УДК 338.27:005.334
JEL classification: H56, H54, H12, D81
https://doi.org/10.31891/dsim-2025-12(31)

ФОРМУВАННЯ МЕХАНІЗМУ УПРАВЛІННЯ РИЗИКАМИ В ПРОЦЕСІ РОЗВИТКУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

ЧОБІТОК Вікторія
доктор економічних наук, професор, в.о. завідувача кафедри маркетингу та торговельного підприємництва
ННІ «Українська інженерно-педагогічна академія»
Харківського національного університету імені В.Н. Каразіна
https://orcid.org/0000-0002-5272-388X
e-mail: viktoriia.chobitok@karazin.ua

ГАВРИШ Ольга
доцент, кандидат економічних наук, доцент кафедри маркетингу та торговельного підприємництва
ННІ «Українська інженерно-педагогічна академія»
Харківського національного університету імені В.Н. Каразіна
https://orcid.org/0000-0003-1438-7528
e-mail: olga.gavrysh@karazin.ua

Сучасні безпекові виклики, спричинені воєнною агресією Російської Федерації проти України, глобальними кризами та зростанням кіберзагроз, істотно посилюють важливість забезпечення ефективного функціонування критичної інфраструктури. Масштабні руйнування енергетичних, транспортних, комунальних та інформаційно-комунікаційних систем виявили високий рівень уразливості національних інфраструктурних об'єктів до комплексних ризиків, підтвердивши необхідність переходу від реактивних заходів до системного, випереджального управління загрозами. В умовах післявоєнного відновлення, цифрової трансформації та стратегічного курсу України на інтеграцію до європейського безпекового простору ключового значення набуває формування ефективного механізму управління ризиками, здатного забезпечувати стійкість, адаптивність і безперервність роботи критично важливих секторів.

Попри наявність нормативно-правових актів і окремих інституційних ініціатив, в Україні досі відсутня цілісна модель ризик-менеджменту, орієнтована не лише на захист, а й на модернізацію та відновлення критичної інфраструктури в кризових умовах. Сучасна практика залишається фрагментарною та здебільшого зосередженою на реагуванні, а недостатня координація між державними структурами, регіонами та операторами об'єктів ускладнює обмін даними й уповільнює ухвалення рішень. Це знижує ефективність безпекових заходів і стримує реалізацію інноваційних та інвестиційних проєктів, необхідних для модернізації критичних секторів.

Метою дослідження є розроблення науково обґрунтованого механізму управління ризиками в процесі розвитку критичної інфраструктури України, який забезпечить підвищення рівня національної стійкості, здатність систем життєзабезпечення протидіяти воєнним, кібер- та техногенним загрозам і підтримувати безперервність функціонування. Запропонована модель ґрунтується на інтеграції організаційної, економічної, нормативно-правової, інформаційно-аналітичної та технічної складових, що формують єдиний комплекс заходів з виявлення, оцінювання, мінімізації та моніторингу ризиків.

Поетапний підхід до формування механізму управління ризиками охоплює ідентифікацію загроз, аналіз їх імовірності та наслідків, розробку превентивних і реагувальних заходів, постійний моніторинг та комунікацію між усіма суб'єктами ризик-менеджменту. Узгоджене функціонування цих елементів забезпечує системність процесу, сприяє зміцненню стійкості критичної інфраструктури й підвищує готовність до дій у надзвичайних ситуаціях.

Таким чином, формування комплексного механізму управління ризиками є необхідною передумовою забезпечення безпеки та сталого розвитку критично важливих секторів економіки України. Інтеграція правових, організаційних, технічних, економічних та аналітичних інструментів створює підґрунтя для ефективного протидії сучасним воєнним і гібридним загрозам та забезпечення довгострокової національної стійкості.

Ключові слова: критична інфраструктура; управління ризиками; механізм ризик-менеджменту; стійкість; безпека; розвиток; цифровізація; нормативно-правове регулювання; інформаційно-аналітична система; стратегічне управління.

DEVELOPMENT OF A RISK MANAGEMENT MECHANISM IN THE PROCESS OF UKRAINE'S CRITICAL INFRASTRUCTURE ADVANCEMENT

CHOBITOK Viktoriia, GAVRISH Olha
National Research Institute "Ukrainian Engineering Pedagogical Academy"
V.N. Karazin Kharkiv National University

Modern security challenges caused by the armed aggression of the Russian Federation against Ukraine, global crisis processes, and the growing number of cyber threats significantly increase the importance of ensuring the effective functioning of the country's critical infrastructure. Large-scale destruction of energy, transport, utility, and information and communication systems has demonstrated the high vulnerability of national infrastructure to complex risks, confirming the need to shift from reactive measures to systematic and anticipatory risk management. In the context of post-war recovery, digital transformation, and Ukraine's strategic integration into the European security space, developing an effective risk management mechanism capable of ensuring the resilience, adaptability, and continuity of critical sectors becomes a priority.

