https://doi.org/10.26565/1992-2337-2025-2-16
УДК 351:005.334

Суворов Валентин Павлович,
кандидат наук з державного управління,
асистент кафедри громадського здоров'я та управління охороною здоров'я
Харківського національного медичного університету,
проспект Науки, 4, м. Харків, 61000, Україна
e-mail: vip.suvorov@gmail.com https://orcid.org/0009-0002-0196-4269

ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ БАГАТОРІВНЕВОГО УПРАВЛІННЯ СУСПІЛЬНИМ РОЗВИТКОМ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

Анотація. У статті досліджено проблематику забезпечення стійкості багаторівневого управління суспільним розвитком в умовах гібридних загроз. Обґрунтовано актуальність проблеми через зростання масштабів та інтенсивності гібридних загроз, що створюють системні виклики для вертикалі публічної влади. Розкрито сутність стійкості як здатності системи зберігати функціональність, адаптуватися до змін та відновлюватися після деструктивних впливів. Визначено чотири ключові виміри стійкості: структурна стійкість через диверсифікацію та відсутність єдиних точок відмови, функціональна стійкість через резервування критичних спроможностей, адаптивна здатність через механізми навчання та реагування, відновлювальна спроможність через плани та ресурси відновлення. Виявлено специфічні загрози для різних рівнів управління: на національному рівні – підрив легітимності центральної влади через дезінформаційні кампанії, кібератаки на критичну інфраструктуру, економічний тиск через енергетичне шантажування; на регіональному рівні – дестабілізація через загострення міжрегіональних протиріч, використання історичних та культурних відмінностей, підтримка сепаратистських рухів; на місцевому рівні – руйнування довіри між владою та громадами, кібератаки на системи послуг, фізична деструкція інфраструктури. Досліджено механізми забезпечення стійкості: структурна диверсифікація для уникнення єдиних точок відмови, функціональне резервування критичних спроможностей, розвиток адаптивних механізмів реагування через системи раннього попередження та сценарне планування, створення резервних ресурсів для швидкого відновлення. Розкрито роль децентралізації у підвищенні стійкості через розподіл повноважень, ресурсів та ризиків між рівнями, водночас виявлено вразливості децентралізації без адекватних механізмів координації. Проаналізовано значення вертикальної та горизонтальної координації для узгодженості дій та взаємодопомоги.

Як цитувати: Суворов В. П. Забезпечення стійкості багаторівневого управління суспільним розвитком в умовах гібридних загроз. *Державне будівництво.* 2025. № 2 (38). С. 254–264. https://doi.org/10.26565/1992-2337-2025-2-16

In cites: Suvorov, V.P. (2025). Ensuring the resilience of multilevel governance of social development under hybrid threats. *State Formation, no. 2 (38), 254–264.* https://doi.org/10.26565/1992-2337-2025-2-16 [in Ukrainian].

Досліджено міжнародний досвід Естонії, Фінляндії, Швеції та Балтійських країн щодо забезпечення стійкості в умовах гібридних загроз. На основі українського досвіду протистояння російській агресії виявлено як критичні вразливості, так і значну адаптивну здатність системи. Запропоновано п'ять пріоритетних напрямів зміцнення стійкості: завершення інституційної розбудови місцевого самоврядування, зміцнення ресурсної бази, створення ефективних систем координації, підвищення кібербезпеки, розвиток спроможностей кризового реагування.

Ключові слова: багаторівневе управління, стійкість, гібридні загрози, децентралізація, координація, суспільний розвиток, публічне управління, національна безпека.

Постановка проблеми. Слід зазначити, що гібридні загрози сучасності створюють безпрецедентні виклики для систем публічного управління, особливо для їх багаторівневої архітектури. Варто підкреслити, що на відміну від традиційних загроз, які зазвичай спрямовані на конкретний рівень влади, гібридні загрози одночасно атакують множинні точки системи – від національного через регіональний до місцевого рівнів, використовуючи при цьому комбінацію військових, економічних, інформаційних, кіберnetичних та інших інструментів впливу [7]. Показовим прикладом є російська агресія проти України, яка продемонструвала, як гібридні кампанії можуть системно підривати спроможність держави до ефективного управління на всіх рівнях одночасно – від спроб делегітимізації центральної влади через дезінформацію до прямих атак на місцеве самоврядування на окупованих та прифронтових територіях [12].

