https://doi.org/10.26565/1684-8489-2025-2-07
УДК 351:005.334

Клочко Іван Андрійович,
аспірант кафедри публічної політики
навчально-наукового інституту "Інститут державного управління"
Харківського національного університету імені В. Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна

https://orcid.org/0009-0007-4881-7107

УДОСКОНАЛЕННЯ МЕХАНІЗМІВ УПРАВЛІННЯ РИЗИКАМИ В ПУБЛІЧНОМУ СЕКТОРІ

Анотація. Представлено концептуальну модель удосконалення механізмів управління ризиками в публічному секторі України з урахуванням сучасних міжнародних стандартів та особливостей вітчизняного контексту. Обґрунтовано недостатність традиційних підходів до управління ризиками в органах публічної влади, що виявляється у фрагментарності процесів ідентифікації загроз, слабкій інтеграції ризик-менеджменту в стратегічне планування, відсутності єдиної методології та культури управління ризиками. Розроблено багаторівневу систему вдосконалення механізмів ризик-менеджменту, що інтегрує інституційний, процесний, інструментальний та культурний виміри трансформації. Запропоновано дванадцять базових принципів побудови інтегрованої системи управління ризиками: системність, адаптивність, інклюзивність, прозорість, пропорційність, доказовість, безперервність, інтегрованість, стійкість, етичність та інноваційність. Детально розкрито архітектуру системи на трьох рівнях із визначенням функцій центральних координаційних органів, галузевих підрозділів управління ризиками та регіональних механізмів імплементації. Обґрунтовано систему практичних інструментів ризик-менеджменту, адаптованих до специфіки публічного сектору, включаючи матриці ризиків, реєстри загроз, індикатори раннього попередження, стрес-тестування та сценарне планування. Розроблено механізми культурної трансформації через навчання персоналу, стимулювання проактивної поведінки, створення каналів комунікації та формування систем мотивації. Доведено, що запропонована модель забезпечує синергетичний ефект через інтеграцію різнорідних компонентів при збереженні їх функціональної автономії, що є критичним для ефективного управління багатовимірними загрозами публічного управління. Впровадження концептуальної моделі дозволить суттєво підвищити стійкість вітчизняного публічного сектору до зовнішніх та внутрішніх викликів.

Ключові слова: публічне управління, управління ризиками, публічний сектор, інтегрована система, адаптивність, організаційна культура, стратегічне планування.

Як цитувати: Клочко І. А. Удосконалення механізмів управління ризиками в публічному секторі. *Актуальні проблеми державного управління*. 2025. № 2 (67). С. 160–177. https://doi.org/10.26565/1684-8489-2025-2-07

In cites: Klochko, I.A. (2025). Improvement of risk management mechanisms in the public sector. *Pressing Problems of Public Administration, 2 (67), 160–177.* https://doi.org/10.26565/1684-8489-2025-2-07 [in Ukrainian].

Вступ. Сучасний публічний сектор України функціонує в умовах безпрецедентної невизначеності та множинності загроз різної природи, що радикально трансформує вимоги до систем управління організаційними ризиками. Повномасштабна війна, тривала економічна нестабільність, прискорена цифровізація, демографічні зрушення, кліматичні зміни створюють складний комплекс взаємопов'язаних викликів, які неможливо ефективно опрацьовувати в рамках традиційних реактивних підходів. Практика останніх років переконливо демонструє, що органи публічної влади з їх традиційною бюрократичною культурою та жорсткими ієрархічними структурами виявляються структурно неспроможними швидко адаптуватися до раптових змін безпекового, економічного та соціального середовища [4]. Фрагментарність процесів ідентифікації та оцінювання ризиків, відсутність цілісної методології управління загрозами, слабка інтеграція ризик-менеджменту в процеси стратегічного планування та прийняття управлінських рішень призводять до накопичення системних вразливостей публічного управління.

Проблема посилюється тим, що в українському публічному секторі домінує реактивна модель реагування на вже реалізовані ризики замість проактивної ідентифікації потенційних загроз та завчасної підготовки контрзаходів. Відсутність інституціоналізованої практики систематичного моніторингу ризикового середовища, недостатня формалізація процедур оцінки імовірності та масштабу потенційних негативних подій, брак кваліфікованих спеціалістів з управління ризиками в органах влади перетворюють ризик-менеджмент на епізодичну діяльність замість неперервного процесу. Інформаційна роз'єднаність між різними відомствами унеможливлює формування цілісного бачення взаємопов'язаних ризиків, що охоплюють декілька сфер публічного управління одночасно. Ситуація ускладнюється відсутністю єдиних стандартів класифікації, оцінювання та звітності щодо ризиків, що унеможливлює порівняння та консолідацію ризикової інформації на національному рівні [25].

Водночас міжнародний досвід провідних країн демонструє можливість створення ефективних систем управління ризиками в публічному секторі через інтеграцію загальновизнаних стандартів, таких як ISO 31000 та COSO ERM, з урахуванням специфіки державного управління [15]. Країни, що успішно імплементували комплексні системи ризик-менеджменту, демонструють вищу стійкість публічних інституцій до кризових явищ, більшу ефективність використання обмежених бюджетних ресурсів, підвищену довіру громадян до органів влади. Проте механічне копіювання зарубіжних моделей без адаптації до українського контексту є неприйнятним через суттєві відмінності в адміністративній культурі, правовому середовищі, рівні інституційної спроможності та специфічних викликах, з якими стикається вітчизняний публічний сектор.

Огляд літератури. Проблематика управління ризиками в публічному секторі активно досліджується міжнародною науковою спільнотою, проте більшість праць зосереджена на окремих аспектах без створення цілісної концептуальної моделі трансформації вітчизняної системи. Фундаментальні засади enterprise risk management закладені в рамках COSO, яка визначила інтеграцію управління ризиками зі стратегічним плануванням та організаційною результативністю як ключовий принцип сучасного ризик-менеджменту [11]. Міжнародний стандарт ISO 31000:2018 надає універсальну методологію для організацій будь-якого типу та розміру, встановлюючи прин-

ципи, рамкову структуру та процес управління ризиками [18]. Ці базові документи формують концептуальну основу для розвитку специфічних підходів до публічного сектору.

Дослідники активно вивчають особливості адаптації загальних принципів управління ризиками до специфіки публічних організацій. E. Bracci та колеги провели структурований огляд літератури з управління ризиками в публічному секторі, виявивши основні тематичні кластери та прогалини в дослідженнях [5]. J. Bullock та співавтори розробили концептуальну основу для вивчення управління ризиками в публічних організаціях, акцентуючи увагу на унікальних характеристиках державних інституцій порівняно з приватним сектором [7]. M. Caldarulo та E. Welch досліджували роль зовнішньої інформації та контрактних відносин у формуванні організаційного сприйняття ризиків державними агенціями [8]. Ці праці підкреслюють необхідність врахування специфічного контексту публічного управління при розробці систем ризик-менеджменту.

