УДК 35.072:355:004
DOI: https://doi.org/10.31470/2786-6246-2026-15-6-13

Абражевич Марина, аспірантка кафедри публічного управління та адміністрування Університету Григорія Сковороди в Переяславі

Abrazhevych Maryna, Postgraduate student at the Department of Public Management and Administration at Hryhorii Skovoroda University in Pereiaslav

ORCID ID: https://orcid.org/0009-0003-3571-3588

ДЕФІНІЦІЯ ТА АРХІТЕКТУРА РИЗИК-МЕНЕДЖМЕНТУ В СТРУКТУРІ ПУБЛІЧНОГО УПРАВЛІННЯ СФЕРОЮ ОБОРОНИ

DEFINITION AND ARCHITECTURE OF RISK MANAGEMENT WITHIN THE PUBLIC DEFENSE GOVERNANCE STRUCTURE

Анотація. У статті здійснений системний аналіз дефініції та архітектури ризик-менеджменту в структурі публічного управління сферою оборони. Зазначено, що ризик-менеджмент у сфері оборони є системним і багатовимірним процесом, який інтегрує нормативно-правові, стратегічні, організаційно-процесуальні, технологічні та кадрові компоненти. Він забезпечує ідентифікацію, оцінку, планування, реагування та контроль ризиків, які можуть впливати на досягнення оборонних цілей та національної безпеки.

Дефініційно ризик розглядається як ефект невизначеності на цілі організації, що підкреслює його динамічний характер. Це означає, що ризик охоплює не лише ймовірність настання негативних подій, а й масштаб потенційного впливу, включно з можливими позитивними наслідками. Таке розуміння відповідає міжнародному стандарту ISO 31000:2018 і формує наукову основу для системного підходу до управління ризиками.

Архітектура ризик-менеджменту є багаторівневою та інтегрованою системою, що включає: нормативно-правове забезпечення і політики як фундамент, що визначає правові рамки, відповідальність та процедури; стратегічний рівень, який забезпечує прогнозування ризикових сценаріїв і інтеграцію у стратегічне планування оборони; організаційно-процесуальний рівень для реалізації циклу управління ризиками через методи і процедури оцінки та контролю; технологічний та інформаційний рівень для оперативного моніторингу, моделювання та підтримки управлінських рішень; організаційну культуру і компетенції, що формують ризико-орієнтоване мислення, кадрову підготовку і ефективну взаємодію між підрозділами.

Інтеграція всіх рівнів архітектури забезпечує системність і ефективність управління ризиками у публічному секторі оборони. Такий підхід дозволяє не лише зменшувати потенційні загрози, а й підвищувати стійкість оборонної системи, адаптивність до змін зовнішнього середовища та оптимізацію ресурсів держави.

Ключовою практичною цінністю ризик-менеджменту в оборонному публічному управлінні є його проактивний характер, який дозволяє державі прогнозувати потенційні загрози, приймати обґрунтовані управлінські рішення і формувати превентивні та коригувальні заходи. Це перетворює управління ризиками на стратегічний інструмент забезпечення національної безпеки.

Ключові слова: публічне управління, ризик-менеджмент, ризики, системи оборони, архітектура ризик-менеджменту, національна безпека.

*Corresponding author

Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/)

ISSN 2786-6246 (print)
ISSN 2786-9091 (online)

Abstract. This article provides a systematic analysis of the definition and architecture of risk management within the structure of public defense governance. It is established that risk management in the defense sector is a systemic, multidimensional process that integrates regulatory, strategic, organizational-procedural, technological, and human resource components. It ensures the identification, assessment, planning, response, and control of risks that may affect the achievement of defense objectives and national security.

Conceptually, risk is viewed as the effect of uncertainty on organizational objectives, highlighting its dynamic nature. This implies that risk encompasses not only the probability of negative events but also the scale of potential impact, including possible positive outcomes. Such an understanding aligns with the international standard ISO 31000:2018 and forms the scientific basis for a systemic approach to risk management.

The architecture of risk management is a multi-layered and integrated system that includes: the regulatory framework and policies as a foundation defining legal boundaries, responsibilities, and procedures; the strategic level, which ensures the forecasting of risk scenarios and integration into strategic defense planning; the organizational-procedural level for implementing the risk management cycle through assessment and control methods; the technological and information level for operational monitoring, modeling, and decision support; and organizational culture and competencies that foster a risk-oriented mindset, personnel training, and effective inter-unit interaction.