Despite the existence of certain legal acts and institutional initiatives, Ukraine still lacks a holistic risk management model focused not only on protection but also on the modernization and reconstruction of critical infrastructure under crisis

conditions. Current practices remain fragmented and predominantly oriented toward response rather than prevention or forecasting of threats. Insufficient coordination between government bodies, regional authorities, and critical infrastructure operators complicates information exchange, slows decision-making, and reduces the effectiveness of security measures. This also hinders the implementation of investment and innovation projects essential for the modernization of critical sectors.

The purpose of this study is to develop a scientifically grounded mechanism for risk management in the development of Ukraine's critical infrastructure that will enhance national resilience, strengthen the capacity of life-support systems to withstand military, cyber, and technogenic threats, and ensure the continuity of their functioning. The proposed model is based on the integration of organizational, economic, legal, information-analytical, and technical components, forming a unified system for identifying, assessing, minimizing, and monitoring risks.

The step-by-step approach to building the risk management mechanism includes threat identification, analysis of their probability and consequences, development of preventive and response measures, continuous monitoring, and communication among all stakeholders. The coordinated functioning of these elements ensures the system's integrity, strengthens the resilience of critical infrastructure, and enhances readiness for emergency situations.

Thus, forming a comprehensive risk management mechanism is a necessary prerequisite for ensuring the security and sustainable development of Ukraine's critical infrastructure sectors. The integration of legal, organizational, technical, economic, and analytical tools creates a foundation for effective counteraction to modern military and hybrid threats and strengthens long-term national resilience.

Keywords: critical infrastructure; risk management; risk management mechanism; resilience; security; development; digitalization; regulatory framework; information-analytical system; strategic management.

Стаття надійшла до редакції / Received 01.10.2025
Прийнята до друку / Accepted 12.11.2025

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Сучасні виклики та проблеми розвитку інфраструктури, зумовлені негативним впливом воєнної агресії, глобальними кризовими процесами та зростанням кіберзагроз, які істотно підвищили значення ефективного функціонування критичної інфраструктури держави. Руйнування енергетичних, транспортних, комунальних та інформаційно-комунікаційних систем засвідчили вразливість національної інфраструктури до комплексних ризиків і необхідність переходу від реактивного до системного управління ними.

В умовах післявоєнного відновлення, цифрової трансформації та інтеграції України до європейського безпекового простору особливої ваги набувають формування дієвого механізму управління ризиками, який забезпечуватиме не лише захист, а й сталий розвиток критичних секторів держави. Розроблення та впровадження такої системи надасть змогу своєчасно ідентифікувати загрози, мінімізувати їх наслідки, забезпечити безперервність функціонування життєво важливих об'єктів і підвищити загальний рівень національної стійкості.

Наявність окремих нормативно-правових актів та інституційних ініціатив у сфері захисту критичної інфраструктури в Україні є підгрунтям того, що досі відсутня цілісна, системно вибудувана модель управління ризиками, орієнтована на розвиток і відновлення об'єктів у кризових умовах. Сучасна практика управління ризиками залишається фрагментарною, переважно спрямованою на реагування, а не на попередження або прогнозування загроз.

Недостатня координація між державними органами, регіональними структурами та операторами об'єктів критичної інфраструктури ускладнює обмін інформацією, уповільнює ухвалення управлінських рішень і знижує ефективність заходів безпеки. Відсутність інтегрованої системи ризик-менеджменту також гальмує реалізацію інвестиційно-інноваційних проєктів, необхідних для модернізації критичних секторів.

Отже, існує об'єктивна потреба у формуванні обґрунтованого механізму управління ризиками, який забезпечить узгодженість дій усіх суб'єктів, своєчасну ідентифікацію загроз, мінімізацію ризиків і підтримання безперервного розвитку критичної інфраструктури України в умовах зростаючих воєнних та гібридних викликів.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Проблематика управління ризиками у сфері критичної інфраструктури та суміжних галузях широко представлена у вітчизняних напрацюваннях, однак переважно розглядається фрагментарно - крізь призму безпеки, окремих технічних рішень чи нормативного забезпечення. У працях Н. О. Євтушенко та А. А. Захаржевської обґрунтовано перехід від реактивного до системного, проактивного ризик-менеджменту, інтегрованого в інвестиційні та інноваційні процеси. Авторки акцентують на зв'язку між «механізмом розвитку» та «механізмом управління ризиками», що є методологічно важливим для перенесення підприємницьких підходів у публічну сферу та інфраструктурні сектори [1].

