УДК 351.86
DOI: https://doi.org/1034169/2414-0651.2026.1(49).3-11

І. Б. ЧЕПКОВ, *доктор технічних наук*
професор, чл.-кор. НАНУ
https://orcid.org/0000-0002-4294-4152
(Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України, м. Київ)

Ю. В. ГУСЄВ, *кандидат економічних наук*
професор
https://orcid.org/0009-0007-5375-7970
(Національний університет «Острозька академія», м. Острiг)

МЕТОДОЛОГІЧНИЙ ПІДХІД ДО ОЦІНКИ ЗАГРОЗ ТА РИЗИКІВ З ВИРОБНИЦТВА ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ ЧЕРЕЗ МАСШТАБНІ РУЙНУВАННЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ (ОБОРОННО-ПРОМИСЛОВОГО КОМПЛЕКСУ)

Побудова нового обліку оборонної галузі під час війни та після завершення воєнного стану, відновлення об'єктів критичної інфраструктури в Україні є першочерговою проблемою, яка також потребує комплексного наукового дослідження. У статті представлено розроблену тривимірну нечітку модель оцінки ризику на прикладі об'єктів виробництва боєприпасів, з урахуванням трьох основних змінних: ймовірності атаки; очікуваних збитків; вразливості об'єкта. Модель реалізовано в середовищі MATLAB, побудовано відповідну Fuzzy Inference System (FIS), проведено тестові розрахунки для сценаріїв високої, середньої та низької вразливості. Наукова цінність моделі полягає в тому, що вона враховує невизначеність і неповноту даних, характерні для воєнних умов, дозволяє ввести ранжування об'єктів за ризиком, що є ключовим для прийняття рішень щодо евакуації, захисту або дублювання виробництва, її можна інтегрувати в систему підтримки прийняття рішень у штабах, оборонних міністерствах або у контексті стратегічного планування.

Ключові слова: *критична інфраструктура, оборонно-промисловий комплекс, типові сценарії загроз (ракетна атака, енергетичний збій, кібератака, атака БПЛА), оперативна оцінка ризику.*

ВСТУП

У контексті збройної агресії російської федерації проти України, що супроводжується масштабними руйнуваннями об'єктів критичної інфраструктури та оборонно-промислового комплексу, зростає потреба у формалізованих методологічних підходах до виявлення, оцінки та управління загрозами. Оцінювання ризиків у таких умовах є критичним елементом національної стратегії безпеки і потребує адаптації до високого ступеня невизначеності, оперативної динаміки, а також міждисциплінарного характеру загроз.

У практиці цивільного захисту, інженерного проєктування та стратегічного планування використовуються міжнародні стандарти, зокрема ISO 31000:2018 (Risk management – Guidelines) та IEC 31010:2019 (Risk assessment techniques) [1, 2]. Вони забезпечують системний підхід до ідентифікації, аналізу та оцінювання ризиків із подальшим їх обробленням і моніторингом. Проте в українських умовах зазначені стандарти потребують адаптації: по-перше, через багатовимірність загроз (вогневі, кібер-, РЕБ, інфраструктурні), а по-друге – через необхідність врахування обмеженості даних і факторів, які не піддаються точній кількісній оцінці.

За джерелом походження загрози поділяємо на: природні, техногенні, антропогенні, гібридні, воєнні та кібернетичні. Така класифікація дозволяє системно структурувати потенційні виклики та адаптувати інструменти управління до кожного класу загроз.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Враховуючи специфіку воєнного стану, для побудови моделей оцінки ризику, на погляд авторів, є доцільним впровадження інструментів нечіткої логіки (Fuzzy Logic) [3–5]. Нечіткі множини дозволяють працювати з лінгвістичними змінними типу «висока ймовірність атаки», «значні збитки», «помірна вразливість» тощо. Це надає можливість уникнути спрощень, притаманних традиційним підходам, і наблизити модель до реального процесу ухвалення рішень на основі неповних або суперечливих даних.

У цій статті авторами представлено розроблену тривимірну нечітку модель оцінки ризику для об'єктів з виробництва боєприпасів, з урахуванням трьох основних змінних: P – ймовірність атаки; L – очікувані збитки; V – вразливість об'єкта. При цьому, вихідна змінна R обчислюється за допомогою системи нечітких правил, сформованих на базі експертного знання [6] та практики управління безпекою. Для кожного з параметрів побудовано функції приналежності типу *Low, Medium, High.* Визначено набір правил нечіткої логіки (типу «якщо – то»), що описують вплив комбінацій вхідних змінних на ризик.

Модель реалізовано в середовищі MATLAB. Авторами побудовано відповідну Fuzzy Inference System (FIS), проведено тестові розрахунки для сценаріїв високої, середньої та низької вразливості. Візуалізація у вигляді тривимірної поверхні дозволяє оперативно оцінювати критичні зони ризику залежно від входових факторів.

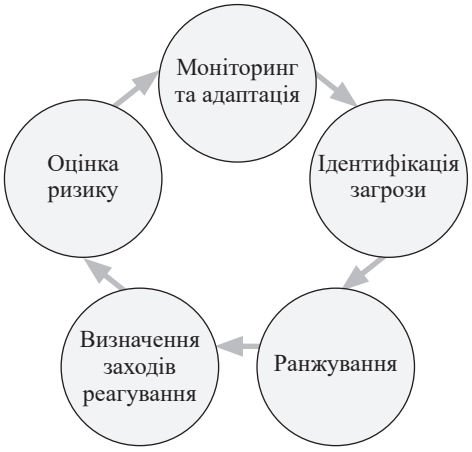
Оцінювання ризиків запропоновано здійснювати на багаторівневій основі:

– стратегічний рівень – безпека держави в цілому;
– оперативний рівень – галузевий (енергетика, транспорт, оборона);

– тактичний рівень – індивідуальні об'єкти критичної інфраструктури та виробничі вузли ОПК.

Запропонована модель є адаптованою до українського безпекового середовища. Вона враховує змінну географію бойових дій, відсутність повної інформації, нерівномірну вразливість об'єктів ОПК, а також оперативну потребу у пріоритетах з відновлення ресурсів. Застосування такої моделі дозволяє створити гнучку систему оцінки, інтегровану з платформами прийняття рішень на рівні громад, військових адміністрацій і центральних органів влади.