Необхідно відзначити, що багаторівневе управління як модель організації публічної влади передбачає розподіл повноважень, ресурсів та відповідальності між національним, регіональним та місцевим рівнями з механізмами вертикальної та горизонтальної координації [8]. Зрозуміло, що така архітектура має потенційні переваги з точки зору ефективності через наближення прийняття рішень до громадян, адаптивності через врахування локальної специфіки, а також демократичності через множинні канали участі. Водночас вона створює специфічні вразливості в умовах гібридних загроз, зокрема множинні точки атаки, складність координації в кризових ситуаціях, а також ризики використання регіональних та місцевих відмінностей для підриву національної єдності.

У зв'язку з цим стійкість багаторівневого управління стає критичною характеристикою, що визначає спроможність системи продовжувати виконувати свої функції в умовах деструктивних впливів, адаптуватися до змін середовища та відновлюватися після кризових подій [3]. Слід підкреслити, що забезпечення такої стійкості вимагає комплексного підходу, що охоплює інституційні, організаційні, технологічні, ресурсні та культурні виміри функціонування системи управління на всіх рівнях. Актуальність дослідження обумовлена необхідністю теоретичного осмислення та практичної розробки механізмів підвищення стійкості багаторівневого управління в умовах загострення гібридних загроз.

Аналіз останніх досліджень і публікацій. Концептуальні основи багаторівневого управління розроблені у фундаментальних працях Hooghe та Marks [8],

які виділяють два типи багаторівневого врядування: тип I з чіткою ієрархією рівнів та непересічними компетенціями, а також тип II з гнучкими мережевими структурами та функціонально специфічними юрисдикціями. Розвиваючи цю проблематику, Bache та Flinders [1] досліджують еволюцію багаторівневого управління в європейському контексті, виявляючи тенденції до підвищення складності через появу нових рівнів та форм взаємодії.

Концепція стійкості в контексті систем управління розвивається у працях Folke [6], який визначає стійкість як здатність соціально-екологічних систем абсорбувати порушення, реорганізовуватися і зберігати базові функції та ідентичність. Продовжуючи цю лінію дослідження, Walker та Salt [15] виділяють три ключові аспекти стійкості: по-перше, здатність абсорбувати зміни, по-друге, здатність самоорганізовуватися, а по-третє, здатність до навчання та адаптації. У свою чергу, Davoudi [4] розглядає стійкість міст та регіонів, пропонуючи еволюційну перспективу, що враховує довгострокові процеси адаптації.

Що стосується гібридних загроз, то вони концептуалізовані у працях Hoffman [7], який визначає гібридну війну як одночасне використання конвенціональних та неконвенціональних засобів. Розвиваючи цю тематику, Lanoszka [10] досліджує виклики для систем колективної оборони, тоді як Renz та Smith [12] аналізують російську практику гібридної агресії, виявляючи специфічні патерни та методи впливу.

Адміністративна децентралізація та її вплив на стійкість систем управління досліджується Smoke [14], який виявляє як потенційні переваги, так і ризики децентралізації для ефективності та підзвітності. У цьому контексті Faguet [5] аналізує наслідки децентралізації для надання публічних послуг, а Rodden [13] досліджує фіскальні аспекти багаторівневого управління та їх вплив на загальну стійкість системи.

Слід відзначити, що український контекст багаторівневого управління в умовах конфлікту досліджується обмежено. Більшість праць зосереджена або на загальних аспектах реформи децентралізації без урахування безпекового виміру, або на окремих викликах гібридної війни без систематичного аналізу впливу на багаторівневу систему управління. Таким чином, відсутні комплексні дослідження механізмів забезпечення стійкості багаторівневого управління в умовах гібридних загроз.