Важливий внесок у розуміння інституційних аспектів управління ризиками зробили дослідження механізмів інтеграції ризик-менеджменту з системами управління результативністю. E. Braumann та колеги проаналізували взаємозв'язки між управлінням ефективністю та управлінням ризиками, виявивши синергетичні ефекти від їх інтеграції в публічних організаціях [6]. T. Andersen та P. Young обґрунтували роль інтерактивної обробки інформації для підвищення ефективності корпоративного управління ризиками в публічному секторі, демонструючи важливість динамічних комунікаційних процесів [4]. A. De Lorena та A. Costa розробили модель зрілості управління ризиками для публічних організацій, що дозволяє оцінювати поточний стан та визначати напрями розвитку систем ризик-менеджменту [13]. E. Tangsgaard та C. Fischer запропонували теоретичну рамку для розмежування управління ризиками та управління помилками в публічному секторі, що має принципове значення для формування відповідної організаційної культури [25].

Порівняльні дослідження національних систем управління ризиками виявляють значну варіативність підходів та інституційних рішень. Gourbier та колеги провели компаративний аналіз систем управління ризиками в центральних урядах Франції, Німеччини та Італії, виявивши як спільні виклики, так і специфічні національні особливості імплементації [15]. P. Young та K. Hoang досліджували трансформацію корпоративного управління ризиками в публічному секторі, обґрунтовуючи необхідність переходу від формальних процедур до справжньої інтеграції ризик-мислення в організаційну культуру [27]. D. Kuchta та колеги зосередили увагу на специфіці управління невизначеністю в публічних проектах, підкреслюючи відмінності від приватного сектору [21]. Ці праці демонструють, що ефективність систем управління ризиками визначається не стільки формальними структурами, скільки культурними та інституційними чинниками.

Окрему увагу дослідники приділяють питанням комунікації ризиків та залучення стейкхолдерів. L. Agyepong та X. Liang здійснили картування наукових фронтирів публічної ризик-комунікації в контексті управління ризиками катастроф, виявивши важливу роль прозорості та доступності інформації [1]. S. Alon-Barkat та M. Busuioc досліджували взаємодію людини та штучного інтелекту в процесах прийняття рішень публічного сектору, що набуває особливої актуальності в контексті цифровізації управління ризиками [3].

Ці праці підкреслюють необхідність переосмислення традиційних підходів до ризик-комунікації з урахуванням нових технологічних можливостей та очікувань громадян щодо прозорості державного управління.

Проте, незважаючи на значний доробок міжнародної наукової спільноти, залишаються недостатньо дослідженими питання адаптації загальних моделей управління ризиками до специфічних умов країн, що перебувають в стані воєнного конфлікту, здійснюють масштабну євроінтеграцію та трансформацію публічного управління одночасно. Відсутні комплексні концептуальні моделі, що інтегрують інституційний, процесний, інструментальний та культурний виміри трансформації систем ризик-менеджменту з урахуванням обмежених ресурсів та множинних викликів перехідних суспільств.

Мета статті полягає у розробці концептуальної моделі удосконалення механізмів управління ризиками в публічному секторі України, що інтегрує міжнародні стандарти з особливостями вітчизняного контексту та забезпечує системну трансформацію інституційних, процесних, інструментальних та культурних аспектів ризик-менеджменту.

Методологія дослідження. Дослідження базується на системному підході до аналізу управління ризиками в публічному секторі, що дозволяє розглядати ризик-менеджмент як цілісну багаторівневу систему взаємопов'язаних елементів. Використано методи структурно-функціонального аналізу для виявлення ключових компонентів системи управління ризиками та визначення їх ролі в забезпеченні організаційної стійкості. Компаративний аналіз міжнародного досвіду дозволив ідентифікувати успішні практики та механізми їх адаптації до українського контексту. Концептуальне моделювання застосовано для формування інтегрованої архітектури системи управління ризиками на стратегічному, галузевому та регіональному рівнях. Методологічною основою слугують положення міжнародних стандартів ISO 31000:2018 та рамкової моделі COSO ERM, адаптовані до специфіки публічного сектору України.

Основні результати дослідження. Удосконалення механізмів управління ризиками в публічному секторі вимагає системної трансформації, що охоплює принципові засади, інституційну архітектуру, процесні механізми, інструментарій та організаційну культуру. Така багатовимірна трансформація може бути ефективною лише за умови цілісного концептуального бачення та послідовної імплементації взаємоузгоджених компонентів.

Базові принципи інтегрованої системи управління ризиками формують концептуальний фундамент для розбудови ефективного ризик-менеджменту в публічному секторі [1; 4; 7; 15; 20; 25; 27]. Принцип системності передбачає розгляд управління ризиками як цілісної системи взаємопов'язаних елементів, що охоплює всі рівні та напрями діяльності публічних організацій. Принцип проактивності орієнтує систему управління ризиками на випередження потенційних загроз замість реагування на вже реалізовані негативні події. Принцип адаптивності забезпечує здатність системи управління ризиками гнучко реагувати на зміни в зовнішньому середовищі та внутрішніх умовах функціонування організації. Принцип інклюзивності наголошує на необхідності залучення широкого кола стейкхолдерів до процесів управління ризиками. Принцип прозорості вимагає відкритості процесів управління ризиками та доступності релевантної інформації для зацікавлених сторін. Принцип пропорційності забезпечує відповідність заходів управління

ризиками рівню загроз та доступним ресурсам. Принцип доказовості орієнтує процеси управління ризиками на використання найкращих доступних даних та наукових знань. Принцип безперервності підкреслює, що управління ризиками не є одноразовою активністю чи періодичним заходом, а становить постійний процес, інтегрований у повсякденну діяльність організації. Принцип інтегрованості вимагає вбудовування управління ризиками в усі організаційні процеси та системи управління. Принцип стійкості спрямований на формування організаційної спроможності не просто уникати чи мінімізувати ризики, а й швидко відновлюватися після реалізації загроз та адаптуватися до нових умов. Принцип етичності наголошує, що управління ризиками повинно здійснюватися з дотриманням етичних норм та цінностей публічного служіння. Принцип інноваційності спрямований на використання нових технологій, методів та підходів для підвищення ефективності управління ризиками.

Архітектура інтегрованої системи управління ризиками в публічному секторі має базуватися на багаторівневій моделі, що забезпечує як вертикальну координацію між різними ієрархічними рівнями, так і горизонтальну інтеграцію між секторальними підрозділами. Така архітектура дозволяє поєднати переваги централізованої координації з необхідною автономією окремих відомств та територій у визначенні специфічних підходів до управління галузевими та регіональними ризиками.

Стратегічний рівень системи управління ризиками формує загальнонаціональну рамку та забезпечує координацію ризик-менеджменту в масштабах всього публічного сектору. На цьому рівні доцільно створити Центральний орган координації управління ризиками при Кабінеті Міністрів України, який би виконував функції методологічного центру, координатора міжвідомчої взаємодії та моніторингу ефективності національної системи ризик-менеджменту. Цей орган повинен розробляти єдині стандарти та методології ідентифікації, оцінювання, моніторингу та звітності щодо ризиків, адаптовані до специфіки українського публічного сектору на основі міжнародних стандартів ISO 31000 та COSO ERM [18; 11]. Важливою функцією центрального органу є формування та підтримка Національного реєстру ризиків, який би консолідував інформацію про критичні загрози на рівні держави, забезпечував би можливість аналізу міжсекторальних та каскадних ризиків, створював основу для стратегічного планування на національному рівні.