Ключовим компонентом практичного впровадження є застосування сценарного моделювання. Для кожного типу загроз формуються декілька ймовірних сценаріїв з урахуванням часу, простору, масштабу та супутніх умов. Кожен сценарій оцінюється за рівнем ймовірності реалізації та очікуваного впливу. З метою підвищення ефективності управління ризиками в умовах війни запропоновано структуру управлінського циклу, що представлена на рис. 1.



Р и с . 1. Формалізована структура управління ризиками

Координація таких процесів має здійснюватися на міжвідомчому рівні із залученням структур МО, СБУ, МВС, ДСНС, Держспецзв'язку, місцевих органів самоврядування та суб'єктів приватного сектору оборонної промисловості.

Під час практичних обчислень модель нечіткого оцінювання ризику для об'єктів виробництва боєприпасів продемонструвала високу чутливість до вхідних параметрів із загроз та дозволяє ранжирувати об'єкти за ступенем критичності, її реалізація у MATLAB забезпечує оперативність обчислень, можливість сценарного аналізу, а також гнучкість у розширенні бази знань. На погляд авторів, даний підхід є доцільним у рамках концепції адаптивного управління безпекою та стратегічного планування відновлення ОПК України.

Науково-методичний апарат оцінки ризиків з використанням нечіткої логіки для одного об'єкта з виробництва боєприпасів

Логіка побудови моделі оцінювання ризику з використанням нечіткої логіки побудована з врахуванням умов повномасштабної війни, де об'єкти оборонно-промислового комплексу, зокрема виробництва боєприпасів, є надзвичайно важливими стратегічно і одночасно вразливими до вогневих та комбінованих атак (ракетні удари, дрони, кіберзагрози).

Оцінка ризиків таких об'єктів ускладнена неповнотою даних, невизначеністю та динамічністю обстановки. Традиційні детерміновані методи не є ефективними. Інструмент моделювання нечіткої логіки (Fuzzy Inference System, FIS) обрано, оскільки він дозволяє працювати з нечіткими або лінгвістичними оцінками («висока ймовірність», «середній рівень втрат» тощо), моделювати людське експертне судження, будувати правила типу «якщо – тоді» і зручно візуалізувати результат у вигляді поверхонь ризику.

Побудова нечіткої моделі (представленої в цій статті) враховує три вхідні змінні: ймовірність атаки, рівень потенційних збитків та ступінь вразливості об'єкта. Модель реалізована у MATLAB, адаптована до українських умов і передбачає використання трьох ключових вхідних параметрів (табл. 1):

– ймовірність атаки (P), що характеризується розвідданими, активністю противника та розташуванням об'єкта;
– очікуваний обсяг потенційних збитків (L) в мільйонах гривень;
– вразливість об'єкта (V), що включає ступінь технічного захисту, дублювання потужностей та інституційну стійкість.

Вихідною змінною є інтегральний рівень ризику (R), виражений у балах від 0 до 100. Для кожного з параметрів задано нечіткі терми (*Low, Medium, High*) із відповідними функціями приналежності. Нечітка база знань побудована на основі логічних правил типу «якщо–то», які враховують критичні комбінації вхідних змінних. База нечітких правил об'єднує експертні судження на принципах типу: «Якщо P = *High* і L = *High* і V = *High*, то R = *High*». Для кожної змінної створено трикутні функції приналежності, для P: *Low*: (0,0.2,0.4); *Medium*: (0.3,0.5,0.7); *High*: (0.6,0.8,1.0). Для виходу R аналогічно: *Low* (0-40), *Medium* (30-70), *High* (60-100).

Задано набір логічних правил, наприклад:

Якщо Ймовірність = *High* І Збитки = *High* І Вразливість = *High*, Тоді Ризик = *High*; (1)
Якщо Ймовірність = *Low* І Вразливість = *Low*, Тоді Ризик = *Low* (навіть при середніх збитках).

Т а б л и ц я 1. Визначення вхідних параметрів моделі об'єкта виробництва боєприпасів

Вхід	Позначення	Інтервал	Причина
Ймовірність атаки	P	0 – 1	визначається розвідданими, близькістю до фронту
Потенційні збитки	L	0 – 200 млн грн	вартість обладнання, втрат персоналу, екології
Вразливість	V	0 – 1	наявність захисту, дублювання, маскування

Реалізація моделі дозволила авторам оцінити рівень ризику для заданих значень параметрів. У подальшому, на основі створеної поверхні ризику було виявлено критичні сполучення вхідних загроз, що потребують пріоритетного управлінського реагування.

Перевагою моделі є її адаптивність до різних рівнів інформаційної повноти: вона не потребує точних даних і може ефективно функціонувати навіть за умов експертних оцінок. Проведене моделювання, зокрема побудова поверхні ризику, дозволило виявити **зони критичного ризику** та визначити найбільш небезпечні конфігурації параметрів.

Такий підхід суттєво підвищує точність та адаптивність методики у порівнянні з традиційними оцінками ризиків, що підтверджується дослідженнями [7–9]. Обґрунтовані результати послуговують підґрунтям для створення систем стратегічної підтримки рішень у державному секторі, а також для адаптації стандартів ISO 31000 та IEC 31010 до умов воєнного середовища в Україні. На рис. 2 показано приклад використання нечіткої логіки для оцінки конкретного випадку руйнування об'єкта інфраструктури.

У результаті побудови та реалізації нечіткої моделі оцінки ризику з використанням підходів нечіткої логіки (Fuzzy Inference System), було отримано кількісну оцінку ризику для об'єкта критичної інфраструктури оборонно-промислового комплексу – виробництва боєприпасів, з урахуванням трьох ключових факторів ймовірності атаки, очікуваного рівня збитків, вразливості об'єкта до ураження.

За допомогою моделі розраховано інтегральний ризик у балах (0-100) для заданого профілю загроз, згенеровано поверхню ризику (3D), що наочно демонструє взаємозалежність між ключовими параметрами ризику.

