Електронний журнал «Державне управління: удосконалення та розвиток» включено до переліку наукових фахових видань України з державного управління (Категорія «Б», Наказ Міністерства освіти і науки України № 1643 від 28.12.2019). Спеціальність – 281.
Державне управління: удосконалення та розвиток. 2026. № 4.
ISSN 2307-2156

DOI: http://doi.org/10.32702/2307-2156.2026.4.20
УДК 351.86:005.334

М. А. Роговець,
к. т. н., доцент, начальник управління,
Науково-дослідний інститут воєнної розвідки
ORCID ID: https://orcid.org/0000-0002-1587-9017

ТЕРМІНОЛОГІЧНЕ РОЗМЕЖУВАННЯ “ВИКЛИКІВ”, “РИЗИКІВ” ТА “ЗАГРОЗ”: ВІД ТЕОРІЇ ДО ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОГО УПРАВЛІННЯ

M. Rohovets,
PhD in Technical Sciences, Associate Professor, Head of the Department,
Defense Intelligence Research Institute

TERMINOLOGICAL DISTINCTION BETWEEN “CHALLENGES”, “RISKS”, AND “THREATS”: FROM THEORY TO INFORMATION-ANALYTICAL SUPPORT OF PUBLIC ADMINISTRATION

У статті здійснено комплексне теоретичне та методологічне обґрунтування розмежування категорій “виклик”, “ризик” і “загроза” як ключових елементів оцінювання безпекового середовища та інформаційно-аналітичного забезпечення державного управління. Показано, що виклики

відображають об'єктивні макрорівневі зміни, які потребують інституційної адаптації; ризики виникають унаслідок взаємодії цих змін із вразливостями системи та можуть бути формалізовані через імовірнісні моделі; загрози ж пов'язані з наявністю активного деструктивного наміру суб'єкта та потребують негайного реагування. Запропонована ескалаційна модель, узгоджена з підходами НАТО, забезпечує логічну послідовність переходу від якісних характеристик до кількісного оцінювання, що підсилює аналітичну прозорість і відтворюваність результатів.

Методологічну основу дослідження становлять PESTLE-аналіз, матриця оцінювання ризиків та матриця оцінювання загроз, які дозволяють системно структурувати фактори безпеки та здійснювати їх математичне моделювання. На прикладі оцінювання ризику ураження енергетичної інфраструктури та визначення рівня загрози від застосування стратегічної авіації противника продемонстровано прикладну придатність моделі для підтримки управлінських рішень у секторі безпеки й оборони.

Результати дослідження свідчать, що уніфікована модель створює методологічні передумови для стандартизації процедур аналізу, зменшення суб'єктивізму та підвищення обґрунтованості рішень. Перспективи подальших розвідок пов'язані з інтеграцією часової динаміки, поведінкових параметрів акторів та цифрових інструментів моніторингу для підвищення стійкості держави до гібридних загроз.

This article develops a comprehensive conceptual and mathematical framework for distinguishing between the categories of "challenge," "risk," and "threat" as foundational components of security environment assessment and information-analytical support of public administration. Challenges are conceptualized as objective macro-level shifts requiring institutional adaptation but lacking hostile intent. Risks emerge when such shifts interact with systemic vulnerabilities and can be formalized through probabilistic models reflecting the likelihood and potential impact of adverse events. Threats, in turn, are associated

with an actor's deliberate hostile intent and the availability of capabilities to implement it, thereby necessitating immediate and coordinated response measures.

The proposed escalation model, aligned with NATO methodological approaches, ensures a coherent transition from qualitative expert judgments to quantitatively verifiable indicators, enhancing analytical transparency, reproducibility, and methodological consistency. The study employs PESTLE analysis, a risk assessment matrix, and a threat assessment matrix to structure security-relevant factors and demonstrate the model's applicability to real-world analytical tasks, including scenarios related to energy infrastructure vulnerability and adversary air capabilities.

The article underscores the importance of harmonizing national analytical practices with international standards to improve interoperability, situational awareness, and coordinated decision-making. Integrating the proposed model into institutional workflows enhances the comparability of assessments and strengthens interagency communication. Additionally, the study highlights the broader implications of adopting a unified conceptual framework for national resilience, emphasizing its potential to support integrated monitoring architectures, early identification of destabilizing trends, and adaptive planning. Embedding these analytical tools into routine governance processes contributes to a more proactive, data-driven, and resilient system of public administration capable of functioning effectively under prolonged strategic pressure.

