рівень взаємодії між органами місцевого самоврядування, службами цивільного захисту та громадськістю можуть істотно обмежити ефективність навіть найкращих стратегічних ініціатив. Саме тому визначення ключових напрямів удосконалення інформаційно-комунікаційних механізмів стратегічного управління ризиками (рис. 2) є пріоритетом як на рівні окремих територіальних громад, так і в масштабі національної політики безпеки.

Одним із ключових напрямів удосконалення інформаційно-комунікаційних механізмів стратегічного управління ризиками є інституційне закріплення цифрової інфраструктури для збору, обробки, збереження та передачі даних. В умовах зростаючої складності

соціально-економічних процесів та зовнішніх загроз громади мають отримати постійний доступ до надійної, стандартизованої та юридично верифікованої інформації. Для цього необхідно на рівні державної політики затвердити модель єдиної цифрової платформи управління ризиками, яка буде використовувати сучасні

інструменти штучного інтелекту, Big Data та інтеграційні API для обміну даними між різними системами – зокрема, між органами місцевого самоврядування, ЦОБВ, службами цивільного захисту, екологічного моніторингу, поліції, ДСНС тощо.



Рис. 2. Напрями вдосконалення інформаційно-комунікаційних механізмів стратегічного управління ризиками на рівні територіальних громад*. Джерело: розробка автора

Наступний напрям удосконалення – створення стійких каналів двосторонньої комунікації між місцевою владою та населенням. Комунікаційна прозорість є запорукою довіри та ефективного реагування на загрози, особливо у сфері управління ризиками. Залучення мешканців до процесів ідентифікації ризиків, формування рішень та оцінки дій влади має стати нормою. Для цього доцільно впровадити інтерактивні платформи зворотного зв'язку (наприклад, мобільні застосунки, чат-боти, електронні опитування), які дозволятимуть швидко отримувати повідомлення про потенційні загрози, аварії, конфлікти тощо. Водночас важливо забезпечити інформаційну безпеку, верифікацію повідомлень та захист персональних даних учасників комунікації.

Третій стратегічний напрям, який полягає в посиленні компетентностей працівників органів місцевого самоврядування у сфері кризової комунікації та цифрової гігієни, є критично важливим елементом стратегічного управління ризиками. У сучасному середовищі, що характеризується підвищенням рівнем загроз, гібридними викликами, кіберзлочинністю, поширенням фейкової інформації та необхідністю швидкого реагування на кризові ситуації, традиційних управлінських знань вже недостатньо [1]. Працівники органів місцевого самоврядування мають не лише орієнтуватися в нормативно-правовому полі чи вміти планувати місцевий бюджет, але й володіти компетенціями, які дозволяють ефективно діяти в умовах невизначеності, забезпечуючи сталу комунікацію з громадянами та координацію між структурами. Саме тому формування відповідних навичок стає третім стратегічним напрямом удосконалення системи управління ризиками на рівні територіальних громад.

У цьому контексті особливо важливою є організація системного навчання працівників громад. Йдеться не про разові тренінги, а про впровадження регулярних програм підвищення кваліфікації, які включають онлайн-курси з кризової комунікації, тренінги з цифрової безпеки, майстер-класи з протидії дезінформації, а також моделювання кризових сценаріїв з реальними симуляціями. Такі симуляції можуть охоплювати реагування на техногенні аварії, інформаційні атаки, перебої в роботі інфраструктури, кібератаки на бази даних чи навіть організацію евакуації. Завдяки цьому формується не лише компетентність, але й здатність діяти під тиском часу, ухвалювати зважені рішення в умовах інформаційного дефіциту або надлишку.

Не менш важливим кроком є створення внутрішньої системи управління знаннями – так званої knowledge base, яка буде доступною для всіх працівників ОМС у цифровому форматі. Ця база має містити шаблони кризових повідомлень, алгоритми дій у випадку різних типів загроз (від інформаційних інцидентів до природних катастроф), рекомендації щодо комунікації з різними цільовими аудиторіями, приклади найкращих практик інших громад, а також адаптовані стандарти

реагування відповідно до українського та міжнародного досвіду. Система повинна бути живою, тобто постійно оновлюватися на основі нових кейсів, змін у законодавстві чи досвіді, отриманого в ході реальних подій.