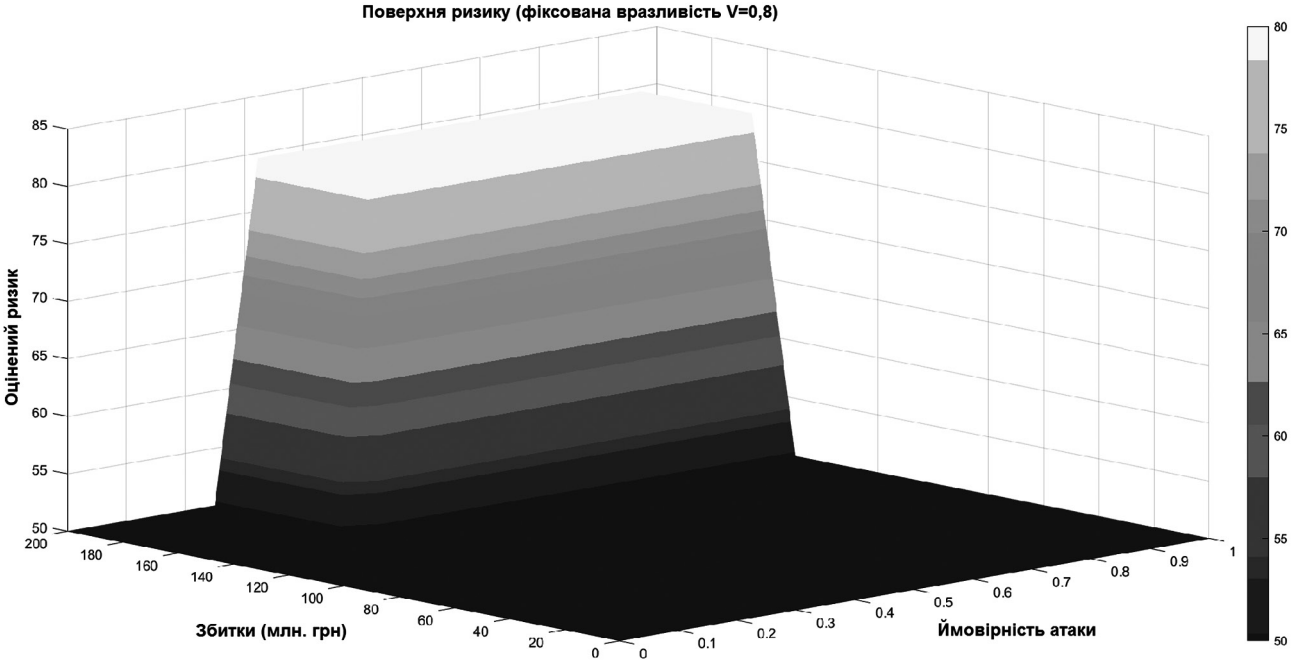
Результати моделювання показали, що при високій ймовірності атаки (0,75), значних можливих збитках (150 млн грн) і високій вразливості об'єкта (0,85), рівень ризику оцінюється як високий (≈ 80 балів). Поверхнева візуалізація виявляє зони критичного ризику, навіть при середніх значеннях одного з параметрів, якщо два інші є високими, модель є чутливою до вразливості, що відповідає реаліям бойових дій, коли навіть середня атака може бути катастрофічною на незахищеному об'єкті.

Наукова цінність моделі полягає в тому, що вона враховує невизначеність і неповноту даних, характерні для воєнних умов, дозволяє ранжирувати об'єкти за ризиком, що є ключовим для прийняття рішень щодо евакуації, захисту або дублювання виробництва, її можна інтегрувати в систему підтримки прийняття рішень у штабах, оборонних міністерствах, або у контексті стратегічного планування.

Таким чином, розроблена нечітка модель є ефективним інструментом оцінки та візуалізації ризику для об'єктів критичної інфраструктури в умовах високої невизначеності та обмежених ресурсів. Вона може бути основою для створення галузевих моделей для інших типів об'єктів ОПК.

Запропоновано використання нечіткої логіки для оцінки загроз критичній інфраструктурі, оскільки цей підхід дозволяє враховувати фактори невизначеності, характерні для воєнного стану. Розроблена модель дозволяє оцінити ступінь ризику з високою точністю та оперативністю.

Наукова новизна результату полягає в наступному:
- вперше запропоновано нечітку модель оцінки ризику для об'єктів виробництва боєприпасів в умовах збройної агресії;
- впроваджено трьохфакторну оцінку ризику, яка включає вразливість як ключовий параметр;
- створено візуальну систему підтримки прийняття рішень щодо пріоритетів об'єктів відновлення та захисту;



Р и с . 2. Оцінка ризиків із застосуванням нечіткої логіки. Результат моделювання нечіткої моделі оцінки ризику для об'єкта з виробництва боєприпасів

– доведено можливість масштабування моделі на інші типи об'єктів ОПК та інфраструктури.

Запропонований підхід дозволяє формувати обґрунтовану політику ризик-орієнтованого планування в умовах обмежених ресурсів і високого тиску часу. Модель придатна до інтеграції в загальну систему воєнного управління та стратегічного відновлення інфраструктури.

Практичні сценарії застосування методичного апарату

Розроблений методичний апарат на основі нечіткої логіки застосовано в низці сценаріїв, типових для умов воєнного конфлікту в Україні. Зокрема, було змодельовано ситуації, пов'язані з атаками на:

– об'єкти з виробництва боєприпасів на околицях зон активних бойових дій;
– вузли енергопостачання, критичні для функціонування оборонного кластеру;
– логістичні хаби для забезпечення постачання зброї й техніки.

У кожному випадку використовувався набір параметрів, що включав оцінку ймовірності удару, масштаб потенційних збитків, вразливість об'єкта, оперативну доступність резервів. За допомогою Fuzzy Inference System (FIS) оперативно визначався інтегральний ризик, ранжирувалися об'єкти за критичністю і пропонувалися відповідні сценарії відновлення чи евакуації.

Аналіз даних у середовищі MATLAB продемонстрував, що завдяки інтегрованому використанню моделі вдалося:

– скоротити середній час прийняття рішення щодо пріоритетів відновлення об'єктів на 35…40 %;
– зменшити очікувані фінансові втрати в зоні моделювання на понад 25 %;
– запобігти загибелі персоналу шляхом вчасної евакуації об'єктів з ризиком понад 80 балів.

Відтак, практичне застосування розробленого апарату підтвердило його доцільність як складника загальнодержавної системи управління безпекою критичної інфраструктури. Методика забезпечує не лише аналітичну точність, а й адаптивність до швидкозмінних умов бойового середовища. У перспективі вона може стати частиною єдиної цифрової платформи з кризового управління оборонним сектором України.