Мета статті полягає у виявленні ключових механізмів забезпечення стійкості багаторівневого управління суспільним розвитком в умовах гібридних загроз та розробці рекомендацій щодо їх практичного впровадження..

Застосована методологія і методи. Методологічною основою дослідження є системний підхід, що дозволяє розглядати багаторівневе управління як складну систему взаємопов’язаних елементів. При цьому використано концепцію стійкості складних адаптивних систем для аналізу здатності багаторівневого управління функціонувати в умовах деструктивних впливів. Крім того, застосовано інституційний підхід для дослідження формальних та неформальних правил взаємодії між рівнями, а компаративний метод використано для

аналізу досвіду різних країн. Також метод кейс-дослідження застосовано для поглибленого вивчення українського досвіду. Емпірична база дослідження включає законодавчі акти, статистичні дані, документи місцевого самоврядування, а також експертні інтерв'ю.

Виклад основного матеріалу. Необхідно підкреслити, що стійкість багаторівневого управління суспільним розвитком являє собою інтегровану характеристику системи, що відображає її здатність зберігати функціональність в умовах деструктивних впливів, адаптуватися до змін зовнішнього середовища та відновлюватися після кризових подій зі збереженням базових цілей та цінностей [6]. Важливо наголосити, що на відміну від простої стабільності, яка передбачає незмінність параметрів системи, стійкість включає динамічний компонент, а саме здатність до трансформації для забезпечення виживання в нових умовах.

Концептуально стійкість багаторівневого управління охоплює чотири ключові виміри, які доцільно розглянути детальніше. По-перше, це структурна стійкість, яка являє собою здатність організаційної архітектури системи зберігатися при втраті окремих елементів або зв'язків між ними. Це передбачає відсутність єдиних точок відмови, наявність резервних структур, а також диверсифікацію каналів комунікації та координації [15]. По-друге, слід виділити функціональну стійкість, тобто здатність системи продовжувати виконувати критичні функції навіть при деградації окремих компонентів, що вимагає функціонального резервування, коли ті самі завдання можуть виконуватися різними способами або різними суб'єктами.

По-третє, важливою є адаптивна здатність, яка визначається як спроможність системи змінювати свою структуру, процеси та поведінку у відповідь на нові виклики [4]. Це включає здатність до навчання на основі досвіду, експериментування з новими підходами, а також швидкого масштабування успішних практик. По-четверте, необхідно відзначити відновлювальну спроможність, тобто здатність системи повертатися до функціонального стану після деструктивних подій, що вимагає наявності планів відновлення, резервних ресурсів, а також навичок персоналу для роботи в умовах кризи.

Зрозуміло, що гібридні загрози створюють специфічні виклики для стійкості багаторівневого управління через свою багатовимірність, адаптивність та системність [7]. На національному рівні гібридні кампанії спрямовані на підрив легітимності центральної влади через масштабні дезінформаційні операції, які ставлять під сумнів спроможність держави захищати національні інтереси, дискредитують демократичні інститути, а також поглиблюють поляризацію суспільства. Водночас кібератаки на критичну інфраструктуру паралізують спроможність центрального уряду координувати дії на нижчих рівнях, тоді як економічний тиск через енергетичне шантажування або торговельні обмеження підриває ресурсну базу для виконання функцій управління.

На регіональному рівні гібридні загрози використовують історичні, культурні, мовні та економічні відмінності між регіонами для загострення міжрегіо-

нальних протиріч та створення сепаратистських настроїв [12]. Інформаційні операції цілеспрямовано конструюють наративи про експлуатацію одних регіонів іншими, дискримінацію за регіональною ознакою, а також необхідність особливого статусу. При цьому підтримка регіональних політичних сил, що виступають за автономізацію або сепаратизм, підриває національну єдність, а економічні диспропорції між регіонами використовуються для посилення відчуття несправедливості та відчуження.