Окремий акцент слід зробити на формуванні цифрової гігієни, яка вклучає вміння працівників ОМС безпечно працювати з інформацією, захищати персональні дані, ідентифікувати фішингові повідомлення, дотримуватись протоколів кібербезпеки, користуватись службовими каналами зв'язку, а також проводити цифрову комунікацію з дотриманням етичних та юридичних норм [10]. У поєднанні з кризовими комунікативними навичками це дозволяє зменшити ризик внутрішніх інформаційних витоків, запобігти поширенню паніки серед населення та зберегти довіру до місцевої влади в критичних умовах.

Таким чином, підвищення людського капіталу в системі стратегічного управління ризиками – це не лише технічне питання підготовки кадрів, а фундаментальний виклик формування нової культури управління на рівні територіальних громад. Тільки через постійне навчання, закріплення практичних навичок, обмін досвідом та впровадження сучасних інструментів цифрової комунікації можна досягти високої стійкості громад перед ризиками і забезпечити належну якість стратегічного управління в умовах багатомірних загроз.

Четвертим важливим напрямом стратегічного удосконалення інформаційно-комунікаційних механізмів управління ризиками в територіальних громадах є розробка та впровадження нормативного забезпечення цифрової комунікаційної взаємодії в умовах ризиків. У сучасних умовах цифрової трансформації управлінських процесів гостро постає проблема відсутності єдиного правового підходу до регулювання комунікаційних потоків у кризових ситуаціях. На місцевому рівні в Україні наразі спостерігається фрагментарність і неузгодженість у нормативно-правових актах, що регулюють порядок дій органів місцевого самоврядування у разі виникнення загроз. Це породжує хаос, дублювання повідомлень, або ж, навпаки, – критичну затримку у передачі життєво важливої інформації населенню. У разі виникнення ризиків, зволікання або неузгодженість у діях можуть призвести до катастрофічних наслідків.

Насамперед необхідно унормувати структуру та форматування даних, які використовуються в системах цифрового управління ризиками. Це стосується як внутрішньої документації, так і публічних повідомлень. Уніфіковані форми звітності, протоколи реагування, шаблони повідомлень для громадян дозволять оперативно обмінюватися інформацією між різними рівнями влади та міжвідомчими структурами [3]. Водночас у законодавчому полі має бути чітко визначено перелік інформації, що вважається критичною, правила її класифікації та збереження конфіденційності, а також встановлено рівні доступу до таких даних для працівників різних підрозділів і служб. Це своєю чергою зменшить ризики витоків або маніпуляцій на основі недостовірної інформації.

Ключовим елементом нормативного забезпечення має стати створення єдиних протоколів цифрової взаємодії між структурами, що беруть участь в управлінні ризиками: органами місцевого самоврядування, підрозділами ДСНС, поліції, медичних служб, освітніх закладів, комунальних підприємств та громадських організацій. Такі протоколи повинні регулювати механізми обміну повідомленнями, черговість дій, часові регламенти інформування, відповідальність за оприлюднення недостовірної інформації або її приховування. У кризовий момент навіть кілька хвилин можуть мати вирішальне значення, тому швидкість і чіткість реагування має бути закладена на нормативному рівні.

Не менш важливим аспектом є встановлення вимог до контенту публічних комунікацій, який транслюється населенням через офіційні канали. Законодавство повинно передбачати обов'язкові стандарти мови повідомлень (зрозумілість, лаконічність, уникнення панічних формулювань), їхню періодичність, підтвердження достовірності та механізми зворотного зв'язку. Регламентція цього процесу дозволить уникнути інформаційного вакууму в перші хвилини або години після виникнення ризику, коли громадяни особливо вразливі до паніки або дезінформації. Крім того, це сприятиме підвищенню довіри до місцевої влади як до компетентного та відповідального джерела інформації.