Ключові слова: *державне управління; інформаційно-аналітичне забезпечення; ескалаційна модель; виклик; ризик; загроза.*

Keywords: *public administration; information-analytical support; escalation model; challenge; risk; threat.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. В умовах динамічної трансформації глобального та регіонального безпекового середовища

ефективність державного управління критично залежить від якості інформаційно-аналітичної роботи. Однією з фундаментальних проблем у цій площині залишається відсутність єдиного, концептуально узгодженого підходу до тлумачення та розмежування ключових безпекових категорій: “виклик”, “ризик” та “загроза”.

У чинній нормативно-правовій базі та відомчих документах ці терміни нерідко використовуються як взаємозамінні синоніми. На практиці така розмитість понятійного апарату безпосередньо ускладнює об’єктивну оцінку безпекового середовища, створює передумови для неефективного розподілу ресурсів і дублювання функцій різних інституцій, а також знижує загальну дієвість планування застосування наявних сил і засобів. Для фахівців, які здійснюють інформаційно-аналітичне забезпечення, відсутність чітких дефініцій стає на заваді переходу від суто описових висновків до точних математичних розрахунків рівнів небезпеки.

Крім того, стратегічний курс на євроатлантичну інтеграцію вимагає глибокої інституційної адаптації. Неузгодженість національної термінології з міжнародними стандартами управління та глосаріями є суттєвою перешкодою для імплементації стандартів НАТО, а також забезпечення оперативної сумісності (інтероперабельності) та синхронізації алгоритмів ухвалення рішень із країнами-партнерами.

Отже, **актуальність проблеми** полягає у нагальній потребі концептуального та методологічного розмежування вказаних категорій для подолання термінологічної ентропії, переведення інформаційно-аналітичних оцінок у вимірювані показники та розробки уніфікованої системи державного управління, адаптованої до сучасного безпекового середовища.

Аналіз останніх досліджень та публікацій. Питання концептуалізації безпекових термінів та управління ризиками перебуває в центрі уваги багатьох вітчизняних і зарубіжних дослідників. Теоретико-методологічні засади формування безпекового середовища, державної політики у сфері національної безпеки та категоріального апарату безпекових студій закладено

у працях В. Горбуліна, О. Власюка, Б. Парахонського [1; 2]. Окремі аспекти адміністративно-правового регулювання, інституційної стійкості та термінологічної визначеності в державному управлінні досліджували Т. Коломоєць, В. Колпаков та інші вчені [3].

У західній науковій традиції проблематика розмежування категорій невизначеності, ризиків та загроз детально розроблена в межах безпекознавства (Security Studies), стратегічного планування та ризик-менеджменту. Міжнародні стандарти ISO 31000, ISO 22301, а також глосарії НАТО (зокрема AAP-06) пропонують формалізовані підходи до класифікації ризиків і загроз, що широко застосовуються в оборонному та цивільному секторах [4; 5]. Значна кількість сучасних публікацій присвячена також питанням імплементації стандартів НАТО в секторі безпеки й оборони України, особливо після 2022 року.

Попри вагомий науковий доробок, більшість існуючих досліджень розглядають поняття “виклики”, “ризики” та “загрози” або у філософсько-політологічному контексті, або в межах широких концепцій глобальної безпеки. Недостатньо опрацьованою залишається прикладна площина – розробка чітких, математично обґрунтованих критеріїв розмежування цих категорій для потреб повсякденної інформаційно-аналітичної роботи державних органів.

Особливо відчутною є відсутність уніфікованих методологічних інструментів, які дозволяли б переводити якісні (описові) характеристики безпекового середовища у вимірювані кількісні показники. Це ускладнює об’єктивне планування використання сил і засобів, знижує точність оцінювання безпекової ситуації та гальмує практичне впровадження термінологічних і процедурних стандартів НАТО у діловодство та аналітичну діяльність державних інституцій.

Формулювання цілей статті (постановка завдання). З огляду на виявлені теоретичні та методологічні прогалини, метою статті є концептуальне й математично обґрунтоване розмежування понять “виклик”,

“ризик” і “загроза” як ключових категорій оцінювання безпекового середовища та інформаційно-аналітичного забезпечення державного управління. Досягнення цієї мети передбачає, по-перше, систематизацію вітчизняного термінологічного апарату та його узгодження з концептуальними підходами і глосаріями НАТО, зокрема AAP-06, що забезпечує методологічну сумісність із міжнародними стандартами. По-друге, необхідним є формування кількісних критеріїв і математичних залежностей, які дозволяють ідентифікувати зазначені категорії на основі оцінювання намірів, спроможностей та ймовірності реалізації подій, що створює підґрунтя для побудови уніфікованої ескалаційної моделі. По-третє, важливо обґрунтувати прикладну цінність запропонованого підходу для підвищення ефективності щоденної інформаційно-аналітичної діяльності державних органів, оптимізації планування сил і засобів та вдосконалення процесів державного управління в умовах динамічних безпекових викликів.