На місцевому рівні гібридні загрози спрямовані на руйнування довіри між органами місцевого самоврядування та громадами через дискредитацію місцевих лідерів, поширення чуток про корупцію, а також провокування конфліктів між різними групами населення [10]. Водночас кібератаки на системи надання адміністративних послуг порушують повсякденне функціонування місцевого управління, а економічний тиск на місцеві бюджети через блокування трансфертів або зниження надходжень обмежує спроможність виконувати повноваження. Особливо гостро ця проблема проявляється на окупованих та прифронтових територіях, де фізична деструкція інфраструктури управління руйнує саму можливість здійснення владних функцій.

У зв'язку з цим механізми забезпечення стійкості багаторівневого управління мають враховувати специфіку викликів на кожному рівні та забезпечувати системну протидію. Зокрема, структурна диверсифікація передбачає розподіл критичних функцій між множинними суб'єктами та рівнями, що унеможливлює паралізацію всієї системи через атаку на окремі елементи [1]. Замість концентрації повноважень на національному рівні, децентралізація розподіляє їх між регіональним та місцевим рівнями, створюючи таким чином резервні спроможності, проте це вимагає чітких механізмів координації для забезпечення узгодженості дій.

Слід зазначити, що функціональне резервування означає, що критичні завдання можуть виконуватися різними способами або різними суб'єктами [15]. Наприклад, надання соціальних послуг може здійснюватися як державними установами, так і недержавними організаціями, а також приватним сектором через делегування повноважень. Аналогічно, комунікація між рівнями може відбуватися через множинні канали – формальні адміністративні, електронні системи, а також особисті контакти керівників, що забезпечує продовження функціонування при виході з ладу окремих механізмів.

Розвиток адаптивних спроможностей вимагає цілеспрямованих інвестицій у здатність системи швидко реагувати на нові виклики [4]. Це включає, по-перше, створення механізмів раннього попередження для виявлення загроз на початкових стадіях, коли протидія ще є ефективною. Варто підкреслити, що такі системи мають інтегрувати різноманітні джерела інформації – від моніторингу соціальних мереж до аналізу економічних показників, від сигналів з місцевого рівня до міжнародних джерел. Критичне значення має розробка індикаторів, що дозволяють виявляти ранні ознаки дестабілізації.

По-друге, розробка сценаріїв можливих кризових ситуацій та планів реагування на них дозволяє скоротити час прийняття рішень в умовах кризи. Сценарне планування має охоплювати широкий спектр можливих загроз – від природних лих через техногенні катастрофи до навмисних гібридних атак. Для кожного сценарію розробляються процедури активації, розподіл ролей та відповідальності, протоколи комунікації, а також критерії ескалації чи деескалації заходів реагування. Важливою є участь усіх рівнів влади у розробці сценаріїв для врахування специфіки територій.

По-третє, регулярні навчання та тренування персоналу для роботи в умовах надзвичайних ситуацій перетворюють плани з паперових документів на операційні процедури, що ефективно спрацьовують під час реальних подій. При цьому навчання мають бути реалістичними, включати несподівані елементи, а також вимагати прийняття рішень в умовах невизначеності та обмеженого часу. Корисним є залучення зовнішніх оцінювачів для об’єктивної оцінки ефективності реагування.

По-четверте, створення інституційних можливостей для експериментування з новими підходами та швидкого масштабування успішних практик підвищує здатність системи еволюціонувати [11]. Це передбачає толерантність до помилок при апробації інновацій, а також платформи для обміну досвідом між територіями. Пілотні проекти дозволяють тестувати нові підходи в контрольованих умовах перед широким впровадженням, тоді як успішні практики документуються та поширюються через спеціалізовані центри компетенцій.

Відновлювальна спроможність забезпечується через створення резервних ресурсів, зокрема фінансових резервів для швидкої мобілізації у кризових ситуаціях, резервних приміщень для переміщення органів управління при фізичній деструкції основних, а також резервних каналів комунікації при виході з ладу основних систем зв’язку [6]. Важливою є наявність детальних планів відновлення з чіткими процедурами, розподілом ролей та відповідальності, а також критеріями оцінки ситуації та активації різних сценаріїв реагування. Крім того, необхідне накопичення досвіду відновлення через документування уроків з попередніх кризових подій та їх систематичну інтеграцію у процедури та навчальні програми.