Отже, запровадження нормативної основи для цифрової комунікації в умовах ризиків є необхідною умовою формування сталої моделі стратегічного управління територіальними громадами. Такий підхід дозволить не лише підвищити ефективність реагування на кризові ситуації, а й забезпечити прозорість, відповідальність і координацію дій усіх учасників системи.

П'ятий напрям удосконалення стосується побудови комунікаційних альянсів на міжгромадському, регіональному та національному рівнях. Жодна громада не є повністю самодостатньою в умовах кризи, тому ключовим є формування мереж кооперації, обміну

даними, ресурсами, методиками управління ризиками. Такі альянси можуть функціонувати у формі міжмуніципальних форумів, спільних електронних хабів, платформ для обміну аналітичними звітами та навчальними матеріалами. Розбудова подібної комунікаційної екосистеми дозволить територіальним громадам ефективно взаємодіяти в умовах багатомірних ризиків: від паводків і кібератак до економічних шоків і внутрішньої міграції.

Важливим вектором удосконалення є інтеграція інформаційно-комунікаційних механізмів стратегічного управління ризиками у процес стратегічного планування громад. Зокрема, йдеться про впровадження спеціальних розділів з оцінкою ризиків у стратегічних документах розвитку (стратегії, плани дій, бюджети), формування сценарного моделювання майбутніх загроз, врахування ризиків у бюджетному процесі та процедурах оцінки ефективності управлінських рішень. Інформація, що генерується цифровими системами, повинна безпосередньо впливати на формування політик, а не залишатися лише на рівні інформування.

Таким чином, удосконалення інформаційно-комунікаційних механізмів в управлінні ризиками – це не лише питання технологій, але й зміни культури управління в територіальних громадах, де інформація, відкритість, швидкість реакції та партнерство є запорукою стійкості до сучасних викликів.

Висновки та перспективи подальших досліджень. Отже, вдосконалення інформаційно-комунікаційних механізмів стратегічного управління ризиками на рівні територіальних громад є необхідною передумовою формування сталих, самодостатніх і здатних до відновлення громад. Така система повинна бути відкритою, інтерактивною, технічно оснащеною та заснованою на партнерстві влади, громадян, бізнесу та науковців. Тільки за таких умов стає можливим досягнення реального управління ризиками, а не лише реагування на їхні наслідки.

Література.