The integration of all architectural levels ensures the consistency and effectiveness of risk management in the public defense sector. This approach not only mitigates potential threats but also increases the resilience of the defense system, its adaptability to environmental changes, and the optimization of state resources.

The key practical value of risk management in public defense governance lies in its proactive nature, which enables the state to forecast potential threats, make informed management decisions, and formulate preventive and corrective measures. This transforms risk management into a strategic tool for ensuring national security.

Keywords: public management, risk management, risks, defense systems, risk management architecture, national security.

Постановка проблеми. В умовах повномасштабних безпекових загроз, гібридної війни та високої невизначеності зовнішнього і внутрішнього середовища система публічного управління сферою оборони перебуває під постійним тиском ризиків різної природи – воєнних, політичних, економічних, технологічних, кадрових та інформаційних. Ефективність оборонної політики держави дедалі більше залежить не лише від наявності ресурсів, а від здатності органів публічної влади своєчасно ідентифікувати, оцінювати, прогнозувати та мінімізувати ризики, що виникають на стратегічному, оперативному й тактичному рівнях управління.

У цьому контексті особливого значення набуває чітке концептуальне визначення ризик-менеджменту як складової сучасного публічного управління сферою оборони, а також формування його внутрішньої архітектури – сукупності інституційних, нормативно-правових, організаційних, інформаційно-аналітичних та процедурних елементів. Відсутність уніфікованого підходу до дефініції ризик-менеджменту, фрагментарність управлінських механізмів і слабка інтеграція ризик-орієнтованого мислення в процес ухвалення управлінських рішень знижують стійкість оборонного сектору та ускладнюють досягнення стратегічних цілей національної безпеки.

Додатковим чинником є необхідність гармонізації національної системи управління ризиками у сфері оборони з міжнародними стандартами та практиками країн – членів НАТО і ЄС, де ризик-менеджмент розглядається як невід'ємний елемент оборонного планування, бюджетування, управління спроможностями та контролю ефективності. Для України, яка перебуває в умовах воєнного стану та одночасно реалізує глибокі інституційні реформи, питання побудови цілісної архітектури ризик-менеджменту в публічному управлінні оборонною сферою має не лише теоретичне, а й прикладне значення.

Звернення до проблеми дефініції та архітектури ризик-менеджменту дозволяє обґрунтувати системний підхід до підвищення керованості, адаптивності та стійкості публічного управління сферою оборони, що є критично важливим для забезпечення національної безпеки в умовах довготривалих воєнних і безпекових викликів.

Аналіз останніх досліджень і публікацій. Сучасні дослідження у сфері ризик-менеджменту в структурі публічного управління обороною демонструють, що ця тема поки що розглядається фрагментарно і не завжди системно. Так, А. Лоїшин, І. Ткач, Д. Окіпняк, М. Потетюєва та О. Угринович здійснюють аналіз організації та функціонування процесів управління ризиками в програмах оборони, зокрема в Збройних Силах України, акцентуючи увагу на практичних аспектах ідентифікації загроз, ролі внутрішнього контролю та компетенцій суб'єктів, залучених до процесу ризик-менеджменту в оборонних структурах. О. Руснак розкриває концептуальні та методологічні основи ризик-менеджменту в публічному управлінні, включно з державними структурами, підкреслюючи значення міжнародних стандартів, зокрема ISO 31000:2018, як фундаменту для формування системного та інтегрованого підходу до управління ризиками в державному секторі. К. Бугайчук досліджує адміністративно-правове регулювання ризик-орієнтованих підходів у діяльності державних органів сектору безпеки й оборони, що є важливим для розуміння нормативно-правового поля управління ризиками в оборонній сфері. Д. Ярмусь у своїй роботі зосереджується на адаптації моделей ризик-менеджменту до умов воєнного стану, що має критичне значення для оборонних публічних органів. Автор пропонує підходи до динамічної оцінки ризиків, гнучкого реагування та інтеграції цифрових інструментів у процес управління.