Центральний координаційний орган має також здійснювати регулярний моніторинг ризикового ландшафту через збір та аналіз інформації від відомств, міжнародних партнерів, аналітичних центрів, громадських організацій. Систематизація та аналіз цієї інформації дозволить виявляти emerging risks – слабкі сигнали наростаючих загроз, які ще не є очевидними на рівні окремих організацій, але можуть трансформуватися в серйозні виклики для всієї держави [4]. Прикладами таких ризиків можуть бути поступова деградація критичної інфраструктури, демографічні зрушення, зміни в глобальних ланцюгах постачання, технологічні зміни, що підривають традиційні моделі надання публічних послуг. Центральний орган повинен не лише ідентифікувати такі стратегічні ризики, а й ініціювати розробку загальнодержавних стратегій реагування, координувати міжвідомчі робочі групи, забезпечувати виділення ресурсів на превентивні заходи.

Важливою функцією стратегічного рівня є інтеграція управління ризиками в процеси довгострокового стратегічного планування та

бюджетування. Це передбачає обов'язкове включення ризик-аналізу в підготовку національних стратегій розвитку, державних програм, проєктів реформ [13]. При формуванні державного бюджету повинні враховуватися ризикові профілі програм та проектів, що фінансуються, з виділенням спеціальних резервів на управління критичними загрозами. Центральний орган має також координувати розробку сценаріїв розвитку ситуації в країні з урахуванням можливої реалізації різних комбінацій ризиків, що дозволить уряду готувати варіантні плани дій та підвищувати адаптивність державної політики до змінних умов. Важливим аспектом роботи стратегічного рівня є комунікація ризиків до найвищого політичного керівництва у формі, що забезпечує розуміння складних взаємозалежностей та довгострокових наслідків для прийняття обґрунтованих рішень.

Галузевий рівень системи управління ризиками втілюється через створення спеціалізованих підрозділів управління ризиками в центральних органах виконавчої влади, які відповідають за операціоналізацію загальних принципів та методологій в контексті специфічних секторальних викликів. Кожне міністерство та інше центральне відомство повинно мати підрозділ чи визначених відповідальних осіб з управління ризиками, які володіють як методологічною експертизою з ризик-менеджменту, так і глибоким розумінням специфіки відповідної галузі [7]. Ці підрозділи формують галузеві реєстри ризиків, що включають як загальні загрози, притаманні всьому публічному сектору (кібератаки, корупція, недостатнє фінансування), так і специфічні галузеві ризики (епідемії для сфери охорони здоров'я, техногенні катастрофи для промисловості, неврожаї для аграрного сектору).

Галузеві підрозділи управління ризиками здійснюють систематичну ідентифікацію ризиків через залучення працівників різних рівнів, консультації з експертами, аналіз міжнародного досвіду аналогічних відомств, вивчення реалізованих ризиків у минулому [1]. Оцінювання ідентифікованих ризиків проводиться з використанням як кількісних методів (статистичний аналіз, моделювання), так і якісних підходів (експертні оцінки, сценарне планування) залежно від доступності даних та природи ризиків. Для пріоритетних ризиків розробляються детальні плани реагування, що специфікують превентивні заходи для зниження імовірності реалізації загрози, контингентні плани дій у випадку реалізації ризику, розподіл ролей та відповідальності, необхідні ресурси. Галузеві підрозділи також відповідають за моніторинг ключових індикаторів ризиків (Key Risk Indicators) – метрик, що дозволяють відстежувати зміни в ризиковому профілі та сигналізувати про наростання загроз.

Важливим аспектом роботи галузевого рівня є горизонтальна координація між відомствами для управління міжсекторальними ризиками, які не можуть бути ефективно опрацьовані одним міністерством. Прикладами таких ризиків є кібератаки на критичну інфраструктуру, що вимагають координації між відомствами, відповідальними за кібербезпеку, енергетику, транспорт, комунікації; пандемії, що потребують узгодженої роботи систем охорони здоров'я, соціального захисту, освіти, економіки; вплив кліматичних змін на сільське господарство, водні ресурси, містобудування [25]. Для управління такими комплексними ризиками галузеві підрозділи повинні брати участь у міжвідомчих робочих групах, обмінюватися інформацією про релевантні загрози, узгоджувати стратегії реагування, проводити спільні навчання та симуляції кризових ситуацій. Галузевий рівень також взаємодіє із стратегічним рівнем

через регулярну звітність про статус управління ризиками, участь у формуванні національного реєстру ризиків, отримання методологічної підтримки та координаційних рекомендацій.

Регіональний рівень системи управління ризиками реалізується через органи місцевого самоврядування та територіальні підрозділи центральних органів виконавчої влади, які адаптують загальнодержавні та галузеві підходи до специфічних територіальних умов та викликів. Регіональні та місцеві органи влади стикаються з унікальними комбінаціями ризиків, що визначаються географічним розташуванням, економічною структурою регіону, демографічними характеристиками, історичною спадщиною, близькістю до кордонів чи зон конфлікту [8]. Наприклад, прикордонні регіони мають підвищені безпекові ризики, промислові регіони стикаються з екологічними та техногенними загрозами, сільськогосподарські території вразливі до погодних умов та коливань цін на продукцію, регіони з депресивною економікою мають ризики соціальної напруженості та відтоку населення.

Органи місцевого самоврядування формують регіональні та місцеві реєстри ризиків, що відображають територіальну специфіку загроз та враховують погляди місцевих громад на пріоритетні проблеми [20]. Процес ідентифікації ризиків на регіональному рівні повинен бути максимально інклюзивним, залучаючи представників бізнесу, громадських організацій, освітніх та наукових установ, активних громадян. Така інклюзивність не лише збагачує розуміння ризиків різноманітними перспективами, а й підвищує легітимність прийнятих рішень та готовність громади до співпраці в управлінні ризиками. Регіональний рівень відповідає за розробку та імплементацію місцевих стратегій управління ризиками, що узгоджуються з національними та галузевими підходами, але враховують територіальні пріоритети та доступні ресурси.

Важливою функцією регіонального рівня є забезпечення готовності до кризових ситуацій та координація оперативного реагування на локальні надзвичайні події. Це включає розробку планів цивільного захисту, організацію систем раннього попередження для природних катастроф, створення резервів критичних ресурсів, проведення регулярних навчань та тренувань служб реагування [23]. Регіональні органи також відповідають за комунікацію ризиків до місцевих громад, що вимагає адаптації повідомлень до культурного контексту, мовних особливостей, рівня освіти населення. Ефективна ризик-комунікація на місцевому рівні будує довіру між владою та громадянами, підвищує готовність населення до самозахисту, зменшує панічні реакції в кризових ситуаціях. Вертикальна інтеграція регіонального рівня з галузевим та стратегічним здійснюється через регулярну звітність про територіальні ризики, участь у загальнодержавних програмах управління ризиками, отримання методологічної та фінансової підтримки з вищих рівнів системи.