У дослідженні О. М. Возненка акцентовано роль держави як координатора політики безпеки: визначення правил, уніфікація процедур, міжвідомча взаємодія й адаптація до міжнародних стандартів (ISO 31000, ISO 22301 тощо). Підкреслюється потреба у цілісній моделі, що поєднує державне регулювання, галузеві механізми та інструменти операторів об'єктів [2].

Робота А. О. Магомедова систематизує спектр загроз (фізичних, кібернетичних, організаційних) і пропонує напрями їх нейтралізації, однак зосереджується головно на аспектах безпеки та захисту, меншою мірою - на інтеграції ризик-менеджменту в процеси модернізації та розвитку [3].

Узагальнюючи, наявні публікації забезпечують важливу теоретико-методичну базу щодо класифікації ризиків, формуванню підходів до оцінювання, визначення ролі державного регулювання тощо. Проте залишається проблематика в формуванні механізму управління ризиками в процесі розвитку критичної інфраструктури: бракує моделей, що синхронізують правове забезпечення, інституційну координацію, фінансово-економічні інструменти, цифрові платформи моніторингу та технічну модернізацію у єдиному інтегрованому контурі.

ВИДІЛЕННЯ НЕДОСЛІДЖЕНИХ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ

Незважаючи на наявні наукові напрацювання щодо управління ризиками у сфері критичної інфраструктури, комплексний механізм управління ризиками в процесі її розвитку залишається недостатньо розробленим. Більшість досліджень зосереджується на нормативно-правових, організаційних чи технічних аспектах без урахування взаємозв'язку між управлінням ризиками, стратегічним плануванням та модернізацією інфраструктурних систем.

Фрагментарно досліджено питання інтеграції ризик-менеджменту у процес відновлення та розвитку об'єктів критичної інфраструктури, особливо в умовах воєнних загроз і цифрової трансформації. Недостатньо розкритими залишаються аспекти оцінювання ефективності механізму управління ризиками, узгодження його із сучасними інвестиційними та інноваційними політиками, а також використання цифрових технологій - зокрема систем штучного інтелекту, кіберзахисту та аналітики великих даних - у процесі прогнозування та мінімізації ризиків.

Таким чином, існує потреба у формуванні науково обґрунтованого, інтегрованого механізму управління ризиками в процесі розвитку критичної інфраструктури України, який поєднував би правові, економічні, організаційні, інформаційно-аналітичні та технічні інструменти у єдину систему забезпечення стійкості та безпеки.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою дослідження є розробка науково обґрунтованого механізму управління ризиками в процесі розвитку критичної інфраструктури України, який забезпечуватиме її стійкість, адаптивність і безперервність функціонування в умовах воєнних, техногенних та кіберзагроз.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Ефективне функціонування критичної інфраструктури України є ключовою умовою забезпечення національної безпеки, стабільності соціально-економічних процесів і безперервності життєво важливих послуг для населення. До системи критичної інфраструктури належать енергетичні, транспортні, комунальні, водопостачальні, інформаційно-комунікаційні, фінансові та оборонно-промислові об'єкти, порушення діяльності яких може мати масштабні наслідки для держави та суспільства. Ефективність функціонування такої системи безпосередньо залежить від здатності держави, регіональних органів влади та операторів об'єктів вчасно виявляти, оцінювати, мінімізувати та контролювати ризики, що можуть призвести до збоїв, втрати функціональності або руйнування елементів інфраструктури. Це потребує наявності інтегрованої системи управління ризиками, заснованої на єдиних принципах, процедурах і стандартах.

Сучасна концепція управління ризиками у сфері критичної інфраструктури повинна спиратися на принципи централізації управління, формалізації процесів та міжгалузевої взаємодії, адже об'єкти інфраструктури мають високий рівень взаємозалежності - технологічної, енергетичної, транспортної, інформаційної. Будь-яке порушення в одному секторі (наприклад, енергетиці чи зв'язку) здатне спричинити ланцюгові наслідки для інших секторів економіки, створюючи каскадний ефект.