Слід зауважити, що наукових публікацій, присвячених безпосередньо дефініції та архітектурі ризик-менеджменту в структурі публічного управління обороною, поки що небагато. Частина наявних робіт розглядає питання лише в суміжних контекстах, таких як внутрішній контроль, воєнний стан або адміністративно-правове регулювання. Водночас ці дослідження висвітлюють ключові аспекти, пов'язані з визначенням, організацією та адаптацією систем управління ризиками в оборонних і безпекових структурах, розкриваючи як окремі, так і комплексні підходи до управління ризиками. Це свідчить про високий ступінь актуальності та міждисциплінарний характер подальших наукових розвідок у цій сфері, які мають поєднувати державне управління, безпеку, стандарти управління ризиками та адаптивні моделі для роботи в умовах невизначеності.

Метою статті є системний аналіз дефініції та архітектури ризик-менеджменту в структурі публічного управління сферою оборони.

Виклад основного матеріалу. Ризик-менеджмент у сфері оборони як галузі публічного управління – це спеціалізований, системний процес і сукупність організаційних механізмів, спрямованих на ідентифікацію, аналіз, оцінку, реагування, моніторинг та контроль ризиків, які можуть впливати на досягнення стратегічних цілей оборонної політики, ефективність використання ресурсів та безпеку держави в умовах невизначеності й загроз. Він інтегрується в загальну систему державного управління і виступає ключовим елементом стратегічного, оперативного та тактичного управління обороною, сприяючи підвищенню стійкості органів оборонного сектору до внутрішніх і зовнішніх викликів.

У сучасному науковому й практичному контексті поняття «ризик» розглядається не як проста ймовірність настання негативного результату, а як вимірювана форма невизначеності, що впливає на досягнення цілей організації. Такий підхід підкреслює не лише можливість втрат, а й ширший спектр наслідків невизначеності – від негативних до потенційно позитивних, що є ключовим для ефективного менеджменту в складних системах управління [1].

Науково-теоретична основа цього підходу ґрунтується на розумінні ризику як ефекту невизначеності на цілі організації, формулювання, яке наразі закріплене в міжнародному стандарті ISO 31000:2018 – Управління ризиками – Керівні принципи. Згідно зі стандартом, ризик визначається саме як «вплив невизначеності на цілі» організації [1]. Такий вплив може бути як позитивним, так і негативним – це залежить від характеру невизначеності та контексту організаційної діяльності.

© Абражевич М.

Це визначення є фундаментально важливим, оскільки воно розширює традиційні уявлення про ризик. У класичних підходах ризик традиційно розглядався як ймовірність настання небажаних подій із негативними наслідками (наприклад, можливість втрат чи шкоди). У такому трактуванні ризик часто асоціювався виключно із загрозами. Натомість сучасні міжнародні стандарти принципово підкреслюють, що ризик виникає у будь-якому контексті невизначеності щодо досягнення цілей – незалежно від позитивного чи негативного характеру впливу.

Це розширене розуміння ризику як ефекту невизначеності на цілі формує більш цілісний науковий підхід, що включає кілька ключових аспектів:

- невизначеність як системний фактор. Невизначеність – це недостатність інформації або непередбачуваність зовнішніх і внутрішніх змін, що впливають на здатність організації досягати своїх стратегічних, тактичних чи оперативних цілей [2]. Цей аспект невизначеності стає джерелом ризику;
- інтеграція ризику з цілями. Підприємство або орган управління визначає ризик саме у відношенні до конкретних цілей (стратегічних показників, операційних завдань тощо), що дозволяє оцінювати не лише ймовірність подій, а їхній вплив на результат діяльності [3];
- позитивні та негативні ефекти. На відміну від вузького трактування лише негативних наслідків, під ризиком у рамках ISO 31000 розуміють будь-яку відмінність від очікуваного результату – як потенційний негатив (загроза), так і позитив (можливість).

Для наукового розуміння ця дефініція є ключовою, оскільки вона дозволяє розглядати ризик не як статичне визначення імовірності втрат, а як динамічну характеристику взаємодії між цілями організації та невизначеністю умов їхнього досягнення. Це відповідає сучасним тенденціям системного та стратегічного мислення, де управління ризиками стає не лише технічною функцією, а й елементом прийняття рішень на всіх рівнях управлінської діяльності.

Таким чином, ризик у сучасному фундаментальному розумінні є складною, багатовимірною категорією, тісно пов'язаною з феноменом невизначеності та процесом досягнення цілей організації. Ризик не зводиться виключно до ймовірності негативних подій або втрат, а відображає потенційний вплив невизначеності на результати діяльності, що робить його невід'ємною характеристикою будь-якої цілеспрямованої управлінської системи.