1. **Бортнік О.В.** Управління ризиками в органах місцевого самоврядування на основі міжнародних стандартів. *Інвестиції: практика та досвід*. 2021. № 1. С. 141-148. DOI: <https://doi.org/10.32702/2306-6814.2021.1.141>
2. **Баранова В., Дворник К.** Діджиталізація ризик-менеджменту: новий вектор стратегічного успіху та сталого розвитку. *Фінансово-кредитні системи: перспективи розвитку*. 2024. № 2(13). С. 132-144. DOI: <https://doi.org/10.26565/2786-4995-2024-2-12>
3. **Дикань В.Л., Посохов І.М.** Дослідження міжнародних стандартів управління ризиками. *Бізнес Інформ*. 2014. № 1. С. 314-319.
4. **Богуславська С., Бондар Ю., Фесун С.** Теоретико-методологічні основи наукових досліджень ризик-орієнтовного стратегічного управління в умовах цифровізації. *Цифрова економіка та економічна безпека*. 2024. № 3 (12). С. 3-7. DOI: <https://doi.org/10.32782/dees.12-1>
5. **Pylypiv N.I., Piatnychuk I.D., Maksymiv Yu.V.** Ensuring sustainable development of the enterprise by modern tools of strategic management: the concept of business administration. *Theory and Practice of Strategic Management of Industrial and Regional Social Systems*, IFNTUOG, Ivano-Frankivsk, Ukraine. 2017, P. 376-379.
6. **Zhuk O., Hoi N., Lopushynskiy I., Drabchuk N., Matiychyk A.** Innovative mechanisms of public management for sustainable territorial development: digitization, analytics, and communication. *Cadernos de Educação, Tecnologia e Sociedade – CETS (Brazilian Journal of Education, Technology and Society – BRAJETS)* Vol. 17 No. se4 (2024). DOI: <https://doi.org/10.14571/brajets.v17.nse4.219-231>
7. **Жук О.І., Гої Н.В., Драбчук Н.Ю., Матійчук А.В.** Ефективне лідерство як основа впровадження змін у систему публічного управління: ключові компетенції та методи для адаптації до нових викликів. *Актуальні питання у сучасній науці*. 2024. № 12(30). С. 316-327. DOI: [https://doi.org/10.52058/2786-6300-2024-12\(30\)-316-327](https://doi.org/10.52058/2786-6300-2024-12(30)-316-327)
8. **Жук О.І., Гої Н.В., Драбчук Н.Ю., Дудкевич В.І.** Формування дерева цілей як інструмент стратегічного планування у публічному управлінні в умовах цифровізації та повного відновлення України. *Успіхи і досягнення у науці*. 2024. № 10(10). С. 426-436. DOI: [https://doi.org/10.52058/3041-1254-2024-10\(10\)-426-436](https://doi.org/10.52058/3041-1254-2024-10(10)-426-436)
9. **Керецман Н.І., Пітолич М.М., Попадинець Н.М.** Стратегічні пріоритети соціально-економічного розвитку територіальних громад регіону. *Регіональна економіка*. 2023. №3(109). С. 28-39. DOI: <https://doi.org/10.36818/1562-0905-2023-3-3>
10. **Олексюк Г.В., Лисяк Н.М., Попадинець Н.М.** Концептуально-структурні моделі ендogenousного потенціалу об'єднаних територіальних громад як передумова підвищення їх конкурентоспроможності. *Економіка України*. 2019. № 3. С. 52-69.
11. **Захаркіна Л., Захаркін О., Сокол Л.** Цифрові інструменти управління фінансовими ризиками бізнесу в умовах воєнного стану. *Актуальні питання економічних наук*. 2024. № 5. DOI: <https://doi.org/10.5281/zenodo.14190965>

References.

1. **Bortnik, O.V.** (2021). «Risk management in local governments based on international standards». *Investytsii: praktyka ta dosvid*. № 1. pp. 141-148. DOI: <https://doi.org/10.32702/2306-6814.2021.1.141>
2. **Baranova, V., Dvornyk, K.** (2024). «Digitalization of risk management: a new vector of strategic success and sustainable development». *Finansovo-kredytni systemy: perspektyvy rozvytku*. № 2(13). pp. 132-144. DOI: <https://doi.org/10.26565/2786-4995-2024-2-12>
3. **Dykan', V.L., Posokhov, I.M.** (2014). «Research on international risk management standards». *Biznes Inform*. № 1. pp. 314-319.
4. **Bohuslavs'ka, S., Bondar, Yu., Fesun, S.** (2024). «Theoretical and methodological foundations of scientific research on risk-oriented strategic management in the context of digitalization». *Tsyfrova ekonomika ta ekonomichna bezpeka*. № 3 (12). pp. 3-7. DOI: <https://doi.org/10.32782/dees.12-1>
5. **Pylypiv, N.I., Piatnychuk, I.D., Maksymiv Yu.V.** (2017). Ensuring sustainable development of the enterprise by modern tools of strategic management: the concept of business administration. *Theory and Practice of Strategic Management of Industrial and Regional Social Systems*. IFNTUOG. Ivano-Frankivsk. Ukraine.