Система практичних інструментів управління ризиками має включати різноманітні методи та технології, адаптовані до специфіки публічного сектору та різних типів ризиків. Матриці ризиків становлять один з найпоширеніших та найбільш інтуїтивно зрозумілих інструментів візуалізації та пріоритизації ризиків [9]. Класична матриця 5х5 розташовує ризики на двовимірній площині, де одна вісь відображає ймовірність реалізації ризику (від дуже низької до дуже високої), а друга – потенційний вплив на організаційні цілі (від незначного до катастрофічного). Кожна комбінація ймовірності та впливу отримує кольорове

кодування (зелений – низький ризик, жовтий – середній, оранжевий – високий, червоний – критичний), що дозволяє швидко ідентифікувати ризики, які потребують першочергової уваги. Heat maps, або теплові карти ризиків, розширюють базову матрицю додатковими аналітичними можливостями, наприклад, використанням різних розмірів маркерів для відображення швидкості зростання ризику чи ступеня готовності до нього.

Для публічного сектору матриці ризиків повинні враховувати не лише фінансові втрати, а й широкий спектр наслідків, включаючи вплив на права людини, соціальну справедливість, довіру до влади, політичну стабільність, міжнародну репутацію [7]. Це вимагає розробки багатокритеріальних систем оцінювання впливу, де ризик може мати високий вплив не через монетарні втрати, а через загрозу фундаментальним цінностям чи довгострокову шкоду суспільним інтересам. Матриці ризиків також можуть бути диференційовані для різних часових горизонтів, оскільки деякі ризики є гострими та вимагають негайного реагування, тоді як інші розгортаються поступово протягом років чи десятиліть, але потенційно мають більш фундаментальний вплив. Динамічні матриці, що оновлюються в режимі реального часу на основі моніторингу ключових індикаторів, дозволяють відстежувати зміни в ризиковому ландшафті та своєчасно коригувати стратегії реагування.

Реєстри загроз або ризиків становлять структуровані бази даних, що консолідують інформацію про ідентифіковані ризики, їх характеристики, стратегії реагування, відповідальних осіб та статус управління [13]. Ефективний реєстр ризиків включає опис кожного ризику (що саме може статися), потенційні причини (чому це може статися), можливі наслідки (як це вплине на організацію), початкову оцінку (ймовірність та вплив до заходів реагування), заплановані заходи реагування (що будемо робити), відповідальних виконавців (хто відповідає), терміни (коли має бути зроблено), залишкову оцінку (очікувана ймовірність та вплив після заходів), індикатори раннього попередження (що моніторимо), статус (відкритий, закритий, реалізований). Реєстри повинні бути «живими» документами, що регулярно переглядаються та оновлюються, а не статичними звітами, складеними раз на рік для виконання формальних вимог.

В контексті публічного сектору реєстри ризиків виконують не лише внутрішньоорганізаційну функцію, а й слугують інструментом підзвітності та прозорості [25]. Публікація реєстрів ключових ризиків (з необхідним захистом чутливої інформації) дозволяє громадянам та парламенту розуміти, які загрози визнаються пріоритетними органами влади, які заходи вживаються для їх мітигації, як використовуються публічні ресурси. Ієрархія реєстрів – від локальних та проектних до відомчих, галузевих та національного – забезпечує можливість консолідації інформації та виявлення системних ризиків, що охоплюють множинні організації чи рівні управління. Інтеграція реєстрів ризиків з іншими управлінськими системами, такими як стратегічне планування, управління проектами, внутрішній аудит, дозволяє забезпечити, щоб ризикова інформація реально впливала на прийняття рішень, а не залишалася ізольованим набором даних.

Індикатори раннього попередження (Key Risk Indicators, KRI) становлять систему метрик, що дозволяють відстежувати зміни в ризиковому профілі та сигналізувати про наростання загроз до їх повної реалізації [4]. На відміну від індикаторів результативності (KPI), які вимірюють досягнення цілей, KRI фокусуються на моніторингу чинників, що можуть перешкодити досягнен-

ню цілей. Ефективні індикатори раннього попередження мають бути провідними (leading), а не запізнілими (lagging) – тобто змінюватися до реалізації ризику, а не після; вимірними та об'єктивними; доступними для регулярного моніторингу; релевантними для конкретного ризику; мати визначені порогові значення, перевищення яких тригерує певні дії. Наприклад, для ризику кібератаки індикаторами можуть бути кількість спроб несанкціонованого доступу, наявність вразливостей у програмному забезпеченні, час з останнього оновлення системи безпеки; для ризику соціальних протестів – рівень безробіття, індекси споживчих цін на критичні товари, активність в соціальних мережах навколо соціальних проблем.

Для публічного сектору розробка ефективних KRI є особливо складним завданням через множинність і різноманітність ризиків, обмеженість доступних даних для моніторингу, складність причинно-наслідкових зв'язків у соціальних системах [1]. Це вимагає креативного підходу до ідентифікації непрямих індикаторів та використання різноманітних джерел інформації, включаючи big data, соціальні медіа, сенсорні мережі, громадські звернення. Система моніторингу KRI повинна включати не лише автоматизоване відстеження кількісних метрик, а й систематичний аналіз якісної інформації з різних джерел для виявлення слабких сигналів наростаючих проблем. Важливим є визначення чіткої процедури ескалації та реагування, коли індикатор перевищує порогове значення – хто інформується, які аналізи проводяться, які заходи можуть бути активовані. Без таких процедур навіть ідеальна система індикаторів залишається марним навантаженням без практичної цінності.

Стрес-тестування публічних організацій передбачає систематичне моделювання екстремальних, але правдоподібних сценаріїв для оцінки стійкості систем та виявлення критичних вразливостей [15]. На відміну від традиційного ризик-аналізу, який фокусується на найбільш імовірних загрозах, стрес-тести досліджують здатність організації функціонувати в умовах реалізації рідкісних, але потенційно катастрофічних подій або комбінацій множинних ризиків. Наприклад, стрес-тест системи охорони здоров'я може моделювати одночасну пандемію, кібератаку на медичні інформаційні системи та масовий відтік медичного персоналу; стрес-тест енергетичної системи – тривалу холодну погоду, обмеження імпорту енергоносіїв та пошкодження критичної інфраструктури. Такі сценарії дозволяють виявити точки відмови, недостатність резервних потужностей, прогалини в планах безперервності, необхідні запаси критичних ресурсів.

Методологія стрес-тестування включає визначення критичних функцій, які повинна забезпечувати організація навіть в екстремальних умовах; розробку правдоподібних екстремальних сценаріїв на основі історичного досвіду, експертних оцінок, наукових прогнозів; симуляцію функціонування організації в умовах реалізації сценаріїв; ідентифікацію точок відмови та критичних вразливостей; розробку заходів з підвищення стійкості [16]. Для публічного сектору стрес-тестування має особливе значення через відповідальність держави за захист громадян та забезпечення критичних послуг навіть в умовах кризи. Регулярне проведення стрес-тестів, включаючи практичні симуляції та навчання, дозволяє не лише виявляти вразливості в планах, а й формувати організаційну культуру готовності, де персонал знає свої ролі та дії в кризових ситуаціях. Результати стрес-тестів повинні систематич-

но інкорпоруватися в оновлення планів безперервності, інвестиційні рішення щодо резервних потужностей, корекцію процедур та тренінги персоналу.