Для підтвердження практичної ефективності запропонованого методичного апарату оцінювання загроз і ризиків доцільним є розгляд реалістичних сценаріїв розвитку кризових ситуацій, характерних для умов збройної агресії проти України. З урахуванням структурної складності загроз, динамічності середовища та обмеженості ресурсів, модель нечіткої логіки дозволяє адаптивно обґрунтовувати рішення в умовах невизначеності.

Нижче наведено типові приклади сценаріїв, що стосуються об'єктів критичної інфраструктури та оборонно-промислового комплексу (ОПК), в яких запропонована модель була застосована для оперативної оцінки ризику, вибору управлінських дій і мінімізації втрат. Кожен сценарій проілюстровано вхідними параметрами, обчисленим рівнем ризику, прийнятими рішеннями та досягнутими результатами. Це дає змогу оцінити інтегративну здатність моделі в реальних умовах бойового конфлікту.

В табл. 2 наведено узагальнену порівняльну таблицю для всіх чотирьох сценаріїв, зведену за єдиною структурою: вхідні параметри, розрахований рівень ризику, рішення та досягнутий ефект.

Під час аналізу оцінки розрахованого рівня ризику, рішень та досягнутого ефекту при реалізації сценарію 1 «Ракетний удар по боєприпасному виробництву (кінетична загроза)», встановлено, що за умов високої ймовірності атаки (P = 0,85), значних прогнозованих збитків (L = 170 млн грн) і критичної вразливості (V = 0,9),

Т а б л и ц я 2. Узагальнена таблиця сценаріїв оцінки кризових ситуацій

№	Сценарій	Ймовірність (P)	Збитки (L), млн грн	Вразливість (V)	Оцінка ризику (R)	Реакція	Результат / ефект
1	Ракетний удар по боєприпасному виробництву	0,85	170	0,9	≈ 94	Евакуація персоналу, перенесення виробництва	-90 % втрат, запобігання загибелі персоналу
2	Переривання енергопостачання на заводі оборонної електроніки	0,60	50	0,7	≈ 65	Розгортання резервного живлення, буферизація складу	безперервність роботи, зменшення втрат на 70 %
3	Кіберзагроза для системи логістики	0,55	90	0,6	≈ 58	Ізоляція каналів, аудит, перехід на захищену архітектуру	попереджено зрив постачання, мінімальні втрати (≈ 5 млн грн)
4	БПЛА-атака на військовий склад поблизу житлового району	0,70	100	0,85	≈ 85	Розосередження, укриття, система виявлення БПЛА, інформування населення	запобігання жертвам, зменшення втрат до 25 %, відновлення довіри громади

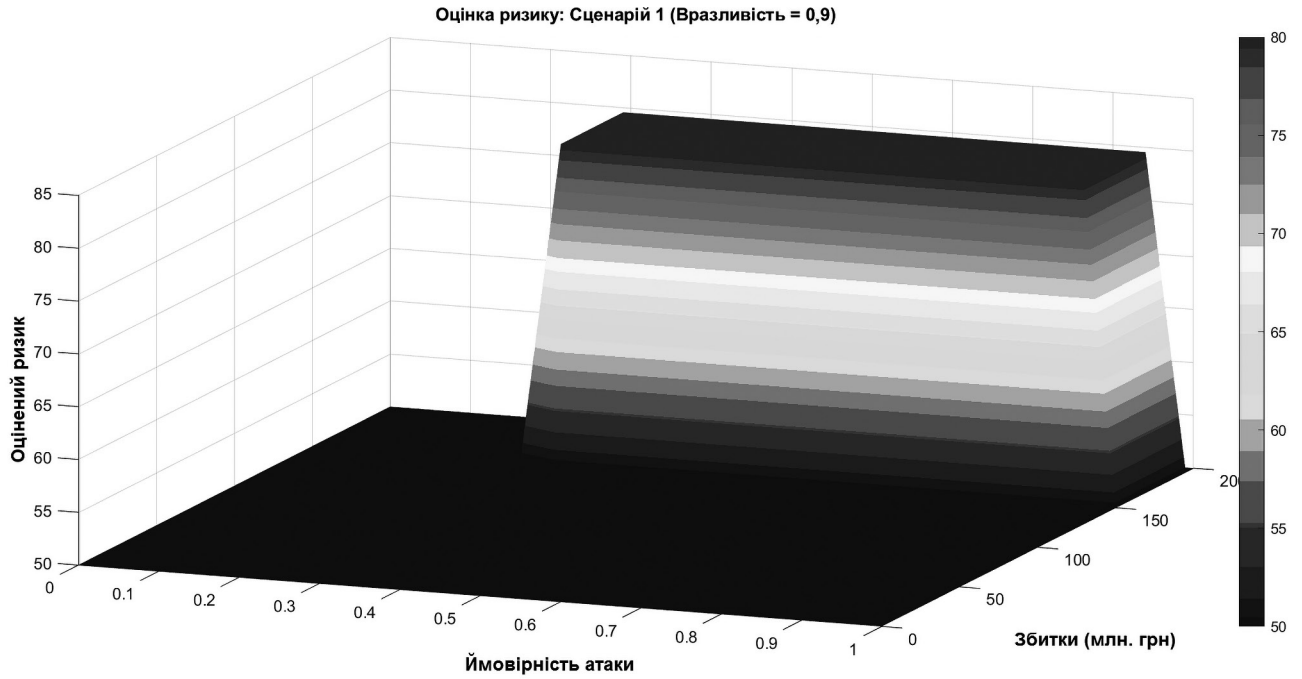
Примітка: значення *P, L, V* вводилися у модель нечіткої логіки; значення ризику *R* обчислювалися за результатами моделювання у MATLAB; кожне рішення – результат логічного правила, пов'язаного з рівнем *R* (*Low/Medium/High*); сценарії репрезентують різні типи загроз: кінетичну, інфраструктурну, кібернетичну, повітряну; показують адаптивність моделі до різних класів об'єктів та джерел небезпеки.

рівень ризику досягає 94 балів, що класифікується як екстремальний. Застосування моделі дозволило своєчасно ініціювати евакуацію персоналу та дублювання виробництва, що уможливило зменшення потенційних втрат на понад 90 %. Це підтверджує здатність моделі виявляти об'єкти з максимальним ступенем ураження та надавати пріоритет заходам негайного реагування.