Слід підкреслити, що децентралізація як інструмент підвищення стійкості має неоднозначні наслідки, які залежать від специфіки дизайну та контексту впровадження [14]. З одного боку, децентралізація підвищує стійкість через розподіл повноважень, що унеможливлює паралізацію всієї системи через захоплення центру. При цьому наближення прийняття рішень до громадян дозволяє швидше реагувати на локальні виклики з урахуванням специфіки ситуації, тоді як розвиток спроможностей на місцевому рівні створює резервні компетенції, які можуть бути мобілізовані в кризових ситуаціях. Крім того, множинність джерел легітимності через виборність місцевої влади ускладнює делегітимізацію всієї системи управління.

З іншого боку, децентралізація створює нові вразливості, якщо не супроводжується адекватними механізмами координації та підтримки [5]. Зокрема, слаб-

кі місцеві органи влади з обмеженими ресурсами та компетенціями стають легкими цілями для гібридних атак, а диференціація між регіонами та громадами може використовуватися для загострення територіальних конфліктів. Водночас фіскальна децентралізація без достатньої місцевої податкової бази робить місцеві бюджети вразливими до економічних шоків, тоді як політична децентралізація може призводити до появи регіональних еліт з сепаратистськими настроями.

У зв'язку з цим оптимальна модель передбачає збалансовану децентралізацію з чіткими механізмами координації між рівнями [8]. Національний рівень зберігає повноваження щодо стратегічного планування, встановлення стандартів, вирівнювання можливостей між територіями, а також координації в кризових ситуаціях, тоді як регіональний та місцевий рівні отримують достатні повноваження та ресурси для вирішення питань місцевого значення з урахуванням специфіки територій. При цьому механізми вертикальної координації забезпечують узгодженість дій та можливість швидкої мобілізації ресурсів у відповідь на загрози.

Варто наголосити, що горизонтальна координація між органами влади одного рівня є не менш важливою для забезпечення стійкості [1]. Співпраця між сусідніми громадами дозволяє спільно вирішувати проблеми, що виходять за межі окремих юрисдикцій, зокрема управління спільними ресурсами, протидію транскордонним загрозам, а також надання послуг, що вимагають масштабу. При цьому обмін досвідом між територіями прискорює поширення кращих практик, тоді як взаємодопомога в кризових ситуаціях підвищує загальну спроможність системи до реагування.

Міжнародний досвід демонструє різноманітні підходи до забезпечення стійкості багаторівневого управління в умовах гібридних загроз. Зокрема, Естонія після кібератак 2007 року, що паралізували критичну інфраструктуру країни, радикально посилила кібербезпеку на всіх рівнях управління [9]. Було створено X-Road – платформу для захищеного обміну даними між державними установами різних рівнів, а критичні державні дані резервуються в дата-центрі в Люксембурзі, що забезпечує можливість швидкого відновлення функціонування навіть при масштабних кібератаках.

Фінляндія розробила комплексну модель всеохоплюючої безпеки, що інтегрує всі рівні влади, приватний сектор та громадянське суспільство у систему готовності до кризових ситуацій [2]. Кожен муніципалітет має детальні плани кризового реагування, що регулярно оновлюються та перевіряються під час навчань, а також створено національний пул експертів, які можуть бути швидко мобілізовані для підтримки місцевих властей. Швеція відновила цивільну оборону на муніципальному рівні після десятиліть занепаду, проводячи Total Defence Exercise кожні чотири роки з участю всіх рівнів влади та суспільства. Балтійські країни створили спільні механізми координації протидії гібридним загрозам, інвестуючи у розвиток спроможностей місцевого рівня через навчання та ресурсну підтримку.

Український досвід протистояння російській агресії виявляє як критичні вразливості, так і значні резерви стійкості багаторівневого управління. Серед основних викликів слід відзначити недостатню інституційну спроможність

новостворених об'єднаних територіальних громад, багато з яких отримали повноваження лише за кілька років до повномасштабного вторгнення. Обмеженість ресурсів місцевих бюджетів ускладнюється військовими діями, тоді як слабкість механізмів координації виявилася особливо проблемною на початковому етапі війни. Вразливість цифрової інфраструктури до кібератак підтверджується численними інцидентами, а дефіцит кваліфікованих кадрів загострився через мобілізацію та міграцію населення.