Після початку повномасштабного вторгнення у 2022 році, система критичної інфраструктури зазнала безпрецедентного навантаження та численних руйнувань. Значна кількість об'єктів енергетики, транспорту, водопостачання, зв'язку та комунальної інфраструктури була пошкоджена, зруйнована або тимчасово виведена з експлуатації. Це призвело до масових перебоїв у постачанні електроенергії, води, газу, інтернету, транспортних перевезень, а також до зниження рівня надання критичних послуг населенню.

Крім фізичних загроз, зросла кількість кіберінцидентів, спрямованих на енергетичні та інформаційно-комунікаційні системи, що свідчить про перехід ризиків у гібридну площину - коли поєднуються військові, інформаційні, економічні та технологічні загрози [4].

Такі умови функціонування актуалізували потребу у переосмисленні ролі державного управління ризиками та впровадженні системного, науково обґрунтованого механізму, який забезпечуватиме безперервність, стійкість і швидке відновлення критичної інфраструктури навіть у кризових обставинах. Вирішальне значення у цьому процесі має нормативно-правове регулювання, яке визначає загальні принципи, вимоги та процедури формування системи управління ризиками безпеки. Саме правові акти закладають базу

для побудови єдиних підходів до оцінювання, моніторингу й реагування на ризики у всіх секторах критичної інфраструктури.