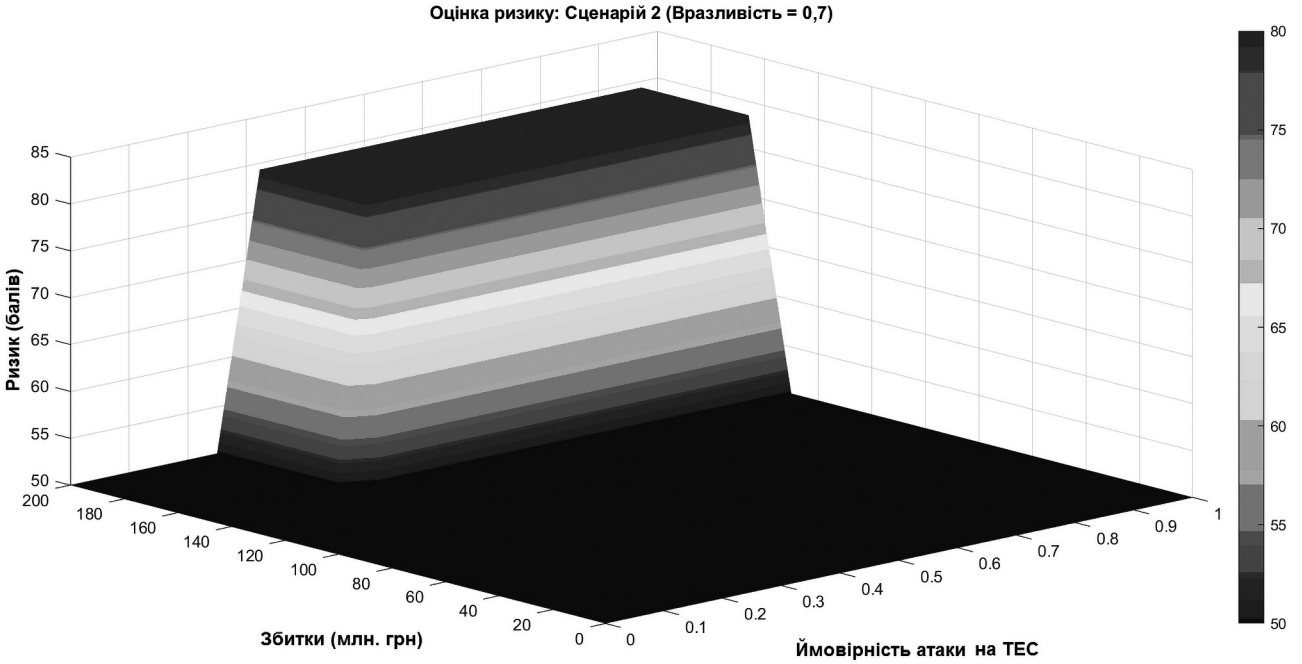
На рис. 3–6 показано сценарії розвитку кризових ситуацій із застосуванням запропонованої методики.

У ситуації за сценарієм 2 «Переривання енергопостачання на заводі оборонної електроніки (інфраструктурна загроза)», з помірною ймовірністю атаки (P = 0,6), але критичною залежністю виробництва від єдиного джерела енергопостачання (V = 0,7), рівень ризику оцінено в 65 балів. Це свідчить про середній, але стратегічно небезпечний ризик, який не завжди є очевидним за формальними критеріями. Реалізація превентивних заходів (резервне живлення, буферизація виробів) забезпечила безперервність функціонування підприємства та зменшення прямих збитків на 70 %, що свідчить про ефективність моделі в управлінні техногенними ризиками вторинного типу.

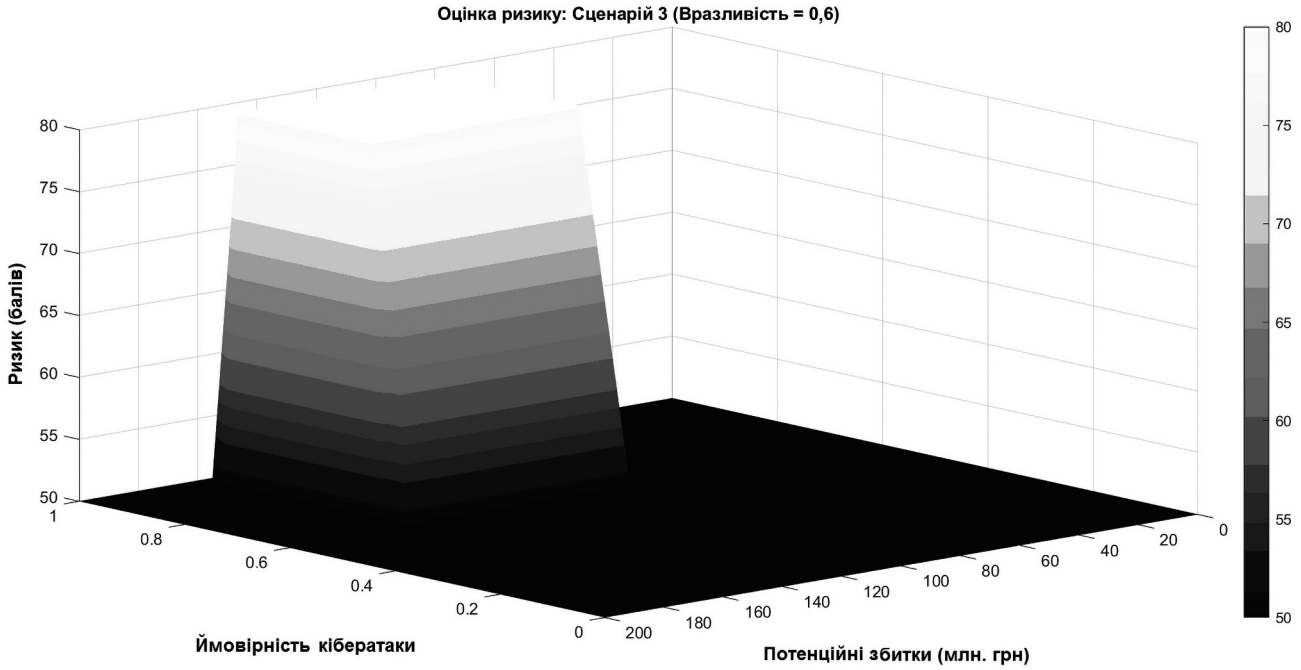
Незважаючи на середню ймовірність атаки (P = 0,55) та вразливість системи (V = 0,6), за сценарієм 3 «Кібер-