Водночас проявилася висока адаптивність системи багаторівневого управління. Зокрема, швидке переформатування повноважень в умовах воєнного стану відбулося з мінімальними збоями у наданні критичних послуг населенню, оскільки місцеві органи влади оперативно адаптували свою діяльність до нових умов, створивши штаби реагування на надзвичайні ситуації, організувавши евакуацію населення, а також налагодивши координацію з військовими та силовими структурами. Мобілізація ресурсів громад для підтримки обороноздатності виявилася потужним резервом стійкості – від закупівлі техніки для територіальної оборони до організації волонтерських мереж підтримки військових та внутрішньо переміщених осіб.

Розвиток горизонтальної співпраці між громадами для взаємодопомоги також став органічною відповіддю на виклики війни. Громади західних регіонів приймали евакуйованих з прифронтових територій, громади зі збереженою інфраструктурою допомагали постраждалим від обстрілів, а також створювалися мережі обміну ресурсами та досвідом. Залучення волонтерського руху для виконання функцій управління компенсувало дефіцит державних спроможностей, оскільки волонтери організовували логістику гуманітарної допомоги, координували евакуації, а також підтримували критичну інфраструктуру. Ця спонтанна самоорганізація громадянського суспільства продемонструвала важливість соціального капіталу для стійкості систем управління [13].

Пріоритетні напрями зміцнення стійкості багаторівневого управління в Україні мають враховувати як виявлені вразливості, так і накопичений досвід адаптації.

По-перше, завершення інституційної спроможності об'єднаних територіальних громад вимагає системної підготовки кадрів через створення спеціалізованих навчальних програм для посадових осіб місцевого самоврядування, регулярне підвищення кваліфікації, а також обмін досвідом між громадами. При цьому створення типових регламентів та процедур дозволить стандартизувати кращі практики та забезпечити сумісність між різними рівнями.

По-друге, зміцнення ресурсної бази місцевого самоврядування є критично важливим для реальної спроможності виконувати повноваження. Розширення податкових повноважень місцевих органів влади має супроводжуватися технічною підтримкою для ефективного адміністрування податків та зборів, тоді як вирівнювання фіскальних диспропорцій через систему трансфертів має забезпечувати мінімальний рівень спроможності для всіх громад незалежно від економічного потенціалу території.

По-третє, розбудова систем координації між рівнями має перетворити епізодичну взаємодію на системну практику. Створення постійних координаційних

платформ на регіональному рівні забезпечить регулярний діалог між представниками різних рівнів влади для вирішення спільних питань, тоді як спільне планування розвитку територій з участю національного, регіонального та місцевого рівнів підвищить узгодженість інвестицій та ефективність використання ресурсів.

По-четверте, підвищення кібербезпеки на всіх рівнях вимагає впровадження єдиних стандартів захисту інформації, що враховують різний рівень технічних можливостей громад. Систематичне навчання персоналу основам кібергігієни та правилам безпечної роботи з інформаційними системами має стати обов'язковим елементом підготовки, тоді як централізована підтримка менших громад у питаннях кібербезпеки через регіональні центри компетенцій компенсує обмеженість ресурсів окремих громад.

По-п'яте, розвиток спроможностей до кризового реагування має включати регулярні навчання з реалістичними сценаріями, що перевіряють як індивідуальні навички, так і взаємодію між різними суб'єктами. Розробка детальних планів реагування на різні типи кризових ситуацій з чіткими протоколами комунікації є необхідною умовою ефективності, а створення стратегічних резервів критичних ресурсів забезпечить автономність функціонування. Інтеграція громадянського суспільства у системи реагування через підтримку волонтерських організацій, координацію зусиль, а також навчання добровольців підвищить загальну спроможність системи.