Виклад основного матеріалу дослідження. Формування дієвої системи державного управління в умовах мінливого безпекового середовища об’єктивно потребує жорсткої термінологічної дисципліни. Проте аналіз чинних стратегічних документів засвідчує практику синонімічного вживання категорій “виклик”, “ризик” і “загроза” або ж їх фрагментарне нормативне закріплення.

Зокрема, у базовому Законі України “Про національну безпеку України” наведено дефініцію лише терміну “загрози національній безпеці”, тоді як “виклики” та “ризики” фактично залишаються поза межами нормативного глосарія [6]. Своєю чергою, у Стратегії національної безпеки України [7] та Стратегії воєнної безпеки України [8] ці категорії часто об’єднуються в єдині семантичні конструкції (наприклад, “глобальні виклики та загрози”) без чіткого розмежування їхньої природи та критеріїв ідентифікації. На етапі оперативного та стратегічного планування така концептуальна розмитість призводить до нераціонального розподілу ресурсів: державний апарат часто

спрямовує зусилля на “протидію” об’єктивним викликам так само, як і конкретним загрозам, що є методологічною помилкою.

Для розв’язання цієї проблеми пропонується впровадити багаторівневу (ескалаційну) модель ідентифікації факторів безпекового середовища, яка базується на математичному моделюванні та концептуально корелюється з підходами країн-членів НАТО, зокрема з глосарієм термінів та визначень AAP-06 [5].

Первинною та найбільш макроскопічною категорією в цій координаті є **виклик (Challenge)**. У контексті державного управління виклик слід розуміти як масштабну, об’єктивну зміну середовища або “статус-кво”, яка сама по собі не містить цілеспрямованого ворожого наміру, проте вимагає обов’язкової інституційної реакції та адаптації системи. Характерними прикладами викликів є стрімкий розвиток технологій штучного інтелекту, глобальні кліматичні зміни або демографічні зсуви. Виклик неможливо “нейтралізувати” силовими методами; до нього можна лише адаптувати державні інституції. Залежно від якості державного управління, виклик може стати вікном можливостей або ж згенерувати спектр системних ризиків.

Наступним рівнем ескалації є **ризик (Risk)**, який виникає внаслідок накладання об’єктивного виклику на вразливість системи державного управління. Відповідно до міжнародного стандарту ризик-менеджменту ISO 31000, ризик визначається як вплив невизначеності на цілі [4]. Його фундаментальна відмінність від виклику полягає в тому, що ризик піддається вимірюванню та безпосередньому управлінню. В інформаційно-аналітичній діяльності ризик доцільно оцінювати через імовірнісну функцію за формулою:

$$R = P \times I_m \qquad (1)$$

де R (Risk) – загальний індекс ризику; P (Probability) – ймовірність настання негативної події; I_m(Impact) – масштаб руйнівних наслідків для державного апарату чи суспільства. Використання цієї залежності дозволяє аналітичним

підрозділам ранжувати події та визначати пріоритетні напрями для превентивного реагування.

Найвищим і найбільш критичним ступенем небезпеки є **загроза (Threat)**. Ключовим критерієм, що відмежовує загрозу від виклику чи ризику, є наявність активного актора (суб'єкта), який має цілеспрямований деструктивний намір щодо системи. У практиці планування операцій за стандартами НАТО загроза розраховується як добуток спроможності противника та його намірів [5; 9]:

$$T = C \times I \qquad (2)$$

де T (Threat) – кількісний рівень загрози; C (Capability) – сукупність наявних сил і засобів (спроможність) суб'єкта; I (Intent) – рівень ворожого наміру застосувати ці сили. Ця математична залежність (2) відіграє вирішальну роль для інформаційно-аналітичного забезпечення: якщо намір дорівнює нулю ($I = 0$), державна система стикається з викликом або ризиком, а не із загрозою, незалежно від потужності наявних спроможностей (C). Системна інтеграція цих понять у єдиний контур дозволяє державним органам здійснити перехід від якісних експертних оцінок до кількісних показників, що є об'єктивною базою для ухвалення рішень щодо цільового розподілу ресурсів.

Для переходу від концептуального розмежування категорій "виклик", "ризик" і "загроза" до їх практичного застосування в інформаційно-аналітичній діяльності державних органів необхідно здійснити первинну структуризацію факторів безпекового середовища. На цьому етапі доцільним є використання PESTLE-аналізу, який дозволяє системно класифікувати макрорівневі виклики за політичними, економічними, соціальними, технологічними, правовими та екологічними вимірами. Така структуризація створює методологічне підґрунтя для подальшої квантифікації ризиків і загроз за допомогою математичних моделей, забезпечуючи логічну послідовність у

побудові ескалаційної моделі оцінювання безпекового середовища. Результати PESTLE-аналізу наведено в табл. 1.