Ризик-менеджмент у структурі публічного управління сферою оборони слід розглядати як системну, цілеспрямовану і структуровану діяльність органів державної влади та силових структур, спрямовану на ідентифікацію, оцінювання, реагування та контроль ризиків, що можуть перешкоджати досягненню оборонних цілей і забезпеченню національної безпеки [4]. Такий підхід виходить за межі традиційного розуміння управління ризиками як набір технічних заходів чи процедур, охоплюючи комплексні управлінські процеси, інтегровані у систему оборонного управління та державного управління загалом.

У наукових джерелах ризик-менеджмент розглядається як інструмент підвищення ефективності управлінських рішень у складних умовах невизначеності, що включає не лише ідентифікацію потенційних загроз, а й прогнозування сценаріїв розвитку подій і формування адекватних стратегій реагування [3]. Важливо, що таке управління є проактивним, а не лише реактивним, і має завдання не тільки мінімізувати наслідки ризиків, а й оптимізувати прийняття стратегічних рішень у сфері оборони.

У контексті оборони публічне управління ризиками передбачає системну інтеграцію у процеси стратегічного та операційного планування, що охоплюють оцінювання зовнішнього безпекового середовища, аналіз внутрішніх можливостей та ресурсів, а також координацію між різними суб'єктами управління – від центральних органів виконавчої влади до військових структур і спеціальних служб [5].

Науковці підкреслюють, що управління ризиками в оборонній сфері включає внутрішній контроль та стандартизовані підходи до ідентифікації, оцінювання та контролю ризиків, що узгоджуються з міжнародними підходами до управління (наприклад, COSO чи ISO-орієнтовані

методики), адаптованими під вимоги безпекового сектору. Це передбачає визначення процесів, відповідальних осіб, процедур моніторингу і оцінювання ефективності заходів реагування.

Таким чином, ризик-менеджмент у сфері оборони у публічному управлінні – це не окрема функція, а інтегральна складова системи управління обороною, що забезпечує своєчасну ідентифікацію ризиків, їхню аналітичну оцінку, формування превентивних та коригувальних заходів і постійний контроль їх реалізації у контексті досягнення стратегічних цілей безпеки держави. Він орієнтований на підвищення стійкості оборонної системи до зовнішніх і внутрішніх викликів, оптимізацію використання ресурсів та посилення адаптивності у складному та динамічному безпековому середовищі.

У контексті публічного управління обороною ризик-менеджмент охоплює широку гаму ризиків: стратегічні ризики (зміни безпекового середовища, технологічні трансформації сил оборони), оперативні (логістичні, кадрові, матеріально-технічні), фінансові, юридичні, політичні та репутаційні. Ефективне управління цими ризиками дозволяє адаптувати політику й практику оборонного планування відповідно до реалій сучасних загроз, включно з умовами воєнного стану та гібридними викликами.

Архітектура ризик-менеджменту в структурі публічного управління сферою оборони виступає не як ізольований набір окремих заходів, а як багаторівнева, інтегрована система, що забезпечує послідовну організацію і реалізацію процесів управління ризиками на всіх рівнях оборонної діяльності держави [6]. Такий підхід відповідає сучасним науковим та управлінським тенденціям щодо створення цілісних систем управління ризиками, що поєднують нормативно-політичні основи, стратегічне планування, операційні процедури, інформаційно-технологічні засоби та людські ресурси в єдину функціональну структуру.

Нормативно-правове забезпечення і політики становлять фундамент цієї архітектури, оскільки визначають правові основи, управлінські принципи, відповідальність суб'єктів та процедури реалізації ризик-менеджменту в оборонному секторі. У публічному управлінні обороною це включає законодавчі акти, підзаконні нормативні документи, внутрішні стандарти і політики Міністерства оборони, Збройних Сил та інших оборонних органів, які формують правове підґрунтя для планування, оцінювання та контролю ризикових процесів [7]. Нормативно-правовий рівень встановлює рамки для звітності, контролю і взаємодії між державними інституціями, що сприяє забезпеченню прозорості, підзвітності та відповідності національним цілям безпеки.

Стратегічний рівень архітектури ризик-менеджменту охоплює визначення ключових оборонних цілей, оцінювання екзогенних загроз і формування моделей прогнозування ризикових сценаріїв. У цьому контексті стратегічне планування включає аналіз зовнішнього безпекового середовища, очікуваних змін геополітичних, технологічних та соціальних факторів, які можуть впливати на обороноздатність держави [8]. Такий підхід забезпечує інтеграцію управління ризиками зі стратегічними документами оборонної політики, що дозволяє органам управління адаптувати свої дії до мінливих умов і формувати політики реагування, засновані на сценарному плануванні й прогнозуванні.