Висновки і перспективи подальших досліджень. Підсумовуючи викладене, слід зазначити, що забезпечення стійкості багаторівневого управління суспільним розвитком в умовах гібридних загроз є комплексним завданням, що вимагає системних змін в архітектурі, процесах та спроможностях системи публічної влади. Встановлено, що стійкість охоплює чотири ключові виміри: структурну стійкість через диверсифікацію та відсутність єдиних точок відмови, функціональну стійкість через резервування критичних спроможностей, адаптивну здатність через механізми навчання та реагування на нові виклики, а також відновлювальну спроможність через плани та ресурси для швидкого відновлення після кризових подій.

Виявлено, що гібридні загрози створюють специфічні виклики на кожному рівні багаторівневого управління: підрив легітимності на національному рівні, загострення міжрегіональних протиріч на регіональному рівні, а також руйнування довіри на місцевому рівні. У зв'язку з цим протидія вимагає комплексних механізмів, що враховують особливості загроз та забезпечують системну стійкість через структурну диверсифікацію, функціональне резервування, розвиток адаптивних спроможностей, а також створення систем раннього попередження та відновлення.

Встановлено, що децентралізація може підвищувати стійкість через розподіл повноважень та створення резервних спроможностей, проте вимагає збалансованого дизайну з адекватними механізмами координації та підтримки. Критичне значення має як вертикальна координація між рівнями для узгодженості дій, так і горизонтальна координація для обміну досвідом та взаємодопомоги. Український досвід демонструє як вразливості системи, так і її значну адаптивну здатність в умовах екстремального тиску.

Визначено, що пріоритетні напрями зміцнення стійкості включають завершення інституційної розбудови місцевого самоврядування, зміцнення ресурсної бази, створення ефективних систем координації, підвищення кібербезпеки, а також розвиток спроможностей кризового реагування. Реалізація цих напрямів вимагає систематичних зусиль та інвестицій, проте є критично важливою для забезпечення спроможності держави ефективно функціонувати в умовах тривалого протистояння гібридним загрозам.

Перспективи подальших досліджень включають емпіричний аналіз ефективності різних механізмів забезпечення стійкості, дослідження факторів успішності адаптації різних громад до кризових умов, аналіз впливу децентралізації на стійкість в українському контексті, вивчення ролі неформальних мереж та громадянського суспільства у підвищенні стійкості, а також розробку індикаторів вимірювання стійкості багаторівневого управління.

Стаття надійшла до редакції 08.08.2025 р.
Стаття рекомендована до друку 12.09.2025 р.
Опубліковано 30.12.2025 р.

Suvorov V. P.,
Candidate of Sciences in Public Administration,
Assistant Professor of the Department of Public Health and Health Care Management of the Kharkiv National Medical University,
4 Nauky Avenue, Kharkiv, 61022, Ukraine
e-mail: vip.suvorov@gmail.com https://orcid.org/0009-0002-0196-4269

ENSURING THE RESILIENCE OF MULTILEVEL GOVERNANCE OF SOCIAL DEVELOPMENT UNDER HYBRID THREATS

Abstract. The article examines the problem of ensuring the resilience of multilevel governance of social development under hybrid threats. The relevance of the problem is substantiated through the growing scale and intensity of hybrid threats that create systemic challenges for the public authority vertical. The essence of resilience is revealed as the ability of the system to maintain functionality, adapt to changes, and recover after destructive impacts. Four key dimensions of resilience are defined: structural resilience through diversification and absence of single points of failure, functional resilience through redundancy of critical capabilities, adaptive capacity through learning and response mechanisms, recovery capability through plans and recovery resources. Specific threats to different levels of governance are identified: at the national level – undermining the legitimacy of central authorities through disinformation campaigns, cyberattacks on critical infrastructure, economic pressure through energy blackmail; at the regional level – destabilization through exacerbation of inter-regional contradictions, use of historical and cultural differences, support for separatist movements; at the local level – destruction of trust between authorities and communities, cyberattacks on service systems, physical destruction of infrastructure. Mechanisms for ensuring resilience are examined: structural diversification to avoid single points of failure, functional redundancy of critical capabilities, development of adaptive response mechanisms through early warning systems and scenario planning, creation of reserve resources for rapid recovery. The role of decentralization in enhancing resilience through the distribution of powers, resources, and risks between levels is revealed, while vulnerabilities of decentralization without adequate coordination mechanisms are identified. The importance of vertical and horizontal coordination for coherence of actions and mutual assistance is analyzed. International experience of Estonia, Finland, Sweden, and the Baltic