6. Zhuk, O., Hoi, N., Lopushynskiy, I., Drabchuk, N., Matychyk, A. (2024). «Innovative mechanisms of public management for sustainable territorial development: digitization, analytics, and communication». *Cadernos de Educação, Tecnologia e Sociedade – CETS (Brazilian Journal of Education, Technology and Society – BRAJETS)* Vol. 17 No. se4 (2024). DOI: <https://doi.org/10.14571/brjets.v17.nse4.219-231>.
7. Zhuk, O.I., Hoi, N.V., Drabchuk, N.Yu., Matychyk, A.V. (2024). «Effective leadership as the basis for implementing changes in the public administration system: key competencies and methods for adapting to new challenges». *Aktual'ni pytannia u suchasnyj nauksi*. № 12(30). pp. 316-327. DOI: [https://doi.org/10.52058/2786-6300-2024-12\(30\)-316-327](https://doi.org/10.52058/2786-6300-2024-12(30)-316-327).
8. Zhuk, O.I., Hoi, N.V., Drabchuk, N.Yu., Dudkevych, V.I. (2024). «Formation of a goal tree as a tool for strategic planning in public administration in the context of digitalization and post-war reconstruction of Ukraine». *Uspikhy i dosiahnennia u nauksi*. № 10(10). pp. 426-436. DOI: [https://doi.org/10.52058/3041-1254-2024-10\(10\)-426-436](https://doi.org/10.52058/3041-1254-2024-10(10)-426-436).
9. Keretsman, N.I., Pitiulych, M.M., Popadynets', N.M. (2023). «Strategic priorities of socio-economic development of territorial communities of the region». *Rehional'na ekonomika*. №3(109). pp. 28-39. DOI: <https://doi.org/10.36818/1562-0905-2023-3-3>.
10. Oleksiuk, H.V., Lysiak, N.M., Popadynets', N.M. (2019). «Conceptual and structural models of the endogenous potential of united territorial communities as a prerequisite for increasing their competitiveness». *Ekonomika Ukrainy*. № 3. pp. 52-69.
11. Zakharkina, L., Zakharkin, O., Sokol, L. (2024). «Digital tools for managing financial risks of business under martial law». *Aktual'ni pytannia ekonomichnykh nauk*. № 5. DOI: <https://doi.org/10.5281/zenodo.14190965>.

Abstract.

Khandoha Y., Drabchuk N. Improvement of information and communication mechanisms for strategic risk management in the system of territorial communities.

The article highlights the importance of improving information and communication mechanisms for strategic risk management at the territorial community level amid social turbulence, external military threats, and growing internal systemic risks. It is argued that the effectiveness of strategic management in communities depends directly on local self-government bodies' ability to ensure continuous data exchange, transparent coordination among management entities, prompt threat identification, and informed decision-making. At the same time, digitization of communication processes, along with its opportunities, creates new vulnerabilities related to cyber risks, disinformation, insufficient trust in official sources, fragmentation of digital infrastructure, and limited digital competencies among the population and local government personnel. The key threats to the functioning of information and communication mechanisms in the strategic risk management of local communities have been systematized, in particular: the fragmentation of information resources and the lack of an integrated data management system; the low quality, incompleteness, and untimeliness of information for strategic analysis; the vulnerability of IT infrastructure and the lack of cybersecurity policies; public mistrust and weak feedback channels; digital inequality as a barrier to participation; information attacks, manipulation, and the spread of fake news in a hybrid environment. It has been proven that ignoring these threats distorts the community's risk profile, reduces crisis management capabilities, disrupts action, and increases social tension. Priority areas for improving information and communication risk management mechanisms have been identified: institutional consolidation of digital infrastructure and creation of a unified risk management platform with data integration and interagency interaction; formation of sustainable two-way communication channels with the population; improving the competencies of local government employees in the field of crisis communications and digital hygiene; regulatory standardization of digital interaction in risk conditions; development of inter-community communication alliances and integration of risk management into strategic planning.

Keywords: strategic management, risks, public administration, territorial communities, information and communication mechanisms, sustainable development, mechanisms, digitalization, local self-government bodies, communication.

Стаття надійшла до редакції / Received 12.10.2025

Прийнята до друку / Accepted 01.11.2025

Бібліографічний опис статті:

Хандога Ю.В., Драбчук Н.Ю. Удосконалення інформаційно-комунікаційних механізмів стратегічного управління ризиками в системі територіальних громад. *Актуальні проблеми інноваційної економіки та права*. 2025. № 6. С. 9-13.