Таблиця 1. PESTLE-класифікація макрорівневих викликів безпекового середовища України

Компонент	Зміст виклику	Приклад впливу	Подальша трансформація
P – Political (політичні)	Поглиблення військово-технічного співробітництва між авторитарними державами; ерозія режимів нерозповсюдження	Формування нових антизахідних блоків	Генерує ризик масштабування виробництва озброєнь агресором
E – Economic (економічні)	Мілітаризація економіки РФ; санкційна адаптація противника	Зростання оборонного виробництва РФ	Підвищує ризик тривалих високих темпів війни
S – Social (соціальні)	Демографічні втрати, міграція, психологічна втома суспільства	Зниження мобілізаційного потенціалу	Підсилює ризики внутрішньої нестабільності
T – Technological (технологічні)	Масове застосування БПЛА, ШІ-систем, високоточної зброї	Зміна характеру бойових дій	Генерує ризики ураження критичної інфраструктури
L – Legal (правові)	Недостатня адаптація законодавства до стандартів НАТО; прогалини у регулюванні оборонних технологій	Уповільнення інтеграції у євроатлантичні структури	Породжує ризики неузгодженості процедур
E – Environmental (екологічні)	Ураження енергетичних об’єктів, техногенні ризики	Блекаути, забруднення довкілля	Підсилює ризики гуманітарної кризи

Для ілюстрації прикладної цінності запропонованої ескалаційної моделі доцільно розглянути практичний сценарій інформаційно-аналітичного

забезпечення планування сил і засобів в умовах повномасштабної російсько-української війни із використанням числових параметрів. На макрорівні об’єктивним викликом для держави виступає мілітаризація російської економіки та технологічна еволюція засобів збройної боротьби, зокрема масове застосування ударних безпілотних літальних апаратів. Цей виклик не може бути усунутий одномоментно, а тому потребує інституційної адаптації, зокрема нарощування спроможностей вітчизняного оборонно-промислового комплексу.

Зазначений виклик генерує конкретний ризик – ураження об’єктів енергетичної інфраструктури. Оцінимо його за формулою (1), використовуючи стандартну п’ятибальну матрицю. Напередодні осінньо-зимового періоду аналітичні підрозділи визначають ймовірність відновлення масованих атак як високу (4 бали), а масштаб можливих наслідків – як критичний для життєзабезпечення суспільства (5 балів). Відповідно, індекс ризику становить

$$R = 4 \times 5 = 20 \qquad (3)$$

(із максимально можливих 25), що переводить його до критичної “червоної зони”. На основі цього кількісного показника ухвалюється управлінське рішення щодо пріоритетного фінансування інженерного захисту енергооб’єктів з метою штучного зниження їхньої вразливості, тобто зменшення параметра I_m.

Отриманий числовий показник ризику дозволяє не лише визначити його критичність, а й інтегрувати оцінку у стандартизовану систему ранжування, що використовується в міжнародній практиці ризик-менеджменту. Для цього доцільно застосувати матрицю оцінювання ризиків (5×5), яка поєднує ймовірність настання події та масштаб її наслідків у єдиному індикаторі. Використання такої матриці забезпечує уніфікований підхід до класифікації

ризиків, спрощує порівняння різних сценаріїв та створює об’єктивну основу для ухвалення управлінських рішень. Структуру матриці наведено в табл. 2.

Таблиця 2. Матриця оцінювання ризиків (5×5)

Ймовірність (P)	1 – Дуже низька	2 – Низька	3 – Середня	4 – Висока	5 – Дуже висока
5 – Катастрофічні наслідки	5	10	15	20	25
4 – Значні наслідки	4	8	12	16	20
3 – Помірні наслідки	3	6	9	12	15
2 – Незначні наслідки	2	4	6	8	10
1 Мінімальні наслідки	1	2	3	4	5

Для демонстрації механізму ідентифікації загроз розглянемо сценарій розгортання противником стратегічної авіації (наприклад, бомбардувальників Ту-95МС). Застосуємо залежність (2), де спроможність (C) оцінюється базовим числом від 0 до 10 (еквівалент кількості боєготових бортів), а намір (I) – як імовірнісний коефіцієнт від 0 до 1. Дані розвідки фіксують наявність 10 боєготових літаків ($C = 10$), при цьому аналіз перехоплених документів противника свідчить про високий намір противника здійснити пуски ($I = 0{,}9$). Початковий рівень загрози становить

$$T = 10 \times 0{,}9 = 9{,}0\,, \tag{4}$$

що відповідає критичному рівню.