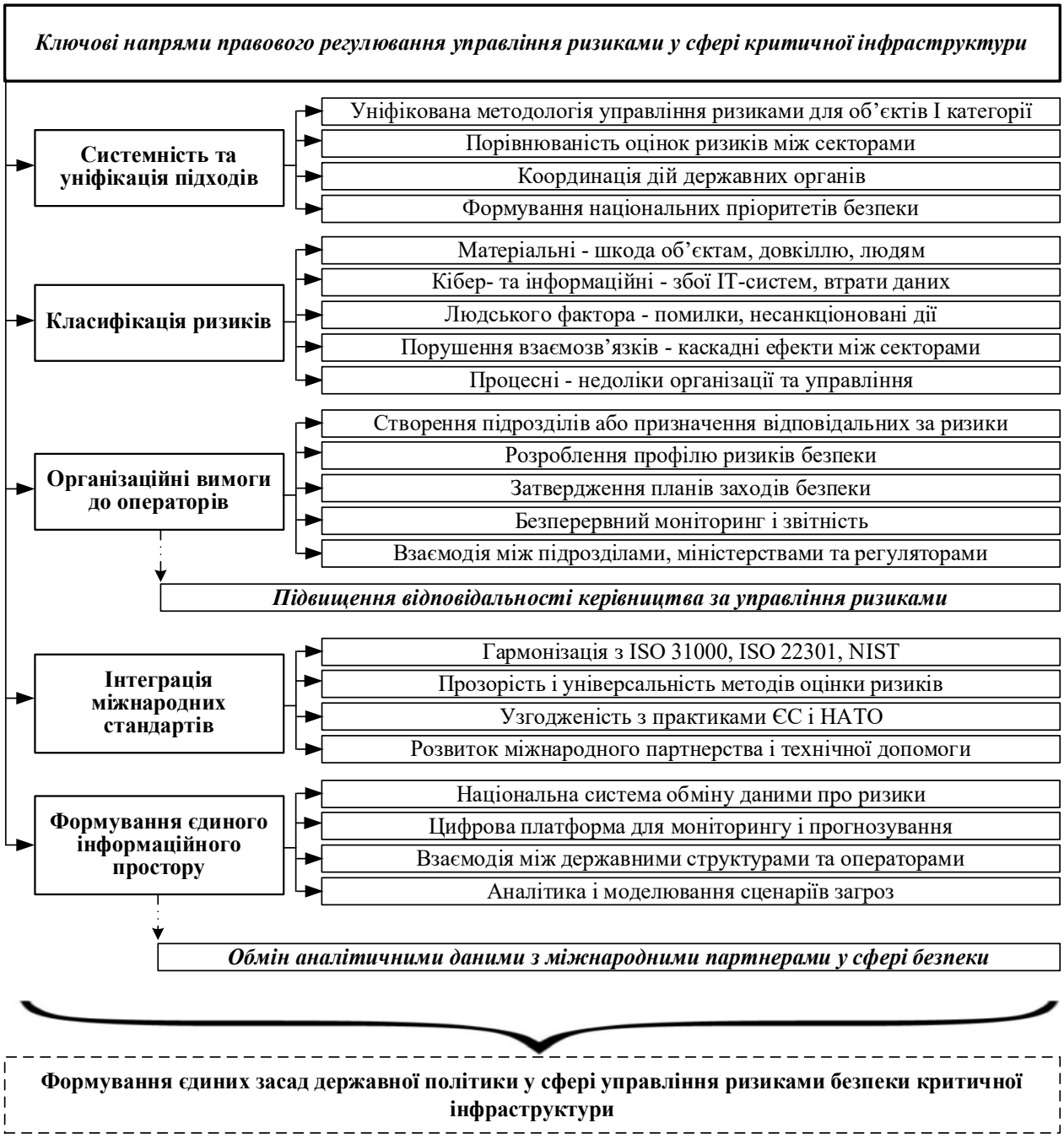

Рис.1. Ключові напрями правового регулювання управління ризиками у сфері критичної інфраструктури України
*сформовано на основі джерела [5]

На сучасному етапі система державного регулювання у сфері критичної інфраструктури в Україні поступово набуває чіткої інституційної форми. Важливим кроком у цьому напрямі стало прийняття Постанови Кабінету Міністрів України № 367 від 1 квітня 2025 р. «Про затвердження Вимог до управління ризиками безпеки на об'єктах критичної інфраструктури І категорії критичності» [5].

З метою узагальнення підходів, визначених у Постанові Кабінету Міністрів України № 367 від 1 квітня 2025 р., структурно ключові напрями правового регулювання управління ризиками можна представити у вигляді системної моделі (рис. 1), яка демонструє взаємозв'язок між державним, організаційним, технологічним та міжнародним рівнями забезпечення процесу управління ризиками безпеки критичної інфраструктури.

Ключові напрями правового регулювання управління ризиками у сфері критичної інфраструктури охоплюють державний, організаційний, інформаційно-аналітичний та міжнародний рівні забезпечення

процесу. Система нормативного регулювання, представлена у Постанові Кабінету Міністрів України № 367 від 1 квітня 2025 р., визначає основні засади формування єдиного підходу до управління ризиками безпеки, спрямованого на запобігання кризовим подіям, зниження їх імовірності та мінімізацію наслідків.

Запровадження уніфікованої методології управління ризиками, заснованої на міжнародних стандартах ISO 31000, ISO 22301, NIST RMF та ДСТУ IEC/ISO 31010:2013, забезпечує системність, порівнюваність і прозорість процесів оцінювання ризиків у різних секторах критичної інфраструктури. Водночас класифікація ризиків за видами - матеріальні, інформаційні, організаційні, процесні, людського фактора - дає можливість структурувати джерела загроз і встановити пріоритети у їх нейтралізації [6].

Важливе місце в системі посідають організаційні вимоги до операторів об'єктів критичної інфраструктури, які передбачають створення спеціалізованих підрозділів або призначення відповідальних осіб за управління ризиками, формування профілів ризиків безпеки, розроблення об'єктових планів стійкості та впровадження постійного моніторингу ризиків. Окремо підкреслюється підвищення відповідальності керівництва підприємств та установ за належну реалізацію політики управління ризиками й інтеграцію превентивних заходів у повсякденну діяльність.

Не менш значущим напрямом є інтеграція міжнародних стандартів і практик, що забезпечує сумісність української системи управління ризиками з європейською та світовою моделями безпеки. Такий підхід відкриває можливості для участі України в міжнародних ініціативах, програмах технічної допомоги та спільних проєктах у сфері кібер- і енергетичної безпеки.

Фінальним елементом нормативно-правової архітектури є створення єдиного інформаційного простору управління ризиками, який забезпечує цифрову взаємодію між державними структурами, регіональними адміністраціями та операторами об'єктів. Національна система обміну даними про ризики сприяє накопиченню аналітичної інформації, прогнозуванню загроз, моделюванню кризових сценаріїв і швидкому реагуванню на інциденти. Її розвиток передбачає також обмін аналітичними даними з міжнародними партнерами у сфері безпеки.

Таким чином, нормативно-правове регулювання управління ризиками у сфері критичної інфраструктури формує основу для створення цілісної системи ризик-менеджменту, яка поєднує державне управління, внутрішній контроль операторів та міжнародну координацію дій.

Подальше розгортання цього процесу передбачає поетапне формування практичного механізму управління ризиками, що деталізує реалізацію основних принципів та інструментів на різних рівнях системи. Результатом якого є узгодженість і взаємодія суб'єктів управління ризиками на всіх рівнях - державному, галузевому, регіональному та об'єктовому, що забезпечує підвищення стійкості, надійності та безпеки критичної інфраструктури України навіть в умовах воєнних і гібридних загроз.