На організаційно-процесуальному рівні архітектура містить сукупність процедур, методів і технік, спрямованих на реалізацію циклу управління ризиками: від ідентифікації потенційних ризикових подій до аналізу, оцінювання, планування заходів, їх реалізації та подальшого моніторингу ефективності. Цей рівень включає стандартизовані алгоритми дій, матриці ризиків, картографування впливів і методи кількісної/якісної оцінки ризиків. Він являє собою практичну реалізацію стратегічних намірів і нормативних вимог, які забезпечують узгодженість дій між різними підрозділами та рівнями управління.

Технологічний і інформаційний рівень є критично важливим в умовах сучасних викликів, оскільки передбачає використання цифрових інструментів, систем аналітики, моніторингу та раннього попередження, що дозволяють оцінювати та прогнозувати ризики в реальному часі. У сфері оборони це може включати системи моделювання загроз, автоматизовані платформи для збирання та обробки даних, інформаційні панелі для підтримки прийняття рішень, а також засоби

© Абражевич М.

кібербезпеки та інтегрованої телеметрії [9]. Такий рівень забезпечує оперативну видимість ризикових факторів та швидку реакцію на зміни зовнішнього середовища, що особливо важливо в умовах гібридних загроз та динамічних викликів.

Організаційна культура і компетенції становлять соціально-управлінський компонент архітектури ризик-менеджменту. Це включає формування ризико-орієнтованого мислення серед управлінців і персоналу, розвиток професійних навичок, систему безперервного навчання та оцінювання компетенцій, а також створення механізмів внутрішньої комунікації й обміну знаннями. Така культура сприяє тому, щоб менеджмент ризиків став органічною частиною всіх управлінських процесів, а не лише формальною процедурою. Ризико-орієнтовані підходи ґрунтують поведінку та рішення на розумінні потенційних впливів і невизначеностей, що підвищує адаптивність організації в цілому [4].

Таблиця 1.

Архітектура ризик-менеджменту в структурі публічного управління сферою оборони

Рівень архітектури	**Компоненти/ Складові**	**Основні функції**	**Призначення/Значення**
Нормативно-правовий	Законодавчі акти, підзаконні нормативні документи, внутрішні стандарти Міністерства оборони та ЗСУ	Визначення правових основ і принципів управління ризиками, регламентація відповідальності та повноважень, стандарти внутрішнього контролю	Забезпечує правове підґрунтя управління ризиками, визначає рамки звітності, взаємодії та підзвітності
Стратегічний	Ключові оборонні цілі, моделі прогнозування ризикових сценаріїв, сценарне планування	Ідентифікація стратегічних загроз, інтеграція ризик-менеджменту в стратегічне планування, формування політик реагування	Забезпечує проактивне управління ризиками, адаптацію оборонної політики до змін зовнішнього середовища
Організаційно-процесуальний	Процедури і методи ідентифікації, оцінки та контролю ризиків, матриці ризиків, алгоритми дій	Виконання циклу управління ризиками: ідентифікація, аналіз, оцінка, планування заходів, реалізація і моніторинг	Реалізація стратегічних і нормативних вимог, забезпечення узгодженості дій між підрозділами
Технологічний та інформаційний	Системи аналітики, цифрові платформи моніторингу, моделювання загроз, системи раннього попередження	Оцінка ризиків у реальному часі, підтримка управлінських рішень, моделювання сценаріїв розвитку подій	Забезпечує швидку реакцію на зміни зовнішнього середовища, оперативне прогнозування загроз
Організаційна культура і компетенції	Структури управління, кадрові ресурси, система навчання та підготовки	Формування ризико-орієнтованого мислення, розвиток професійних компетенцій, забезпечення взаємодії між підрозділами	Підвищує ефективність управлінських рішень, сприяє адаптивності та стійкості організації

Синтезуючи наведені компоненти, можна констатувати, що архітектура ризик-менеджменту в публічному управлінні сферою оборони виступає як комплексна система зі взаємопов'язаними рівнями, що забезпечують як нормативно-технічне обґрунтування, так і оперативну реалізацію управлінських рішень щодо ризиків. Така структура сприяє підвищенню стійкості оборонної системи до зовнішніх і внутрішніх загроз, координації дій між функціональними підрозділами, а також удосконаленню процесів планування й реагування, що в свою чергу посилює здатність держави забезпечувати національну безпеку і оборону.