У разі успішних превентивних дій українських сил (наприклад, ураження аеродрому базування ударними БПЛА), внаслідок яких 4 літаки знищено або виведено з ладу, спроможність противника зменшується до $C = 6$. За незмінного наміру ($I = 0{,}9$) оновлений індекс загрози дорівнюватиме

$$T = 6 \times 0{,}9 = 5{,}4\,. \tag{5}$$

Таким чином, загроза знижується приблизно на 40 % виключно за рахунок деградації спроможностей противника (рис. 1).

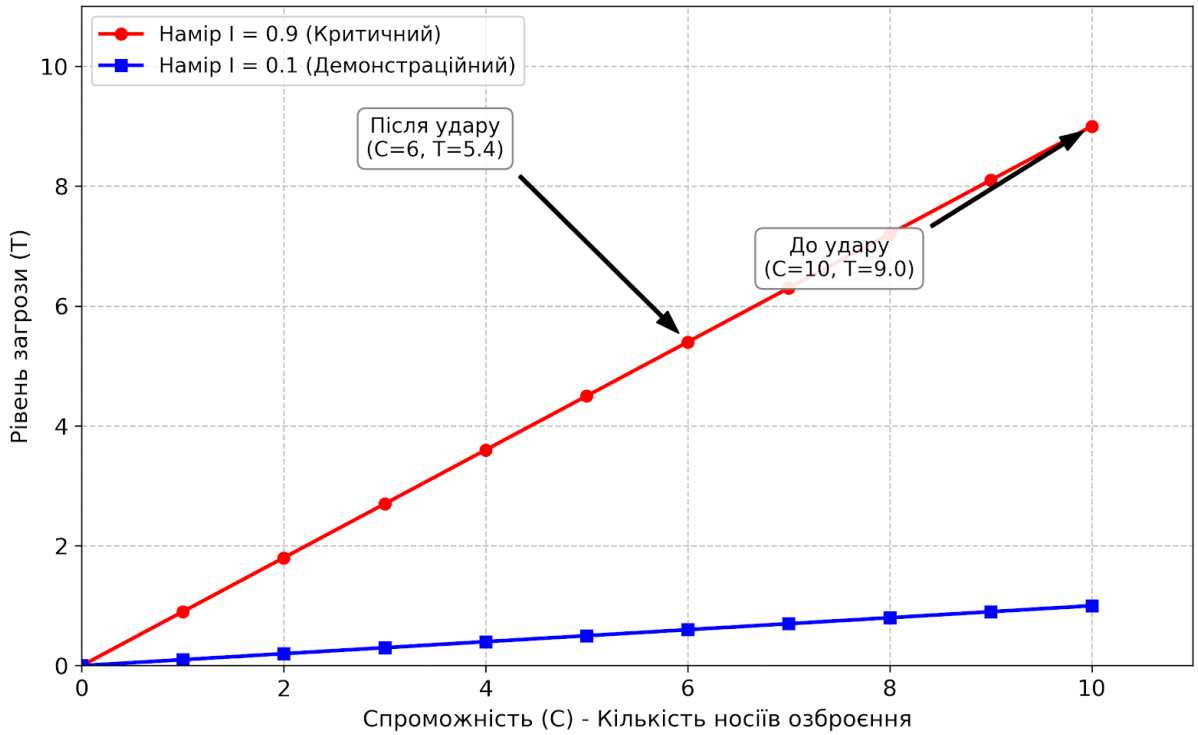

Рис. 1. Динаміка індексу загрози (T) залежно від спроможностей (C)

Отримані числові значення дозволяють не лише визначити рівень загрози у конкретному сценарії, а й інтегрувати ці оцінки у стандартизовану систему аналізу, що використовується в оборонному плануванні країн-членів НАТО. Для цього застосовується матриця оцінювання загроз, яка поєднує два ключові параметри – спроможність актора (C) та його намір (I). Така матриця забезпечує уніфікований підхід до класифікації загроз, дозволяє порівнювати різні сценарії та формує об’єктивну основу для ухвалення рішень щодо пріоритетного розподілу сил і засобів. Структуру цієї матриці наведено в табл. 3.