Подальше впровадження визначених нормативно-правових засад потребує практичного механізму, який забезпечує конкретизацію, координацію та інтеграцію процесів управління ризиками в межах єдиної системи функціонування критичної інфраструктури. З цією метою доцільно розглянути етапи формування механізму управління ризиками, що відображають логіку переходу від ідентифікації потенційних загроз до реалізації превентивних і реагувальних заходів, моніторингу їх ефективності та вдосконалення управлінських рішень.

Процес формування механізму управління ризиками у сфері критичної інфраструктури є поетапним і системним. Він охоплює взаємопов'язані заходи, спрямовані на виявлення, оцінювання, мінімізацію та постійний контроль загроз, що можуть вплинути на стабільність функціонування систем життєзабезпечення держави [7].

Основні етапи його реалізації включають п'ять послідовних складових: ідентифікацію ризиків, оцінювання ризиків, розроблення заходів реагування, моніторинг і контроль, а також звітність і комунікацію (рис.2).

Науково-теоретичний підхід до формування механізму управління ризиками у сфері критичної інфраструктури України відображає логічну послідовність, та базується на принципах циклічності, адаптивності й безперервного вдосконалення.

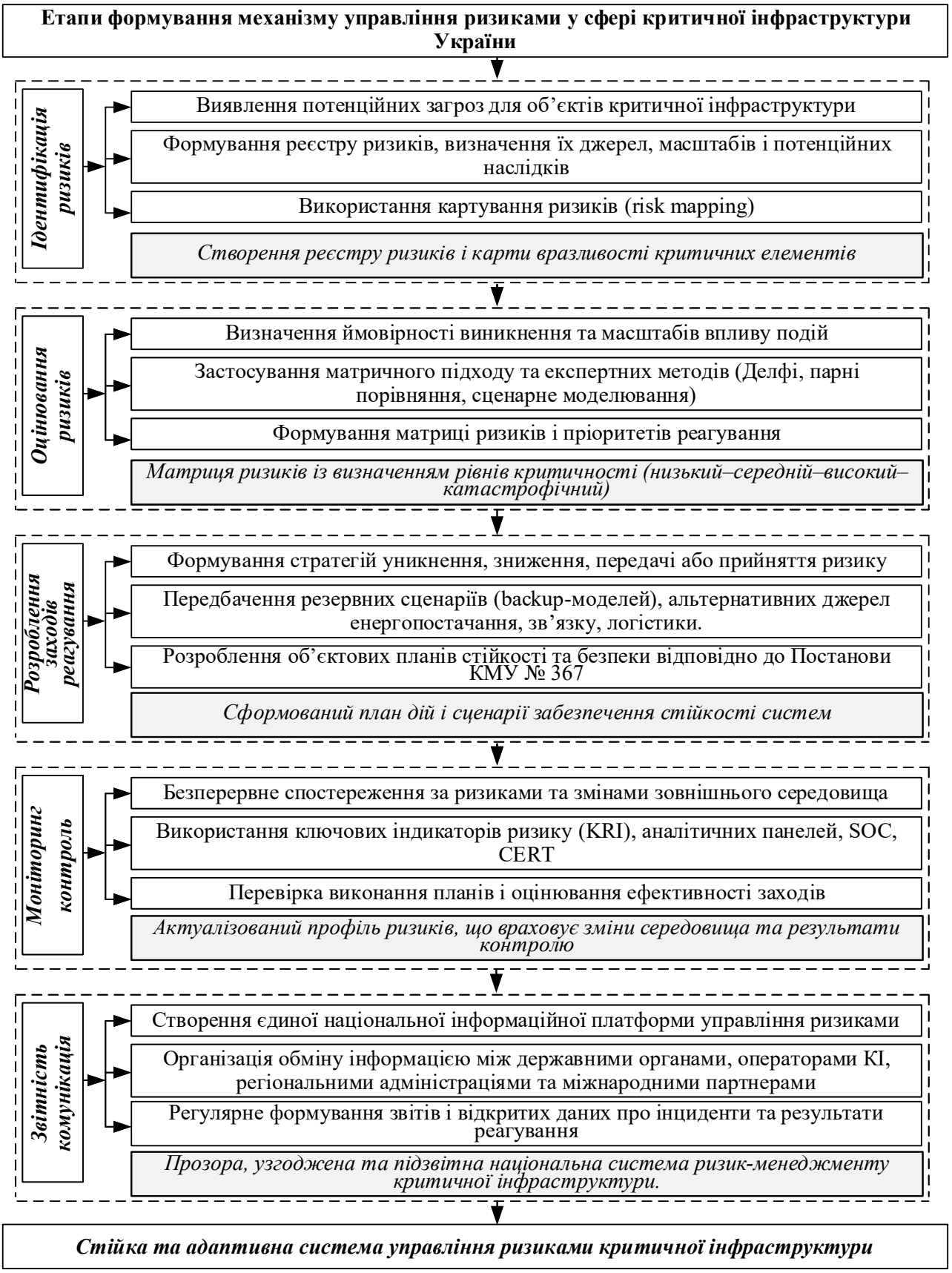

Рис. 2. Науково-теоретичний підхід до формування механізму управління ризиками у сфері критичної інфраструктури України