Висновки. Проведений аналіз дає підстави зазначити, що ризик-менеджмент у сфері оборони є системним і багатовимірним процесом, який інтегрує нормативно-правові, стратегічні, організаційно-процесуальні, технологічні та кадрові компоненти. Він забезпечує ідентифікацію, оцінку, планування, реагування та контроль ризиків, які можуть впливати на досягнення оборонних цілей та національної безпеки.

Дефініційно ризик розглядається як ефект невизначеності на цілі організації, що підкреслює його динамічний характер. Це означає, що ризик охоплює не лише ймовірність настання

негативних подій, а й масштаб потенційного впливу, включно з можливими позитивними наслідками. Таке розуміння відповідає міжнародному стандарту ISO 31000:2018 і формує наукову основу для системного підходу до управління ризиками.

Архітектура ризик-менеджменту є багаторівневою та інтегрованою системою, що включає: нормативно-правове забезпечення і політики як фундамент, що визначає правові рамки, відповідальність та процедури; стратегічний рівень, який забезпечує прогнозування ризикових сценаріїв і інтеграцію у стратегічне планування оборони; організаційно-процесуальний рівень для реалізації циклу управління ризиками через методи і процедури оцінки та контролю; технологічний та інформаційний рівень для оперативного моніторингу, моделювання та підтримки управлінських рішень; організаційну культуру і компетенції, що формують ризико-орієнтоване мислення, кадрову підготовку і ефективну взаємодію між підрозділами.

Інтеграція всіх рівнів архітектури забезпечує системність і ефективність управління ризиками у публічному секторі оборони. Такий підхід дозволяє не лише зменшувати потенційні загрози, а й підвищувати стійкість оборонної системи, адаптивність до змін зовнішнього середовища та оптимізацію ресурсів держави.

Ключовою практичною цінністю ризик-менеджменту в оборонному публічному управлінні є його проактивний характер, який дозволяє державі прогнозувати потенційні загрози, приймати обґрунтовані управлінські рішення і формувати превентивні та коригувальні заходи. Це перетворює управління ризиками на стратегічний інструмент забезпечення національної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. ISO 31000:2018. URL: https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_31000_2018.pdf (дата звернення: 16.12.2025).
2. Науменко В. Поняття невизначеності та відображення ризику у практиці формування державних цільових програм соціально-економічного розвитку. *Інвестиції: практика та досвід*. 2023. №7. DOI: https://doi.org/10.32702/2306-6814.2023.7.135
3. Руснак О. Ризик-менеджмент у стратегічному управлінні: від загроз до проактивних стратегій. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління*. 2025. № 2(78). С. 148–156. DOI: https://doi.org/10.32689/2523-4625-2025-2(78)-22
4. Пащенко Є.М., Іващенко С.М. Поняття та принципи управління ризиками в Міністерстві оборони України та Збройних Силах України. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2023. Вип. 77. Ч. 2. С. 102–107. DOI: https://doi.org/10.24144/2307-3322.2023.77.2.17.
5. Степанян М., Шевченко А. Оцінка координації управління ризиками та загрозами. Київ: ПРООН в Україні, 2020. 60 с. URL: https://www.undp.org/sites/g/files/zskgke326/files/migration/ua/Risk-and-Threats-Management-Coordination-Assessment_UA.pdf (дата звернення: 16.12.2025).
6. Ярмусь Д. В. Ризик-менеджмент в умовах воєнного стану:адаптація моделей управління. *Вісник ХНТУ. Управління та адміністрування*. 2025. № 2(93). Ч. 1. DOI: https://doi.org/10.35546/kntu2078-4481.2025.2.1.45.
7. Kustrich K., Loishyn A. Analysis of factors of external and internal influence on the efficiency of the functioning of the internal control system. *Journal of Scientific Papers «Social Development and Security»*. 2019. № 9 (2). P. 37–56. DOI: https://doi.org/10.33445/sds.2019.9.2.4
8. Турінський О.В., Демідов Б.О., Гриб Д.А., Хмелевська О.О. Науково-методологічні аспекти управління ризиками у системі державного оборонного замовлення. *Наука і техніка Повітряних Сил Збройних Сил України.* 2020. № 2(39). С. 37–46. https://doi.org/10.30748/nitps.2020.39.04
9. Kustrich K., Loishyn A. To the issue of risk management in the Ministry of defense of Ukraine and Armed Forces of Ukraine. *Journal of scientific papers "social development & security".* 2018. №1(1). P. 27–36. DOI: https://doi.org/10.5281/zenodo.1183889