Таблиця 3. Матриця оцінювання загроз за спроможністю (*C*) та наміром (*I*)

Спроможність (C)	Намір (I = 0,1)	0,3	0,5	0,7	0,9
2	0,2	0,6	1,0	1,4	1,8
4	0,4	1,2	2,0	2,8	3,6
6	0,6	1,8	3,0	4,2	5,4
8	0,8	2,4	4,0	5,6	7,2
10	1,0	3,0	5,0	7,0	9,0

Математична динаміка цього процесу (рис. 1) демонструє, що за умов стабільно високого наміру противника єдиним ефективним шляхом зниження інтегрального індексу загрози (*T*) є фізичне або інформаційне зменшення його спроможностей (*C*). Така квантифікація забезпечує вище військово-політичне керівництво об'єктивним, математично верифікованим обґрунтуванням для перерозподілу дефіцитних засобів ураження та систем протиповітряної оборони на пріоритетні напрямки, мінімізуючи суб'єктивізм у процесі ухвалення управлінських рішень.

Рисунок відображає зміну інтегрального індексу загрози T за умови фіксованого високого наміру актора ($I = 0{,}9$) та варіативності його спроможностей (*C*) у діапазоні від 0 до 10. Графік (рис. 1) демонструє лінійну залежність між параметрами: зі зростанням спроможностей противника значення індексу загрози пропорційно збільшується, досягаючи критичних рівнів за високих значень *C*. Водночас зменшення спроможностей – унаслідок їх фізичної деградації, ураження або виведення з ладу – призводить до пропорційного зниження загрози, навіть за незмінно високого наміру. Це підтверджує, що у воєнних сценаріях ключовим механізмом зниження загрози є вплив саме на спроможності актора, тоді як намір залишається відносно стабільним і менш піддатливим до прямого управлінського впливу.

Розглянемо інший, воєнно-політичний вимір застосування запропонованої методології на стратегічному рівні державного управління. У цій площині макрорегіональним викликом виступає поглиблення військово-технічного співробітництва між авторитарними режимами та поступова ерозія

глобальних режимів нерозповсюдження озброєнь. Зазначений процес є об'єктивною реальністю, на яку держава не може вплинути виключно силовими інструментами. Відповідно, реакція державного апарату полягає в інституційній адаптації – розбудові власних союзницьких форматів, посиленні дипломатичного корпусу та активізації зовнішньополітичної діяльності.

Цей глобальний виклик породжує конкретний воєнно-політичний ризик – імовірність того, що технологічний обмін між державами-партнерами агресора дозволить йому масштабувати виробництво озброєнь. Оцінюючи цей ризик за формулою (1), розвідувальні органи можуть визначати ймовірність технологічного прориву (P) на рівні 3 балів (із 5), тоді як масштаб можливих наслідків (I_m) – як надзвичайно важкий (5 балів). Отриманий індекс ризику (R = 15) вимагає управлінського реагування шляхом застосування політико-економічних інструментів: ініціювання нових пакетів санкцій, дипломатичного тиску та координації з країнами-партнерами з метою зниження ймовірності (P) реалізації такого сценарію.

Безпосередньою загрозою у цьому контексті стає зафіксоване рішення третьої країни – союзника агресора – передати партію балістичних ракет для їх застосування проти України. Для оцінювання рівня загрози знову застосовується математична модель (2).

Нехай спроможність (C) визначається фізичною кількістю підготовлених до передачі пускових установок та ракетного озброєння, оціненою розвідкою на високому рівні (C = 8). Намір (I) інтерпретується як політична згода керівництва цієї країни на передачу озброєння і становить (I = 0,9). Початковий рівень загрози дорівнює (T = 7,2), що відповідає критичному значенню.

У разі якщо шляхом жорсткого дипломатичного тиску, консолідованої позиції міжнародної спільноти або застосування вторинних санкцій вдається змусити країну-донора відмовитися від передачі озброєння, її намір фактично знижується до нуля (I = 0). Відповідно до математичної моделі, рівень

безпосередньої загрози також нівелюється (T = 0). Математичну динаміку цього процесу відображено на рис. 2.