Кожен етап, від ідентифікації загроз до налагодження звітності та комунікації, становить взаємопов'язану складову єдиного процесу, спрямованого на забезпечення стійкості та безпеки критичної інфраструктури. Ідентифікація дозволяє виявити потенційні джерела небезпеки, оцінювання надає

можливість визначати масштаби їх впливу, а розроблення заходів реагування формує стратегії мінімізації ризиків.

Моніторинг і контроль забезпечують своєчасне коригування управлінських рішень, тоді як ефективна звітність і комунікація сприяють узгодженості дій усіх суб'єктів системи ризик-менеджменту. Таким чином, представлена модель формує стійку та адаптивну систему управління ризиками критичної інфраструктури, здатну оперативно реагувати на зовнішні виклики, зменшувати уразливість об'єктів і забезпечувати безперервність їх функціонування навіть в умовах кризових та воєнних ситуацій.

Подальше вдосконалення цієї системи вимагає чіткої структуризації її елементів та визначення функціональних взаємозв'язків між ними.

У цьому контексті доцільно розглянути структурні складові механізму управління ризиками, які забезпечують узгоджене функціонування організаційних, економічних, інформаційно-аналітичних, нормативно-правових і технічних компонентів єдиної системи ризик-менеджменту [8].

Особливе значення має інтеграція управління ризиками в процес цифрової трансформації критичної інфраструктури. Використання цифрових двійників об'єктів, систем штучного інтелекту, платформ моніторингу та кіберзахисту дозволяє не лише реагувати на ризики, а й передбачати їх у процесі проектування та експлуатації. Це сприяє формуванню адаптивної, інноваційно орієнтованої моделі розвитку, здатної самостійно оновлюватися та вдосконалюватися під впливом зовнішніх викликів.

Таким чином, управління ризиками у процесі розвитку критичної інфраструктури України набуває подвійного значення: воно виступає водночас інструментом безпеки та каталізатором розвитку. Системний ризик-менеджмент створює умови для ефективного використання ресурсів, підвищення інвестиційної привабливості, зміцнення довіри міжнародних партнерів і забезпечення сталого розвитку критично важливих секторів економіки.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Таким чином, управління ризиками у процесі розвитку критичної інфраструктури України набуває подвійного значення: воно виступає водночас інструментом безпеки та каталізатором розвитку. Системний ризик-менеджмент створює умови для ефективного використання ресурсів, підвищення інвестиційної привабливості, зміцнення довіри міжнародних партнерів і забезпечення сталого розвитку критично важливих секторів економіки.

Отже, формування механізму управління ризиками в процесі розвитку критичної інфраструктури України є ключовою передумовою підвищення її стійкості, безпеки та здатності до відновлення, що інтегрує правові, організаційні, економічні, технічні та аналітичні інструменти, створює умови для ефективного управління ризиками, мінімізації загроз і забезпечення сталого розвитку критично важливих секторів економіки навіть в умовах воєнних і гібридних викликів.

Література

1. Євтушенко Н. О., Захаржевська А. А. Особливості формування механізму розвитку управління ризиками в підприємствах. Економічний простір, 2022, № 182, с. 61-66 https://doi.org/10.32782/2224-6282/182-8

2. Возненко О. М. Управління ризиками об'єктів критичної інфраструктури: державно-управлінський аспект. Держава та регіони. Серія: Державне управління, 2022, № 4. С.22-27. https://doi.org/10.32840/1813-3401.2022.4.4

3. Магомедов А. О. Ризики та загрози для об'єктів критичної інфраструктури та шляхи їх подолання. *Investytsiyi: praktyka ta dosvid*. 2024. № 15. С. 216–221 https://doi.org/10.32702/2306-6814.2024.15.216

4. Гуцалюк М. В. Стратегії протидії сучасним кіберзагрозам та забезпеченняь кіберстійкості критичної інфраструктури України. Інформація і право. 2024. № 2. С. 164-177. https://doi.org/10.37750/2616-6798.2024.2(49).306199