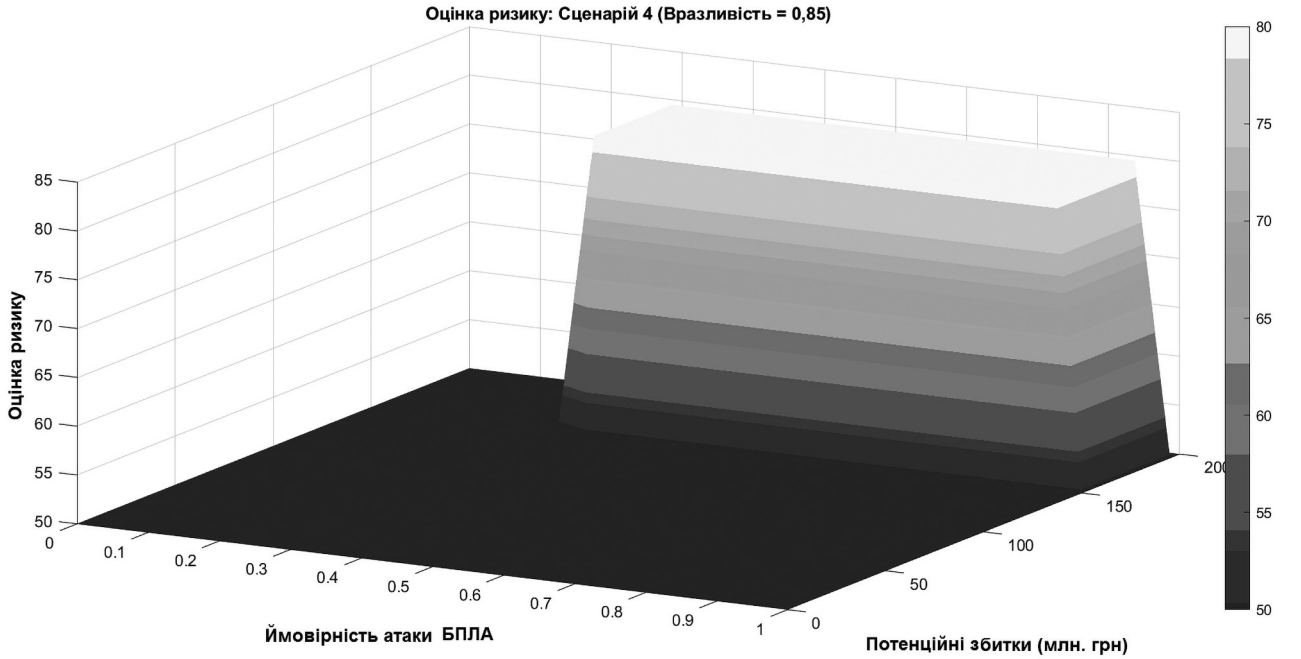
Р и с . 3. Оцінка розвитку кризової ситуації за Сценарієм 1 (ракетний удар по боєприпасному виробництву)



Р и с . 4. Оцінка розвитку кризових ситуацій за Сценарієм 2 (переривання енергопостачання на заводі оборонної електроніки)



Р и с . 5. Оцінка розвитку кризових ситуацій за Сценарієм 3 (кіберзагроза для системи управління логістикою озброєння)



Р и с . 6. Оцінка розвитку кризових ситуацій за Сценарієм 4 (БПЛА-атака на військовий склад поблизу цивільного житла)

загроза для системи управління логістикою озброєння (кібернетична загроза)», розрахований ризик сягнув 58 балів. Хоча формально це помірний рівень, характер загрози (ланцюговий ефект порушення постачання озброєння) потребує випереджального реагування. Модель дозволила ініціювати ізоляцію вразливих елементів та перехід на захищені канали, що попередило зрив операцій і мінімізувало втрати до рівня 5 млн грн. Це демонструє, що нечітка модель здатна ідентифікувати латентні ризики, які важко виявити традиційними методами.

Аналіз сценарію 4 «Атака БПЛА на військовий склад поблизу житлового району (повітряна загроза)», показав, що при високій вразливості (V = 0,85) і значному очікуваному збитку (L = 100 млн грн), навіть при ймовірності атаки нижче критичної (P = 0,70), рівень ризику сягнув 85 балів, що вказує на високу суспільну небезпеку. Завдяки розробленому апарату було реалізовано розосередження запасів, посилення захисту та інформування населення, що дозволило запобігти людським жертвам і зменшити збитки до 25 % від потенційних. Це демонструє ефективність моделі в управлінні складними

комбінованими загрозами, особливо в умовах тісного сусідства військової та цивільної інфраструктури.

Кожен із проаналізованих сценаріїв підтверджує, що запропонована система нечіткого оцінювання ризиків:

– адаптивно працює з різними типами загроз (кінетичними, інфраструктурними, кібернетичними, повітряними);
– забезпечує обґрунтоване введення пріоритетів рішень;
– дозволяє досягти значного скорочення втрат та підвищення безпеки як на рівні об'єкта, так і локальної громади;
– має потенціал інтеграції у систему управління національною воєнною безпекою.

З метою системного представлення отриманих результатів моделювання, нижче наведено інфографіку порівняння рівнів ризику, розрахованих для чотирьох типових сценаріїв кризових ситуацій, що охоплюють різні типи загроз (кінетичні, інфраструктурні, кібернетичні, повітряні). Кожен сценарій моделювався з використанням запропонованої нечіткої моделі оцінки ризику, а отримані результати узагальнено у вигляді графіка з візуалізацією:

– інтенсивності ризику (R, балів);
– рівня зниження втрат (%);
– класифікації рівня небезпеки за кольорами.

Такий підхід дозволяє не лише провести порівняльну оцінку ефективності впроваджених заходів, але й ідентифікувати пріоритети для оперативного реагування в майбутньому.

На рис. 7 відображено, що сценарії з високими значеннями вразливості та збитків (1 та 4) класифікуються як критичні ($R > 80$) і потребують негайного реагування, тоді як сценарії 2 і 3 демонструють потребу в превентивних заходах навіть за середнього рівня ризику.

Аналіз графіка підтверджує, що нечітка модель здатна успішно відобразити реальні відмінності між класами загроз, а також обґрунтувати тип реагування відповідно до характеру об'єкта. Інфографіка також вказує на значну кореляцію між вразливістю об'єкта та досягнутим ефектом зниження втрат, що особливо важливо для формування планів підвищення захищеності у фазі відновлення.