countries in ensuring resilience under hybrid threats is studied. Based on Ukrainian experience of resisting Russian aggression, both critical vulnerabilities and significant adaptive capacity of the system are identified. Five priority directions for strengthening resilience are proposed: completion of institutional development of local self-government, strengthening of the resource base, creation of effective coordination systems, enhancement of cybersecurity, development of crisis response capabilities.

Keywords: multilevel governance, resilience, hybrid threats, decentralization, coordination, social development, public administration, national security.

REFERENCES

1. Bache, I., & Flinders, M. (2004). Multi-level governance. *Public Policy and Administration, vol. 19, is. 1, 31-51*. https://doi.org/10.1177/095207670401900103

2. Boin, A., & Lodge, M. (2016). Designing resilient institutions for transboundary crisis management: a time for public administration. *Public Administration, 94(2), 289–298*. https://doi.org/10.1111/padm.12264

3. Comfort, L.K., Boin, A., & Demchak, C.C. (2010). *Designing resilience: Preparing for extreme events*. Pittsburgh: University of Pittsburgh Press. https://doi.org/10.1108/ijdrbe.2011.2.2.178.1

4. Davoudi, S. (2012). Resilience: A bridging concept or a dead end? *Planning Theory & Practice, 13(2), 299–333*. http://dx.doi.org/10.1080/14649357.2012.677124

5. Faguet, J.P. (2014). Decentralization and governance. *World Development, 53, 2–13.* https://doi.org/10.1016/j.worlddev.2013.01.002

6. Folke, C. (2006). Resilience: The emergence of a perspective for social-ecological systems analyses. *Global Environmental Change, 16(3), 253–267*. https://doi.org/10.1016/j.gloenvcha.2006.04.002

7. Hoffman, F.G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Arlington: Potomac Institute for Policy Studies.

8. Hooghe, L., & Marks, G. (2003). Unraveling the central state, but how? Types of multi-level governance. *American Political Science Review, 97(2), 233–243*. https://doi.org/10.1017/S0003055403000649

9. Jore, S.H. (2017). The conceptual and scientific demarcation of security in contrast to safety. *European Journal for Security Research, 2, 157–174*. https://doi.org/10.1007/s41125-017-0021-9

10. Lanoszka, A. (2016). Russian hybrid warfare and extended deterrence in eastern Europe. *International Affairs, 92(1), 175–195*. https://doi.org/10.1111/1468-2346.12509

11. Manyena, S.B. (2006). The concept of resilience revisited. *Disasters, 30(4), 434–450*. https://doi.org/10.1111/j.0361-3666.2006.00331.x

12. Renz, B., & Smith, H. (2016). *Russia and hybrid warfare: Going beyond the label*. Helsinki: Aleksanteri Institute. URL: http://www.helsinki.fi/aleksanteri/english/publications/presentations/papers/ap_1_2016.pdf

13. Rodden, J. (2004). Comparative federalism and decentralization: On meaning and measurement. *Comparative Politics, 36(4), 481–500*. https://doi.org/10.2307/4150172

14. Smoke, P. (2001). *Fiscal decentralization in developing countries: A review of current concepts and practice*. Geneva: UNRISD. URL: https://www.researchgate.net/publication/31721101_Fiscal_Decentralization_in_Developing_Countries_A_Review_of_Current_Concepts_and_Practice_P_Smoke

15. Walker, B., & Salt, D. (2006). *Resilience thinking: Sustaining ecosystems and people in a changing world*. Washington: Island Press.

The article was received by the editors 08.08.2025.
The article is recommended for printing 12.09.2025.
Published 30.12.2025.