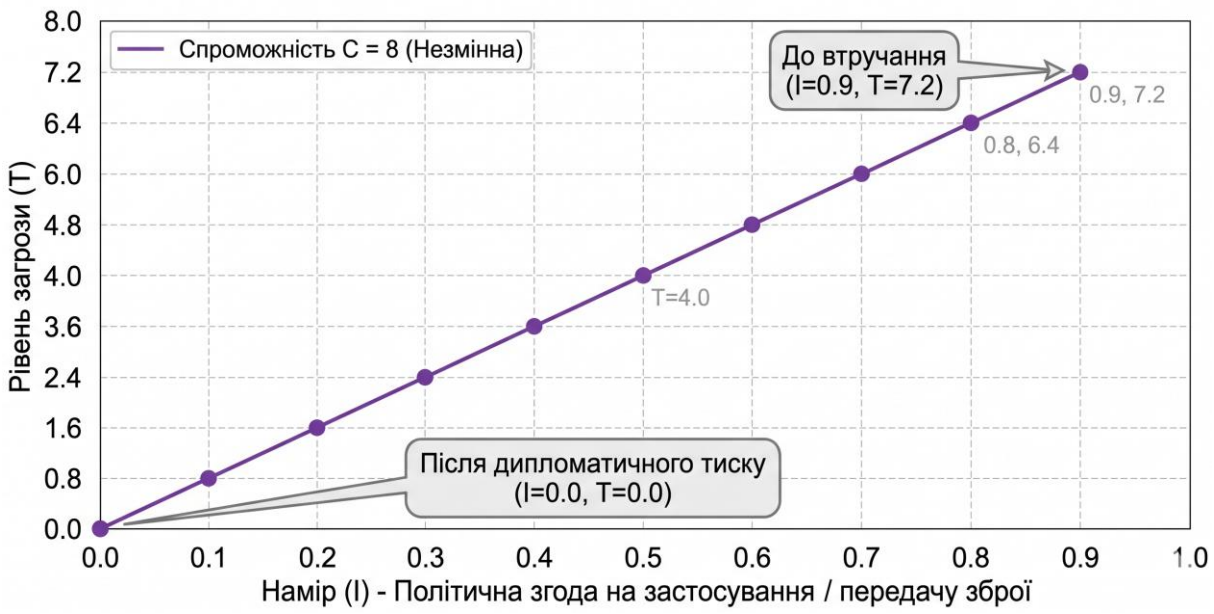

Рис. 2. Динаміка індексу загрози (T) залежно від намірів (I) при незмінній спроможності (C)

Рисунок відображає зміну інтегрального індексу загрози T за умови фіксованої спроможності актора (C = 8) та варіативності його намірів (I) у діапазоні від 0 до 1. Графік демонструє лінійну залежність між параметрами: зі зростанням наміру політичного керівництва третьої країни передати озброєння значення індексу загрози пропорційно збільшується, досягаючи критичних рівнів за високих значень I. Водночас повне нівелювання наміру (I = 0) призводить до математичного обнулення загрози (T = 0), навіть за збереження незмінно високої спроможності (C = 8).

Це підтверджує, що у воєнно-політичних сценаріях ключовим механізмом зниження загрози є вплив саме на наміри актора, а не на його матеріальні можливості.

Прикладне значення та управлінські імплікації запропонованої ескалаційної моделі. Запропонована ескалаційна модель розмежування категорій “виклик”, “ризик” і “загроза” формує цілісну аналітичну рамку, яка

дозволяє інтегрувати різнорідні елементи безпекового середовища у єдину систему оцінювання. Її застосування забезпечує можливість переходу від фрагментарних описових характеристик до кількісно верифікованих параметрів, що істотно підвищує точність ситуаційної обізнаності та обґрунтованість управлінських рішень. У практичній площині це створює умови для стандартизації процедур аналізу, уніфікації міжвідомчих підходів та підвищення сумісності з методологіями НАТО, зокрема у частині оцінювання намірів і спроможностей потенційних противників.

Використання моделі дозволяє державним органам чітко розмежовувати сфери відповідальності та відповідні механізми реагування: **виклики** потребують інституційної адаптації та стратегічного планування; **ризики** – превентивного управління, спрямованого на зниження ймовірності або масштабів наслідків; **загрози** – негайного застосування сил і засобів, оскільки вони містять активний деструктивний намір. Така диференціація мінімізує управлінські помилки, пов’язані з хибною класифікацією подій, та дозволяє оптимізувати розподіл ресурсів у режимі обмеженого часу.

Крім того, модель створює підґрунтя для формування адаптивних сценаріїв реагування, у яких зміна одного параметра (наприклад, спроможності противника) може бути оперативно врахована в оновлених розрахунках рівня загрози. Це підвищує гнучкість системи державного управління, дозволяє швидко коригувати пріоритети та забезпечує прозорість логіки ухвалення рішень. У сукупності такі можливості роблять модель не лише інструментом аналітичної підтримки, а й елементом інституційної модернізації процесів планування у секторі безпеки й оборони.

Висновки та перспективи подальших розвідок у даному напрямі. Проведене дослідження дозволило концептуально та математично обґрунтувати розмежування категорій “виклик”, “ризик” і “загроза” як ключових елементів оцінювання безпекового середовища та інформаційно-аналітичного забезпечення державного управління. Запропонована ескалаційна модель демонструє, що виклики мають об’єктивний характер і

потребують інституційної адаптації; ризики виникають унаслідок взаємодії викликів із вразливостями системи та піддаються превентивному управлінню; загрози ж пов’язані з наявністю активного деструктивного наміру та вимагають негайного реагування. Така диференціація забезпечує методологічну чіткість, усуває термінологічну ентропію та створює підґрунтя для уніфікації підходів до аналізу безпекових ситуацій.