Сценарне планування становить стратегічний інструмент для управління довгостроковою невизначеністю через розробку альтернативних правдоподібних майбутніх, аналіз їх імплікацій та підготовку адаптивних стратегій [13]. На відміну від прогнозування, що намагається передбачити найбільш імовірне майбутнє, сценарне планування визнає фундаментальну непередбачуваність складних систем та готує організацію до множинних можливих траєкторій розвитку подій. Процес сценарного планування включає ідентифікацію ключових невизначеностей, що можуть суттєво вплинути на організацію; визначення критичних драйверів, що будуть формувати майбутнє; конструювання кількох (типово 3-4) внутрішньо несуперечливих сценаріїв, що охоплюють простір можливих майбутніх; аналіз імплікацій кожного сценарію для організаційних цілей та стратегій; розробку адаптивних стратегій, що будуть ефективними в множинних сценаріях або дозволять швидко переорієнтуватися при зміні траєкторії розвитку подій.

Для публічного сектору сценарне планування є критично важливим інструментом через необхідність формування довгострокових політик в умовах високої невизначеності та irreversibility багатьох урядових рішень [21]. Наприклад, сценарії майбутнього енергетичної системи повинні враховувати невизначеність темпів переходу на відновлювану енергетику, технологічних проривів у зберіганні енергії, геополітичних змін на ринках енергоносіїв; сценарії розвитку системи освіти – демографічні зрушення, трансформацію ринку праці через автоматизацію, зміни в суспільних цінностях та очікуваннях. Сценарне планування дозволяє уникнути пасток лінійного екстраполювання поточних трендів та готує органи влади до можливих стрибкоподібних змін. Важливим аспектом є використання сценаріїв не для вибору «правильної» стратегії, а для формування адаптивних портфелів політик, що включають як універсальні дії (що мають сенс в усіх сценаріях), так і контингентні плани для специфічних траєкторій розвитку подій.

Bow-tie діаграми надають візуальний метод для аналізу причин та наслідків ризиків, а також планування превентивних та контингентних заходів [18]. Діаграма має форму метелика (bow-tie), де центральна небезпечна подія (наприклад, витік хімічних речовин, кібератака, корупційний скандал) з'єднується ліворуч з причинами, що можуть призвести до цієї події, та праворуч з можливими наслідками. На лівій стороні розміщуються превентивні бар'єри – заходи, що знижують імовірність реалізації події (наприклад, системи безпеки, процедури перевірки, тренінги персоналу). На правій стороні розташовуються заходи контролю наслідків (recovery controls) – дії для мінімізації впливу, якщо подія все ж відбулася (наприклад, системи автоматичного гасіння пожежі, плани комунікації з громадськістю, процедури відновлення даних). Кожен бар'єр оцінюється з точки зору ефективності та надійності, що дозволяє виявити слабкі ланки в системі захисту.

Для публічного сектору bow-tie діаграми особливо корисні при аналізі комплексних ризиків з множинними причинами та каскадними наслідками [7]. Наприклад, bow-tie для ризику кібератаки на державні інформаційні системи може включати причини (вразливості програмного забезпечення, соціальна

інженерія, інсайдери, недостатня обізнаність персоналу) та наслідки (розголошення персональних даних, порушення надання послуг, втрата довіри, фінансові втрати). Превентивні бар'єри можуть включати багатофакторну автентифікацію, регулярні оновлення безпеки, тренінги з кібергігієни, системи виявлення аномалій; контрольні заходи – плани відновлення даних з резервних копій, процедури інцидент-менеджменту, системи резервування критичних функцій, протоколи комунікації зі стейкхолдерами. Систематичне застосування bow-tie аналізу для пріоритетних ризиків дозволяє виявляти прогалини в системі захисту, оптимізувати інвестиції в превентивні та контингентні заходи, формувати цілісне розуміння ризиків серед менеджерів та персоналу.

Методології FMEA (Failure Mode and Effects Analysis) та FMECA (додатково включає Criticality Analysis) надають систематичний підхід до ідентифікації потенційних точок відмови в процесах та системах, оцінювання їх впливу та пріоритизації заходів з підвищення надійності [17]. FMEA включає декомпозицію системи або процесу на компоненти, для кожного компонента ідентифікацію можливих режимів відмови (як саме може відмовити), аналіз причин кожного режиму відмови, оцінювання наслідків для системи в цілому, визначення пріоритетності через індекс RPN (Risk Priority Number), що обчислюється як добуток оцінок тяжкості наслідків, ймовірності виникнення та складності виявлення проблеми. Компоненти з високим RPN потребують першочергових заходів з редизайну, додаткових перевірок, резервування функцій. FMECA додає аналіз критичності, що враховує не лише частоту та наслідки відмов, а й важливість функції для місії системи.

У контексті публічного сектору FMEA/FMECA особливо корисні при аналізі критичних процесів надання послуг, складних адміністративних процедур, інформаційних систем [6]. Наприклад, FMEA процесу видачі паспортів може виявити точки, де можливі помилки або затримки (невірні дані в заяві, технічні збої друку, недоступність баз даних, проблеми доставки), їх причини та наслідки для громадян. Це дозволяє цілеспрямовано вдосконалювати процес через спрощення процедур, автоматизацію перевірок, створення резервних механізмів, поліпшення навчання персоналу. FMECA критичних інфраструктурних систем допомагає пріоритизувати інвестиції в модернізацію та резервування на основі аналізу того, відмова яких компонентів має найбільш критичні наслідки для виконання публічних функцій. Систематичне застосування цих методологій формує культуру проактивного виявлення та усунення потенційних проблем до їх реалізації.

Культурна трансформація для впровадження ефективного управління ризиками становить, можливо, найскладніший, але найважливіший аспект удосконалення ризик-менеджменту в публічному секторі. Навіть найдосконаліші методології та інструменти залишаться формальними процедурами без реального впливу, якщо не сформовано організаційну культуру, що цінує проактивну ідентифікацію та відкрите обговорення ризиків, підтримує обґрунтоване ризик-прийняття, навчається на помилках [10]. Традиційна бюрократична культура публічного сектору часто створює бар'єри для ефективного управління ризиками через акцент на дотримання правил замість досягнення результатів, покарання за помилки замість навчання, ієрархічне приховування проблем замість прозорої комунікації ризиків [24].