5. Постанова Кабінету Міністрів України № 367 від 1 квітня 2025 р. «Про затвердження Вимог до управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності». Офіційний вебсайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/367-2025-%D0%BF#Text

6. ISO 31000:2018, ISO 22301:2019, NIST Risk Management Framework, ДСТУ IEC/ISO 31010:2013 — міжнародні та національні стандарти управління ризиками. URL: https://www.iso.org/standard/65694.html

7. Чобіток В., Чобіток І. Стратегічні напрями забезпечення енергетичної безпеки підприємств в період нестабільності. Adaptive Management: Theory and Practice. Economics, 2024, Т. 19, № 38. https://doi.org/10.33296/2707-0654-19(38)-06

8. Glette-Iversen I., Flage R., Aven T. Extending and improving current frameworks for risk management and decision-making: A new approach for incorporating dynamic aspects of risk and uncertainty. Safety Science, 2023, Vol. 168, p. 106317. https://doi.org/10.1016/j.ssci.2023.106317

9. Морозова О. О. Інтеграційний підхід до оцінювання ефективності управління людським капіталом підприємств у цифровому середовищі. Вісник економіки транспорту і промисловості, 2024, № 87, с. 161–173.

10. Mikac R. Protection of the EU's Critical Infrastructures: Results and Challenges. Atlantic Journal of Communication and International Governance (ACIG Journal), 2023, Vol. 3, No. 2, p. 45–58.

References

1. Yevtushenko N. O., Zakharzhevska A. A. Osoblyvosti formuvannia mekhanizmu rozvytku upravlinnia ryzykamy v pidpryiemstvakh. Ekonomichnyi prostir, 2022, № 182, s. 61-66 https://doi.org/10.32782/2224-6282/182-8

2. Voznenko O. M. Upravlinnia ryzykamy obiektiv krytychnoi infrastruktury: derzhavno-upravlinskyi aspekt. Derzhava ta rehiony. Seriia: Derzhavne upravlinnia, 2022, № 4. S.22-27 https://doi.org/10.32840/1813-3401.2022.4.4

3. Mahomedov A. O. Ryzyky ta zahrozy dlia obiektiv krytychnoi infrastruktury ta shliakhy yikh podolannia. Investytsiyi: praktyka ta dosvid. 2024. № 15. S. 216–221 https://doi.org/10.32702/2306-6814.2024.15.216

4. Hutsaliuk M. V. Stratehii protydii suchasnym kiberzahrozam ta zabezpechennia kiberstiikosti krytychnoi infrastruktury Ukrainy. Informatsiia i pravo. 2024. № 2. S. 164-177. https://doi.org/10.37750/2616-6798.2024.2(49).306199

5. Postanova Kabinetu Ministriv Ukrainy № 367 vid 1 kvitnia 2025 r. «Pro zatverdzhennia Vymoh do upravlinnia ryzykamy bezpeky na obiektakh krytychnoi infrastruktury I katehorii krytychnosti». Ofitsiinyi vebsait Verkhovnoi Rady Ukrainy. URL: https://zakon.rada.gov.ua/laws/show/367-2025-%D0%BF#Text

6. ISO 31000:2018, ISO 22301:2019, NIST Risk Management Framework, DSTU IEC/ISO 31010:2013 — mizhnarodni ta natsionalni standarty upravlinnia ryzykamy. URL: https://www.iso.org/standard/65694.html

7. Chobitok V., Chobitok I. Stratehichni napriamy zabezpechennia enerhetychnoi bezpeky pidpryiemstv v period nestabilnosti. Adaptive Management: Theory and Practice. Economics, 2024, T. 19, № 38. https://doi.org/10.33296/2707-0654-19(38)-06

8. Glette-Iversen I., Flage R., Aven T. Extending and improving current frameworks for risk management and decision-making: A new approach for incorporating dynamic aspects of risk and uncertainty. Safety Science, 2023, Vol. 168, p. 106317. https://doi.org/10.1016/j.ssci.2023.106317

9. Morozova O. O. Intehratsiinyi pidkhid do otsiniuvannia efektyvnosti upravlinnia liudskym kapitalom pidpryiemstv u tsyfrovomu seredovyshchi. Visnyk ekonomiky transportu i promyslovosti, 2024, № 87, s. 161–173.

10. Mikac R. Protection of the EU's Critical Infrastructures: Results and Challenges. Atlantic Journal of Communication and International Governance (ACIG Journal), 2023, Vol. 3, No. 2, p. 45–58.