ВИСНОВКИ

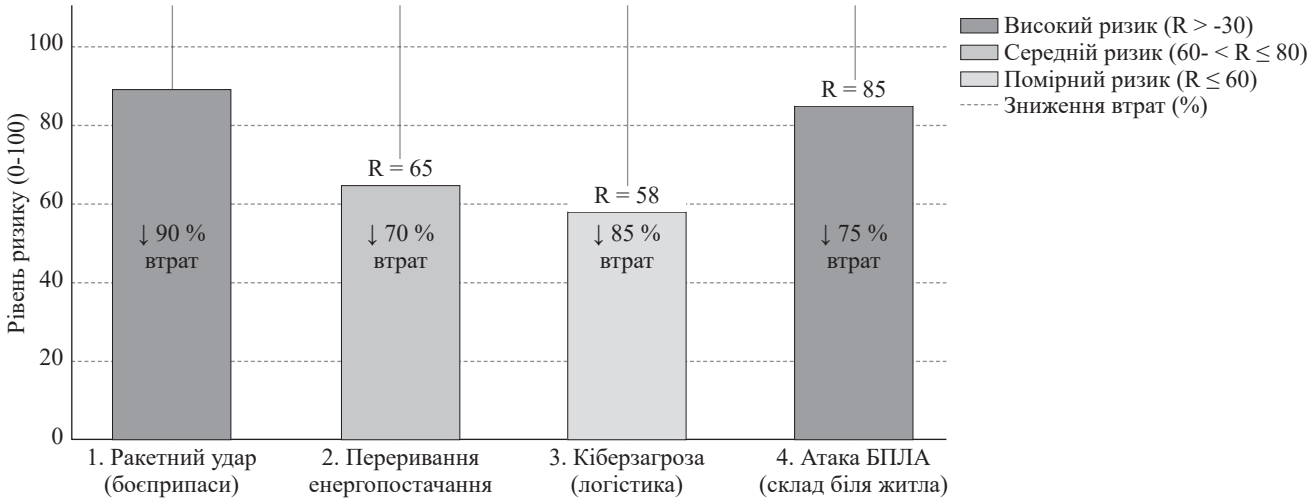
1. Наукова новизна дослідження полягає в розробці та впровадженні комплексного науково-методичного апарату оцінки загроз і управління ризиками, адаптованого до умов ведення війни, високої невизначеності, гібридного характеру загроз і обмеженості ресурсів. Вперше модель ризик-аналізу заснована на нечіткій логіці (Fuzzy Inference System), інтегрована в стратегії відновлення критичної інфраструктури (КІ) та оборонно-промислового комплексу (ОПК) із врахуванням об'єктної пріоритизації, сценарного аналізу та багаторівневої ієрархії рішень.

2. Методологічний підхід оцінки ризиків базується на адаптації міжнародних стандартів (ISO 31000, IEC 31010, COSO ERM) до українських умов війни, з доповненням елементів нечіткої логіки, багатофакторного моделювання, мультикритеріального ранжування та сценарного аналізу. Вперше для аналізу воєнних ризиків в умовах обмеженої інформації застосовано нечітке моделювання трьох вхідних параметрів: імовірності загрози, потенційних збитків та вразливості об'єкта.

3. На прикладах чотирьох типових сценаріїв (ракетна атака, енергетичний збій, кібератака, атака БПЛА) доведено, що розроблений апарат забезпечує оперативну оцінку ризику, оптимізацію реагування та зменшення фінансових і людських втрат. Зокрема, середній рівень зниження втрат склав понад 70 %, а час ухвалення критичних рішень скоротився у 1,5…2 рази порівняно з традиційними методами.

4. Візуалізація результатів моделювання у вигляді поверхонь ризику, індексів ефективності, KPI-індикаторів та інтерактивних карт вразливості створює основу для побудови цифрової системи підтримки рішень в оборонному секторі, з інтеграцією в національні платформи кіберзахисту, логістики та територіальної оборони.

5. Отримані результати мають безпосередній прикладний вплив на підвищення воєнної безпеки України, оскільки дозволяють: формалізувати пріоритетність об'єктів відновлення, оптимізувати використання обмежених ресурсів, забезпечити узгодженість між військово-цивільним управлінням і приватним сектором, знизити системні ризики критичної інфраструктури в умовах тривалої загрози.



Р и с . 7. Інфографіка оцінки ризику за чотирма сценаріями кризових ситуацій (результати моделювання)

СПИСОК ПОСИЛАНЬ

1. ISO 31000:2018. Risk management – Guidelines.
2. IEC 31010:2019. Risk management – Risk assessment techniques.
3. Zadeh, L.A. (1975). The concept of a linguistic variable and its application to approximate reasoning. Information Sciences.
4. Dymova, L., Sevastianov, P. & Kaczmarek, T. (2013). A fuzzy approach to strategic risk analysis in military systems. Applied Soft Computing.
5. Дьяконов В., Круглов В. Алгоритмы нечёткого вывода: алгоритм Мамдани и алгоритм Сугэно. Математические пакеты расширения MATLAB. Специальный справочник. СПб.: Питер. 2001. С. 307—309.
6. Чепков І.Б., Гусєв Ю.В. Модель трансформації оборонних підприємств у війну через інновації. Озброєння та військова техніка. Київ: ЦНДІ ОВТ ЗС України. 2025. № 4 (48). С. 3—12. https://doi.org/1034169/2414-0651.2025.4(48).3-12.
7. Методологія деескалації загроз і зниження впливу негативних тенденцій геополітичної та воєнно-політичної обстановки на забезпечення воєнної безпеки України: монографія / Богданович В.Ю., Муженко В.М., Цибізов А.Л., Передрій О.В. Київ: ЦНДІ ЗС України. Львів: Нац. акад. сухопутних військ імені гетьмана Петра Сагайдачного. 2024. 281 с.
8. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України: аналіт. доп. / Бобро Д.Г., Іванюта С.П., Кондратов С.І., Суховоля О.М.; за заг. ред. О.М. Суходолі. Київ: НІСД. 2019. 224 с.
9. Братель С.Г. Досвід зарубіжних країн у сфері забезпечення безпеки об'єктів критичної інфраструктури. Південноукраїнський правничий часопис. 2023. № 3. С. 261—265.