Навчання та розвиток компетентностей персоналу становлять фундамент культурної трансформації. Програми навчання управлінню ризиками повинні бути диференційованими для різних цільових груп з урахуванням їх ролей та потреб [4]. Для вищих керівників необхідні короткі, стратегічно орієнтовані програми, що формують розуміння цінності ризик-менеджменту для організаційної результативності, демонструють успішні кейси, надають інструменти для включення ризикових міркувань у процеси прийняття рішень та стратегічного планування. Для середніх менеджерів потрібні більш детальні програми, що охоплюють методології ідентифікації та оцінювання ризиків, розробку та імплементацію планів реагування, моніторинг та звітність, координацію між підрозділами. Для спеціалізованих ризик-менеджерів необхідне глибоке технічне навчання з використання аналітичних інструментів, статистичних методів, специфічних методологій типу FMEA чи Monte Carlo. Для всього персоналу потрібна базова обізнаність про принципи управління ризиками, їх роль в ідентифікації загроз, канали комунікації проблем.

Навчання має поєднувати теоретичні знання з практичними навичками через використання реалістичних кейсів, симуляцій, настільних вправ [27]. Особливо ефективними є програми, що базуються на аналізі реальних кризових ситуацій з власної організації або аналогічних публічних установ – такі кейси мають високу релевантність та емоційний вплив, що посилює навчальний ефект. Важливим аспектом є не лише початкове навчання, а й безперервний професійний розвиток через регулярні освіжаючі курси, участь у професійних асоціаціях ризик-менеджерів, обмін досвідом з колегами з інших організацій та країн. Система сертифікації фахівців з управління ризиками в публічному секторі може підвищити професійний статус цієї функції та забезпечити стандарти компетентності.

Створення ефективних каналів комунікації ризиків як по вертикалі (між рівнями ієрархії), так і по горизонталі (між підрозділами) є критичним для функціонування інтегрованої системи управління ризиками [1]. Вертикальні канали повинні забезпечувати швидку ескалацію критичних ризиків до вищого керівництва, що вимагає визначення чітких критеріїв, які ризики та коли ескалюються, процедур повідомлення, очікуваних часових рамок реагування. Горизонтальна комунікація між підрозділами є критично важливою для управління міжфункціональними ризиками, що не вписуються в межі відповідальності одного департаменту [25]. Регулярні міжвідомчі зустрічі з обговорення ризиків, спільні воркшопи з ідентифікації системних загроз, практики job rotation для формування розуміння взаємозалежностей сприяють горизонтальній інтеграції. Призначення «ризик-чемпіонів» (risk champions) в різних підрозділах – осіб, що мають додаткову підготовку з управління ризиками та виконують роль промоутерів ризикової культури у своїх підрозділах та зв'язкових осіб з центральним ризик-офісом – формує мережу комунікації та впливу.

Врахування української специфіки є критично важливим для забезпечення реалістичності та ефективності концептуальної моделі удосконалення механізмів управління ризиками. Функціонування публічного сектору в умовах воєнного стану радикально трансформує ризиковий ландшафт та вимагає адаптації стандартних підходів до управління ризиками. Повномасштабна війна створює множинні специфічні ризики –

пряма військова загроза для населення та інфраструктури в окремих регіонах, масштабні руйнування критичної інфраструктури, енергетична вразливість через систематичні атаки на енергосистему, масові внутрішні переміщення населення, економічна дестабілізація через втрату виробничих потужностей та експортних ринків. Ці ризики часто реалізуються одночасно та підсилюють один одного, створюючи каскадні ефекти, що вимагають інтегрованих стратегій реагування.

Система управління ризиками в умовах воєнного стану повинна враховувати необхідність балансування між короткостроковими потребами виживання та довгостроковими завданнями розбудови стійких інституцій. З одного боку, органи влади мають оперативно реагувати на гострі кризові ситуації – забезпечувати евакуацію населення з зон бойових дій, відновлювати пошкоджену інфраструктуру, координувати гуманітарну допомогу. З іншого боку, не можна відкладати системну роботу з ідентифікації та мітигації стратегічних ризиків, що формуватимуть майбутнє країни після завершення активної фази конфлікту – демографічні наслідки війни, травматизація населення, можливість повторної агресії, виклики реінтеграції тимчасово окупованих територій [9]. Адаптивна матриця ризиків для воєнного стану може включати додатковий вимір «тривалості впливу» (короткостроковий, середньостроковий, довгостроковий), що дозволяє балансувати увагу до різних часових горизонтів.

Обмежені ресурси публічного сектору України в умовах війни та економічної кризи вимагають особливо ретельної пріоритизації ризиків та оптимізації витрат на управління загрозами. Принцип пропорційності набуває критичного значення – неможливо інвестувати рівномірно в управління всіма ідентифікованими ризиками, необхідно концентрувати обмежені ресурси на найбільш критичних загрозах. Це вимагає розробки строгих критеріїв пріоритизації, що враховують не лише імовірність та вплив ризиків, а й наявність альтернатив, можливість міжнародної підтримки, синергії між заходами реагування на різні ризики. Креативні підходи до мобілізації ресурсів – залучення міжнародної технічної допомоги, партнерства з громадським сектором та бізнесом, використання волонтерського потенціалу – можуть розширити можливості управління ризиками за обмеженого державного бюджету.

Цифровізація публічного сектору, яка прискорилася в Україні протягом останніх років, трансформує як ризиковий ландшафт, так і можливості для управління ризиками. З одного боку, цифрові технології створюють нові ризики – кібератаки на державні інформаційні системи, цифрову нерівність через обмежений доступ окремих груп населення до онлайн-послуг, вразливість до технологічних збоїв, ризики приватності та захисту персональних даних [3]. Ефективна система управління ризиками повинна включати спеціалізовані підрозділи з управління кіберризиками, регулярне тестування стійкості критичних систем до атак, розробку планів безперервності для випадків масштабних технологічних збоїв, етичні рамки для використання даних. З іншого боку, цифрові технології надають потужні інструменти для покращення управління ризиками – big data analytics для виявлення патернів та раннього попередження, штучний інтелект для автоматизації моніторингу та прогнозування, цифрові платформи для координації між відомствами, blockchain для забезпечення прозорості та незмінності критичної інформації.

Механізми імплементації концептуальної моделі повинні забезпечити поступовий, реалістичний перехід від поточного стану до бажаної інтегрованої системи управління ризиками. Пілотні проекти в обраних відомствах чи регіонах дозволяють протестувати запропоновані підходи, ідентифікувати практичні виклики, адаптувати методології та інструменти до специфічних контекстів перед масштабуванням на весь публічний сектор. Вибір пілотних організацій повинен враховувати як їхню готовність та спроможність (ліпше почати з більш зрілих організацій, які мають шанс на успіх), так і різноманітність контекстів (щоб протестувати адаптивність підходів). Детальна документація та аналіз досвіду пілотів, включаючи як успіхи, так і проблеми, формує базу знань для подальшого масштабування (табл. 1).