REFERENCES

1. ISO 31000:2018. Retrieved from https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_31000_2018.pdf [in English].
2. Naumenko, V. (2023). Poniattia nevyznachenosti ta vidobrazhennia ryzyku u praktytsi formuvannia derzhavnykh tsilovykh prohram sotsialno-ekonomichnoho rozvytku [The concept of uncertainty and risk reflection in the practice of forming state target programs of socio-economic development]. *Investytsii: praktyka ta dosvid – Investments: practice and experience*, *7.* DOI: https://doi.org/10.32702/2306-6814.2023.7.135 [in Ukrainian].
3. Rusnak, O. (2025). Ryzyk-menedzhment u stratehichnomu upravlinni: vid zahroz do proaktyvnykh stratehii [Risk management in strategic management: from threats to proactive strategies]. *Naukovi pratsi Mizhrehionalnoi Akademii upravlinnia personalom. Politychni nauky ta publichne upravlinnia – Scientific works of the Interregional Academy of Personnel Management. Political Science and Public Administration, 2(78),* 148–156. DOI: https://doi.org/10.32689/2523-4625-2025-2(78)-22 [in Ukrainian].

© Абражевич М.

4. Pashchenko, Ye.M., & Ivashchenko, S.M. (2023). Poniattia ta pryntsypy upravlinnia ryzykamy v Ministerstvi oborony Ukrainy ta Zbroinykh Sylakh Ukrainy [Concepts and principles of risk management in the Ministry of Defense of Ukraine and the Armed Forces of Ukraine]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo – Scientific Bulletin of Uzhhorod National University. Series: Law, 77,* 2, 102–107. DOI: https://doi.org/10.24144/2307-3322.2023.77.2.17 [in Ukrainian].
5. Ctepanian, M., & Shevchenko, A. (2020). Otsinka koordynatsii upravlinnia ryzykamy ta zahrozamy [Assessment of coordination of risk and threat management]. Kyiv: PROON v Ukraini. *www.undp.org.* Retrieved from https://www.undp.org/sites/g/files/zskgke326/files/migration/ua/Risk-and-Threats-Management-Coordination-Assessment_UA.pdf [in Ukrainian].
6. Iarmus, D. V. (2025). Ryzyk-menedzhment v umovakh voiennoho stanu:adaptatsiia modelei upravlinnia [Risk management in wartime conditions: adaptation of management models]. *Visnyk KhNTU. Upravlinnia ta administruvannia - Bulletin of KhNTU. Management and administration*, *2(93),* 1. DOI: https://doi.org/10.35546/kntu2078-4481.2025.2.1.45 [in Ukrainian].
7. Kustrich, K., & Loishyn, A. (2019). Analysis of factors of external and internal influence on the efficiency of the functioning of the internal control system. *Journal of Scientific Papers "Social Development and Security*, *9 (2),* 37–56. DOI: https://doi.org/10.33445/sds.2019.9.2.4 [in English].
8. Turinskyi, O.V., Demidov, B.O., Hryb, D.A., & Khmelevska, O.O. (2020). Naukovo-metodolohichni aspekty upravlinnia ryzykamy u systemi derzhavnoho oboronnoho zamovlennia [Scientific and methodological aspects of risk management in the system of state defense orders]. *Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy - Science and Technology of the Air Force of the Armed Forces of Ukraine*, *2(39),* 37–46. DOI: https://doi.org/10.30748/nitps.2020.39.04 [in Ukrainian].
9. Kustrich, K., & Loishyn, A. (2018). To the issue of risk management in the Ministry of defense of Ukraine and Armed Forces of Ukraine. *Journal of scientific papers "social development & security"*, *1(1),* 27–36. DOI: https://doi.org/10.5281/zenodo.1183889 [in English].

Історія статті / Article history:
Подано до редакції / Submitted to the editorial office (17.12.2025);
Прийнято до друку / Accepted for publication (20.01.2026);
Опубліковано / Published (06.04.2026).