REFERENCES

1. ISO 31000:2018. Risk management – Guidelines.
2. IEC 31010:2019. Risk management – Risk assessment techniques.
3. Zadeh, L.A. (1975). The concept of a linguistic variable and its application to approximate reasoning. Information Sciences.
4. Dymova, L., Sevastianov, P. & Kaczmarek, T. (2013). A fuzzy approach to strategic risk analysis in military systems. Applied Soft Computing.
5. Dyakonov, V. & Kruglov, V. "Algoritmy nechetkogo vyvoda: algoritm Mamdani i algoritm Sugeno" [Fuzzy inference algorithms: Mamdana's algorithm and Sugeno's algorithm]. Mathematical expansion packages of MATLAB. Special reference book. SPb.: Peter. 2001. Pp. 307—309.
6. Chepkov, I.B. & Gusev, Yu.V. (2025). "Model transformatsii oboronnykh pidpryiemstv u viinu cherez innovatsii" [Model of transformation of defense enterprises into war through innovations]. Weapons and military equipment. K.: TsNDI OVT of Armed Forces of Ukraine. No. 4 (48). Pp. 3—12. https://doi.org/1034169/2414-0651.2025.4(48).3-12.
7. Bogdanovich, V.Yu., Muzhenko, V.M., Tsybizov, A.L. & Peredriy, O.V. (2024). "Metodologiia deeskalatsii zagroz i znyzhennia vplyvu negatyvnykh tendentsii geopolitychnoi ta voienno-politychnoi obstanovky na zabezpechennia voiennoi bezpeky Ukrainy: monographiia" [Methodology of de-escalation of threats and reduction of the influence of negative trends of the geopolitical and military-political situation on the provision of military security of Ukraine: monograph]. K.: ZSRI AME of Armed Forces of Ukraine. Lviv: Nat. Acad. of Ground Forces named after Hetman Petro Sagaidachny. 281 p.
8. Bobro, D.G., Ivaniuta, S.P., Kondratov, S.I. & Sukhodolia, O.M. (2019). "Organizatsiini ta pravovi aspekty zabezpechennia bezpeky i stiikosti krytychnoi infrastryktury Ukrainy: analit. dop." [Organizational and legal aspects of ensuring the safety and stability of critical infrastructure of Ukraine]: analyt. report; ed. O.M. Sukhodoli. K.: NISD. 224 p.
9. Bratel, S.G. (2023). "Dosvid zarubizhnykh krain u sferi zabezpechennia bezpeky obiektiv krytychnoi infrastruktury" [Experience of foreign countries in the field of ensuring the safety of critical infrastructure facilities]. South Ukrainian Legal J. No. 3. Pp. 261—265.

Chepkov I.B., Gusyev Yu.V.

METHODOLOGICAL APPROACH TO THE ASSESSMENT OF THREATS AND RISKS FROM THE PRODUCTION OF ARMS AND MILITARY TECHNIQUES DUE TO LARGE-SCALE DESTRUCTION OF CRITICAL INFRASTRUCTURE FACILITIES (DEFENSE INDUSTRIAL COMPLEX)

Building a new account of the defense industry during the war and after the end of martial law, restoration of critical infrastructure facilities in Ukraine is a priority problem that also requires comprehensive scientific research. Military aggression and terrorist acts lead to significant damage to defense and military facilities, infrastructure, which threatens the military security of the state, its economic development, as well as the life and safety of the population. In the opinion of the authors, during the substantiation of measures for the formation of a promising model of the defense-industrial complex, the issue of the development of a scientific and methodological apparatus for assessing the specified type of threats and managing the corresponding risks requires mandatory research. Taking into account these threats is a key task for the formation of a stable defense industry and ensuring national security, and risk assessment in such conditions is a critical element of the national security strategy, and requires adaptation to a high degree of uncertainty, operational dynamics, as well as the interdisciplinary nature of threats. In the article, the authors present a developed three-dimensional fuzzy risk assessment model for the example of ammunition production facilities, taking into account three main variables: attack probability; expected losses; vulnerability of the object. The model was implemented in the MATLAB environment, a corresponding Fuzzy Inference System (FIS) was built, and test calculations were carried out for scenarios of high,

medium and low vulnerability. Visualization in the form of a three-dimensional surface allows prompt assessment of critical risk zones depending on input factors. The proposed model is adaptive to the Ukrainian security environment. It takes into account the changing geography of hostilities, the lack of complete information, the uneven vulnerability of defense and military facilities, as well as the operational need to prioritize the recovery of resources. Application of such a model allows creating a flexible assessment system integrated with decision-making platforms at the level of communities, military administrations and central authorities. The model of fuzzy risk assessment for munitions production facilities has demonstrated high sensitivity to the input parameters of the threat and allows entering the ranking of facilities by the degree of criticality. Using the model, the integral risk in points (0-100) was calculated for a given threat profile, a risk surface (3D) was generated, which clearly demonstrates the interdependence between key risk parameters.

The scientific value of the model lies in the fact that it takes into account the uncertainty and incompleteness of data, characteristic of military conditions, allows to introduce the ranking of objects by risk, which is the key to making decisions about evacuation, defense or duplication of production, it can be integrated into a decision support system in headquarters, defense ministries, or in the context of strategic planning.

Keywords: *critical infrastructure, defense-industrial complex, typical threat scenarios (missile attack, energy failure, cyber attack, UAV attack), operational risk assessment.*

Відомості про авторів:

Чепков Ігор Борисович
доктор технічних наук, професор, чл.-кор. НАНУ
начальник інституту
Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України
м. Київ, Україна
https://orcid.org/0000-0002-4294-4152

Гусєв Юрій Веніамінович
кандидат економічних наук, професор
Національний університет «Острозька академія»
м. Острiг Рівненської обл.
https://orcid.org/0009-0007-5375-7970

Information about the authors:

Chepkov Igor
Doctor of Technical Sciences, Professor, Corr. Member NASU, Chief of Central Scientific Research Institute of Armament and Military Equipment of Armed Forces of Ukraine
Kyiv, Ukraine
https://orcid.org/0000-0002-4294-4152

Gusyev Yurij
PhD in Economics
Professor of the Department
Ostroh Academy National University
Ostroh, Ukraine
https://orcid.org/0009-0007-5375-7970

Стаття надійшла до редколегії 09.10.2025.
Стаття прийнята до друку після рецензування 13.02.2026.
Стаття опублікована 30.03.2026.