Таблиця 1. Система практичних інструментів управління ризиками для публічного сектору України

Table 1. System of practical risk management tools for the public sector of Ukraine

Інструмент Tool	**Призначення Purpose**	**Методологія застосування Methodology of application**	**Адаптація до публічного сектору Adaptation to the public sector**	**Специфіка для воєнного стану Specifics for martial law**
1) Матриці ризиків	Візуалізація та пріоритизація загроз	Оцінка ймовірності та впливу з кольоровим кодуванням	Багатокритеріальне оцінювання (не лише фінансові втрати)	Додатковий вимір «тривалості впливу»
2) Реєстри ризиків	Структуровані бази даних загроз	Систематична документація з постійним оновленням	Інструмент підзвітності та прозорості	Ієрархічна консолідація від локального до національного
3) Key Risk Indicators	Раннє попередження про загрози	Моніторинг провідних метрик з встановленими порогами	Використання аналітики великих даних та соціальних медіа	Інтеграція з системами національної безпеки
4) Стрес-тестування	Оцінка стійкості до екстремальних сценаріїв	Моделювання комплексних катастрофічних подій	Фокус на критичних публічних функціях	Симуляція каскадних ефектів військових дій
5) Bow-tie діаграми	Аналіз причин та наслідків ризиків	Візуальний метод планування превентивних заходів	Врахування множинних стейкхолдерів	Аналіз гібридних загроз
6) FMEA/ FMECA	Ідентифікація точок відмови систем	Систематична декомпозиція з RPN індексами	Застосування до процесів надання послуг	Аналіз критичної інфраструктури

**Джерело: розробка автора.*

**Source: author's development.*

Поетапне впровадження передбачає розбиття трансформації на керовані фази з чіткими цілями, критеріями успіху та часовими рамками для кожної фази [6]. Розумна послідовність може включати: 1) створення мінімально необхідної інституційної інфраструктури (центральний координаційний орган, базові нормативні документи), 2) пілотування в обраних організаціях,

3) масштабування на центральні органи виконавчої влади, 4) поширення на регіональний рівень та місцеве самоврядування, 5) поглиблення інтеграції з іншими управлінськими системами. Кожна фаза будується на досягненнях попередньої, дозволяючи акумулювати досвід та адаптувати підходи. Важливо встановлювати реалістичні часові рамки – глибока культурна трансформація вимагає років, а не місяців, і спроби штучного прискорення часто призводять до формальних систем без реального впливу на організаційну поведінку.

Висновки з даного дослідження і перспективи подальших досліджень. Удосконалення механізмів управління ризиками в публічному секторі України вимагає системної багатовимірної трансформації, що інтегрує принципові засади, інституційну архітектуру, процесні механізми, практичні інструменти та організаційну культуру в цілісну модель. Запропонована концептуальна модель базується на дванадцяти базових принципах, що формують концептуальний фундамент ефективного ризик-менеджменту: системність, проактивність, адаптивність, інклюзивність, прозорість, пропорційність, доказовість, безперервність, інтегрованість, стійкість, етичність та інноваційність. Ці принципи забезпечують орієнтири для розбудови системи, що не лише формально відповідає міжнародним стандартам, а й є функціонально ефективною в специфічному українському контексті.

Багаторівнева архітектура системи управління ризиками забезпечує необхідний баланс між централізованою координацією та децентралізованою адаптацією до специфічних контекстів. Стратегічний рівень через Центральний орган координації забезпечує методологічну єдність, координацію міжсекторальних зусиль, моніторинг національних ризиків та інтеграцію управління ризиками зі стратегічним плануванням. Галузевий рівень через відомчі підрозділи управління ризиками операціоналізує загальні підходи в контексті специфічних секторальних викликів та забезпечує горизонтальну координацію для управління міжвідомчими ризиками. Регіональний рівень адаптує підходи до територіальних особливостей, залучає місцеві громади та забезпечує оперативне реагування на локальні кризові ситуації.

Система практичних інструментів, включаючи матриці ризиків, реєстри загроз, індикатори раннього попередження, стрес-тестування, сценарне планування, bow-tie діаграми, FMEA/FMECA надає публічним організаціям конкретні методології для ідентифікації, аналізу, оцінювання та моніторингу ризиків. Адаптація цих інструментів до специфіки публічного сектору з урахуванням множинності стейкхолдерів, неринкових цілей, обмежених ресурсів забезпечує їх практичну застосовність та цінність для підтримки управлінських рішень.

Культурна трансформація через цілеспрямоване навчання персоналу, перебудову систем мотивації, формування психологічної безпеки, створення ефективних каналів комунікації є, можливо, найскладнішим, але найбільш критичним аспектом удосконалення управління ризиками. Без глибинних змін в організаційній культурі, що перетворюють управління ризиками з формальної процедури на інтегровану частину повсякденного управлінського мислення, навіть найдосконаліші методології залишаться паперовими вправами без реального впливу на організаційну стійкість.

Врахування української специфіки – функціонування в умовах воєнного стану, обмежені ресурси, корупційні виклики, євроінтеграційні зобов'язання, прискорена цифровізація – є гострим важливим для забезпечення

реалістичності та ефективності запропонованої моделі. Адаптивні підходи, що балансують між короткостроковими потребами виживання та довгостроковими завданнями інституційної розбудови, використовують можливості міжнародної підтримки та технологічних інновацій, дозволяють трансформувати обмеження у можливості для стрибкоподібного розвитку.

У цілому успішна реалізація запропонованої моделі суттєво підвищить спроможність вітчизняного публічного сектору запобігати кризовим ситуаціям, ефективно реагувати на реалізовані ризики, швидко відновлюватися після потрясінь та навчатися на досвіді для підвищення майбутньої готовності. Також запропонована концептуальна модель відкриває широкі можливості для подальших емпіричних досліджень та теоретичного розвитку проблематики управління ризиками в публічному секторі. Пріоритетним напрямом є емпірична верифікація запропонованих принципів та інструментів через лонгітюдні дослідження процесів імплементації системи ризик-менеджменту в українських органах публічної влади різних рівнів, що дозволить виявити специфічні бар'єри, каталізатори та критичні фактори успіху трансформації в умовах воєнного стану та обмежених ресурсів.

Стаття надійшла до редакції 20.08.2025 р.
Стаття рекомендована до друку 06.10.2025 р.
Опубліковано 30.12.2025 р.

Klochko Ivan Andriyovich,
PhD student of the Department of Public Policy, Education and Research Institute of Public Administration, V. N. Karazin Kharkiv National University,
4, Svobody Sq., Kharkiv, 61022, Ukraine

https://orcid.org/0009-0007-4881-7107

IMPROVEMENT OF RISK MANAGEMENT MECHANISMS IN THE PUBLIC SECTOR

Abstract. This article addresses the critical inadequacy of reactive risk management approaches in Ukraine's public sector, which operates under unprecedented uncertainty conditions including full-scale war, prolonged economic instability, accelerated digitization, demographic shifts, and climate change. The research identifies fundamental systemic vulnerabilities in current risk management practices: fragmented risk identification and assessment processes, absence of comprehensive threat management methodology, weak integration of risk management into strategic planning and decision-making processes, and predominant reactive response models rather than proactive threat anticipation and prevention. The study reveals that Ukrainian public sector organizations, constrained by traditional bureaucratic culture and rigid hierarchical structures, demonstrate structural inability to rapidly adapt to sudden changes in security, economic, and social environments. Information disconnection between different agencies prevents formation of comprehensive understanding of interconnected risks spanning multiple public administration spheres simultaneously. The absence of unified standards for risk classification, assessment, and reporting makes comparison and consolidation of risk information at national level impossible. The research develops a comprehensive conceptual model for systematic multidimensional transformation encompassing fundamental principles, institutional architecture, procedural mechanisms, practical tools, and organizational culture. Twelve foundational principles form the conceptual framework: systematicity, proactivity, adaptability, inclusiveness, transparency, proportionality, evidence-based approach, continuity, integration, resilience, ethics, and innovation. The multilevel architecture operates across strategic, sectoral, and regional levels, with the strategic level establishing a Central Risk Management Coordination Body within the Cabinet of Ministers, sectoral level implementing specialized risk management units in central exec-