Khandoha Y., Drabchuk N. Improvement of information and communication mechanisms for strategic risk management in the system of territorial communities. *Actual problems of innovative economy and law*. 2025. No. 6, pp. 9-13.

УДК: 352.075; JEL Classification: R53, H54, H70, L86

DOI: <https://doi.org/10.36887/2524-0455-2025-6-3>

ІВАСЮТИН Ігор Михайлович, аспірант кафедри публічного управління та адміністрування Карпатського національного університету імені Василя Стефаника, <https://orcid.org/0009-0006-3694-6991>
ЖУК Ольга Іванівна, к.е.н., доцент, завідувач кафедри публічного управління та адміністрування Карпатського національного університету імені Василя Стефаника, <https://orcid.org/0000-0001-8519-5529>

УДОСКОНАЛЕННЯ ІНФРАСТРУКТУРИ ІНФОРМАЦІЙНО-КОМУНІКАТИВНОГО ЗАБЕЗПЕЧЕННЯ УПРАВЛІННЯ ТЕРИТОРІАЛЬНОЮ ГРОМАДОЮ

Івасютин І.М., Жук О.І. Удосконалення інфраструктури інформаційно-комунікативного забезпечення управління територіальною громадою.

У статті досліджено теоретичні та прикладні аспекти розвитку інфраструктури інформаційно-комунікативного забезпечення системи управління територіальною громадою як ключового чинника модернізації місцевого самоврядування в умовах цифровізації, воєнних загроз і децентралізаційних трансформацій. Обґрунтовано, що перехід від фрагментарного використання інформаційних технологій до формування інтегрованої цифрової інфраструктури є необхідною передумовою підвищення ефективності управлінських рішень, прозорості діяльності органів місцевого самоврядування та розширення участі мешканців у процесах формування і реалізації місцевої політики. Розкрито сутність та структуру інфраструктури інформаційно-комунікативного забезпечення управління громадою, визначено її організаційну, технічну та функціональну складові. Особливу увагу приділено ролі цифрового менеджера як стратегічного координатора процесів цифрової трансформації, відповідального за розвиток електронних сервісів, управління IT-інфраструктурою, забезпечення кібербезпеки, аналітичний супровід управлінських рішень і комунікацію між владою та громадянами. Показано, що запровадження такої управлінської ролі сприяє системності цифрових змін і підвищенню інституційної спроможності органів місцевого самоврядування. Проаналізовано можливості використання мобільних застосувань, чат-ботів, платформ електронних консультацій, відкритих бюджетних сервісів та геоінформаційних систем як інструментів смарт-врядування, що забезпечують доступність адміністративних послуг, прозорість бюджетних процесів, розвиток партисипативних механізмів і підтримку кризових комунікацій. Обґрунтовано доцільність інтеграції локальних цифрових рішень з національними платформами електронного врядування та застосування хмарних технологій і відкритих API. Визначено фінансові механізми розвитку інформаційно-комунікативної інфраструктури громад, зокрема використання місцевих бюджетів, державних субвенцій, міжнародних грантів і моделей державно-приватного партнерства.

Ключові слова: інформаційно-комунікативне забезпечення, механізм, державне управління, територіальна громада, місцеві органи самоврядування, публічне управління, регіон, населення, конкурентоспроможність.

Постановка проблеми у загальному вигляді. Удосконалення інфраструктури інформаційно-комунікативного забезпечення системи управління територіальною громадою є стратегічним напрямом модернізації місцевого самоврядування, який безпосередньо впливає на ефективність управлінських рішень, прозорість діяльності органів влади та рівень участі громадян у процесах

формування політики розвитку. Сучасна цифрова трансформація вимагає переходу від фрагментарного використання інформаційних технологій до створення цілісної інтегрованої інфраструктури, що поєднує апаратне та програмне забезпечення, телекомунікаційні мережі, інструменти аналітики та системи захисту даних. Така інфраструктура повинна забезпечувати швидкий обмін