Практична апробація моделі на прикладі оцінювання ризику ураження енергетичної інфраструктури та визначення рівня загрози від застосування стратегічної авіації противника підтвердила її операційну придатність. Використання кількісних індикаторів, матриць PESTLE, Risk Matrix та Threat Matrix дозволяє підвищити точність прогнозування, стандартизувати процедури аналізу та забезпечити сумісність з методологіями НАТО. Це створює можливість для об’єктивного ранжування подій, оптимізації розподілу ресурсів і формування прозорих управлінських рішень у режимі обмеженого часу.

Перспективи подальших наукових розвідок полягають у розширенні запропонованої моделі шляхом інтеграції додаткових параметрів, зокрема часової динаміки, індикаторів стійкості, поведінкових характеристик акторів та міждоменних залежностей. Доцільним є також розроблення адаптивних сценаріїв реагування, побудованих на автоматизованому оновленні параметрів ризику та загрози, а також створення цифрових інструментів моніторингу, що дозволять застосовувати модель у реальному часі. Окремим напрямом подальших досліджень має стати інтеграція соціогуманітарних, інформаційних та кібернетичних факторів у єдину аналітичну архітектуру, що сприятиме підвищенню стійкості держави до комплексних гібридних впливів.

Література

1. Горбулін В. П. Світова гібридна війна: український фронт : монографія. Київ : НІСД, 2017. 496 с.

2. Парахонський Б. О., Яворська Г. М. Онтологія війни і миру: безпека, стратегія, смисл : монографія. Київ : НІСД, 2019. 560 с.

3. Коломоєць Т. О., Колпаков В. К. Сучасна парадигма адміністративного права: ґенеза і поняття. Право України. 2017. № 5. С. 71–79.

4. Керування ризиками. Настанови (ISO 31000:2018, IDT) : ДСТУ ISO 31000:2018. [Чинний від 2018-11-01]. Київ : Держспоживстандарт України, 2018. 24 с.

5. AAP-06. Глосарій термінів та визначень НАТО. Brussels : NATO Standardization Office, 2020. 254 с.

6. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. Відомості Верховної Ради України. 2018. № 31. Ст. 241.

7. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14.09.2020 р. № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037 (дата звернення: 16.04.2026).

8. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України» : Указ Президента України від 25.03.2021 р. № 121/2021. URL: https://www.president.gov.ua/documents/1212021-37573 (дата звернення: 16.04.2026).

9. Guide to Capability-Based Planning (TR-SAS-081). Brussels : NATO Science and Technology Organization, 2014. 144 p.

References

1. Horbulin, V.P. (2017), *Svitova hibrydna viina: ukrainskyi front* [World hybrid war: Ukrainian front], NISD, Kyiv, Ukraine.

2. Parakhonskyi, B.O. and Yavorska, H.M. (2019), *Ontolohiia viiny i myru: bezpeka, stratehiia, smysl* [Ontology of war and peace: security, strategy, meaning], NISD, Kyiv, Ukraine.

3. Kolomoets, T. and Kolpakov, V. (2017), “Modern paradigm of administrative law: genesis and concept”, *Pravo Ukrainy*, vol. 5, pp. 71–79.

4. State Statistics Service of Ukraine (2018), DSTU ISO 31000:2018. *Keruvannia ryzykamy. Nastanovy* [ISO 31000:2018. Risk management – Guidelines], Derzhspozhyvstandart Ukrainy, Kyiv, Ukraine.

5. NATO Standardization Office (2020), “*AAP-06. NATO Glossary of Terms and Definitions*”, Brussels, Belgium.

6. The Verkhovna Rada of Ukraine (2018), The Law of Ukraine “On National Security of Ukraine”, available at: https://zakon.rada.gov.ua/laws/show/2469-19 (Accessed 16 April 2026).

7. President of Ukraine (2020), Decree “On the decision of the National Security and Defense Council of Ukraine dated September 14, 2020 “On the National Security Strategy of Ukraine””, available at: https://www.president.gov.ua/documents/3922020-35037 (Accessed 16 April 2026).

8. President of Ukraine (2021), Decree “On the decision of the National Security and Defense Council of Ukraine dated March 25, 2021 “On the Military Security Strategy of Ukraine””, available at: https://www.president.gov.ua/documents/1212021-37573 (Accessed 16 April 2026).

9. NATO Science and Technology Organization (2014), “*Guide to Capability-Based Planning (TR-SAS-081)*”, Brussels, Belgium.

Отримано редакцією журналу / Received: 15.04.26
Прорецензовано / Revised: 20.04.26
Схвалено до друку / Accepted: 23.04.26