utive bodies, and regional level adapting approaches to territorial specificities while engaging local communities. The practical toolkit integrates risk matrices, threat registers, key risk indicators, stress testing, scenario planning, bow-tie diagrams, and FMEA/FMECA methodologies specifically adapted for public sector characteristics. Cultural transformation through systematic personnel training, restructured motivation systems, and effective communication channels represents the most critical transformation aspect, converting formal procedures into integrated components of daily management thinking. The model specifically addresses Ukrainian wartime realities including martial law operations, resource limitations, corruption challenges, European integration commitments, and accelerated digitization. Implementation mechanisms include pilot projects, phased rollout, and adaptive approaches balancing short-term survival needs with long-term institutional development goals. Successful realization will fundamentally transform Ukrainian public sector capabilities from reactive crisis response to proactive risk anticipation, prevention, and organizational resilience building.

Keywords: public administration, risk management, public sector, integrated system, adaptability, organizational culture, strategic planning.

REFERENCES

1. Agyepong, L.A., & Liang, X. (2023). Mapping the knowledge frontiers of public risk communication in disaster risk management. *Journal of Risk Research, 26(3), 302–323*. https://doi.org/10.1080/13669877.2022.2127851

2. Alberts, D.S., & Hayes, R.E. (2006). *Understanding Command and Control*. Washington: CCRP Publication Series.

3. Alon-Barkat, S., & Busuioc, M. (2023). Human–AI interactions in public sector decision making: «Automation bias» and «selective adherence» to algorithmic advice. *Journal of Public Administration Research and Theory, 33(1), 153–169*. https://doi.org/10.1093/jopart/muac007

4. Andersen, T.J., & Young, P.C. (2023). Enhancing public sector enterprise risk management through interactive information processing. *Frontiers in Research Metrics and Analytics, 8*. https://doi.org/10.3389/frma.2023.1239447

5. Bracci, E., Tallaki, M., Gobbo, G., & Papi, L. (2021). Risk Management in the Public Sector: A Structured Literature Review. *International Journal of Public Sector Management, 34(2), 205–223*. https://doi.org/10.1108/IJPSM-02-2020-0049

6. Braumann, E.C., Hiebl, M.R.W., & Posch, A. (2024). Enterprise Risk Management as Part of the Organizational Control Package: Review and Implications for Management Accounting Research. *Journal of Management Accounting Research, 36(2), 7–29*. https://doi.org/10.2308/JMAR-2021-071

7. Bullock, J.B., Greer, R.A., & O'Toole Jr., L.J. (2019). Managing Risks in Public Organizations: a Conceptual Foundation and Research Agenda. *Perspectives on Public Management and Governance, 2(1), 75–87*. https://doi.org/10.1093/ppmgov/gvx016

8. Caldarulo, M., & Welch, E.W. (2023). Organizational Risk Perception in Public Agencies: The Role of Contracting and Scientific and Professional Information. *Public Management Review, 26(3), 746–771*. https://doi.org/10.1080/14719037.2023.2191629

9. Carlucci, P., & Mumford, A. (2023). Hybrid Warfare: The Continuation of Ambiguity by Other Means. *European Journal of International Security, 8(2), 192–206*. https://doi.org/10.1017/eis.2022.19

10. Christensen, C.M. (2016). *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*. Boston: Harvard Business Review Press.

11. COSO. (2017). *Enterprise Risk Management – Integrating with Strategy and Performance*. Committee of Sponsoring Organizations of the Treadway Commission. URL: https://www.coso.org/guidance-erm

12. Dannreuther, R. (2007). *International Security: The Contemporary Agenda*. Cambridge: Polity Press.

13. De Lorena, A.L.F., & Costa, A.P.C.S. (2024). PRisk-MM: a public sector risk management maturity model for Brazilian public organizations. *Journal of Risk Research, 27(1), 46–62*. https://doi.org/10.1080/13669877.2023.2293039

14. Garvin, D.A., Edmondson, A.C., & Gino, F. (2008). Is Yours a Learning Organization? *Harvard Business Review, 86(3), 109–116*.

15. Gourbier, J., Iacuzzi, S., Padovani, E., & Saliterer, I. (2024). Risk Management in the Public Sector: A Comparative Analysis of Central Government Settings in France, Germany, and Italy. *Financial Accountability & Management, 1–15*. https://doi.org/10.1111/faam.12416

16. Hillmann, J., & Guenther, E. (2021). Organizational Resilience: A Valuable Construct for Management Research? *International Journal of Management Reviews, 23(1), 7–44*. https://doi.org/10.1111/ijmr.12239

17. Hood, C., Rothstein, H., & Baldwin, R. (2001). *The Government of Risk: Understanding Risk Regulation Regimes*. Oxford: Oxford University Press.

18. ISO 31000:2018. (2018). *Risk management – Guidelines. International Organization for Standardization*. URL: https://www.iso.org/standard/65694.html

19. Kaplan, R.S., & Norton, D.P. (2008). *The Execution Premium: Linking Strategy to Operations for Competitive Advantage*. Boston: Harvard Business Press.

20. Kapuścińska, K., & Matejun, M. (2014). Risk Management in Public Sector Organizations: A Case Study of Local Government. *International Journal of Business and Management, 2(3), 129–143*.

21. Kuchta, D., Canonico, P., Capone, V., & Capaldo, G. (2023). Uncertainty in public projects. *Administrative Sciences, 13(3)*. https://doi.org/10.3390/admsci13060145

22. Nye, J.S. (2011). *The Future of Power*. New York: PublicAffairs.

23. Power, M. (2007). *Organized Uncertainty: Designing a World of Risk Management*. Oxford: Oxford University Press.

24. Senge, P.M. (2006). *The Fifth Discipline: The Art and Practice of the Learning Organization*. New York: Doubleday.

25. Tangsgaard, E.R., & Fischer, C. (2024). Disentangling Risk Management and Error Management in the Public Sector: A Theoretical Framework. *The American Review of Public Administration*. https://doi.org/10.1177/02750740241229996

26. Weissmann, M., Nilsson, N., Thune, H., & Palosaari, T. (2021). *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. London: I.B. Tauris.

27. Young, P.C., & Hoang, K. (2023). Reshaping Public Sector (Enterprise) Risk Management. *International Journal of Public Administration*. https://doi.org/10.1080/01900692.2023.2197170

The article was received by the editors 20.08.2025.
The article is recommended for printing 06.10.2025.
Published 30.12.2025.