Методичний підхід до пріоритезації когнітивних загроз та оцінки їх впливу для підвищення стійкості інформаційного простору Збройних Сил України

Methodological Approach to Prioritizing Cognitive Threats and Assessing Their Impact to Enhance the Resilience of the Information Space of the Armed Forces of Ukraine

Олег Темний
ад'юнкт кафедри інформаційної боротьби інституту стратегічних комунікацій, e-mail: o.temnyi@edu.nuou.org.ua, ORCID ID: https://orcid.org/0009-0009-3173-094X

Oleh Temnyi
Doctoral Candidate of the Department of Information Warfare, Institute of Strategic Communications, e-mail: o.temnyi@edu.nuou.org.ua, ORCID ID: https://orcid.org/0009-0009-3173-094X

Національний університет оборони України, Київ, Україна

National Defence University of Ukraine, Kyiv, Ukraine

Received: February 22, 2026 | Revised: February 27, 2026 | Accepted: February 28, 2026

UDC 355.40:316.77:519.83

DOI: https://doi.org/10.33445/sds.2026.16.1.34

Мета роботи. Розроблення та наукове обґрунтування методики пріоритезації та оцінювання впливу когнітивних загроз на ефективність системи стратегічних комунікацій Збройних Сил України на основі інтеграції теоретико-ігрового підходу, положень теорії ймовірностей, методу адитивної згортки та методу аналізу ієрархій.

Метод дослідження. Сукупність математичних і аналітичних методів, зокрема теоретико-ігрове моделювання когнітивного протиборства, інструментарій теорії ймовірностей для оцінювання невизначеності та ризиків, метод адитивної згортки для інтегральної оцінки багатокритеріальних показників, а також метод аналізу ієрархій для визначення ваг критеріїв і ранжування когнітивних загроз.

Практична цінність дослідження, Можливості використання запропонованої методики для формалізованого визначення пріоритетності когнітивних загроз, підвищення обґрунтованості управлінських рішень у сфері стратегічних комунікацій, оптимізації розподілу ресурсів інформаційної протидії та підвищення стійкості інформаційного простору Збройних Сил України.

Майбутні дослідження. Удосконалення моделей оцінювання когнітивних загроз шляхом застосування нечітких багатокритеріальних методів (Fuzzy AHP), розробленням динамічних стохастичних моделей інформаційного протиборства та створенням програмного інструментарію підтримки прийняття рішень у системі стратегічних комунікацій.

Тип статті. Теоретично-методологічний.

Purpose: development and scientific substantiation of a methodology for prioritizing and assessing the impact of cognitive threats on the effectiveness of the strategic communications system of the Armed Forces of Ukraine based on the integration of a game-theoretic approach, the provisions of probability theory, the additive convolution method, and the method of hierarchy analysis.

Method. A set of mathematical and analytical methods, including game-theoretic modelling of cognitive confrontation, probabilistic methods for assessing uncertainty and risks, the additive aggregation method for the integral evaluation of multicriteria indicators, and the Analytic Hierarchy Process (AHP) for determining criterion weights and ranking cognitive threats.

Practical implications. lies in the possibility of using the proposed methodology for formalized prioritization of cognitive threats, increasing the validity of management decisions in the field of strategic communications, optimizing the allocation of information countermeasure resources, and increasing the stability of the information space of the Armed Forces of Ukraine.

Future research. Improving models for assessing cognitive threats through the application of fuzzy multi-criteria decision-making methods (Fuzzy AHP), the development of dynamic stochastic models of information confrontation, and the creation of decision support software tools for strategic communications.

Paper type: Theoretical, practical.

Ключові слова: когнітивні загрози, стратегічні комунікації, інформаційне протиборство, метод аналізу ієрархій, теорія ймовірностей, теорія ігор, адитивна згортка, багатокритеріальне оцінювання, пріоритезація загроз, інформаційна безпека, російсько-українська війна, підтримка прийняття рішень, стратегічні комунікації Збройних Сил України.

Key words: Cognitive Threats, Strategic Communications, Information Confrontation, Method of Hierarchy Analysis, Probability Theory, Game Theory, Additive Convolution, Multi-Criteria Assessment, Threat Prioritization, Information Security, Russian-Ukrainian War, Decision Support, Strategic Communications of the Armed Forces of Ukraine.

Вступ

У контексті триваючої російсько-української війни інформаційно-психологічний фронт став не менш важливим за традиційні бойові операції. Спрямована когнітивна війна, що ведеться агресором, включає систематичне використання дезінформації, маніпуляцій суспільною

думкою, фейків, інформаційних вкидів та психо-підривних наративів, які мають на меті підірвати моральний дух військовослужбовців, посіяти недовіру до державних інститутів та знизити ефективність системи стратегічних комунікацій Збройних Сил України (ЗСУ). Вплив таких когнітивних загроз не обмежується суто інформаційною сферою, бо він безпосередньо позначається на здатності ЗСУ формувати правильне сприйняття цілей і дій оборонних і оперативних органів, підтримувати внутрішню єдність та підсилювати міжнародну підтримку України [1–4].

Сучасні теоретико-методологічні підходи [1–20] ще недостатньо адаптовані до вимірювання та порівняння рівнів впливу когнітивних загроз у реальних умовах широкомасштабної агресії. Існуючі системи оцінювання інформаційних ризиків та стратегічних комунікацій часто мають фрагментарний характер, і не забезпечують комплексної, структурованої оцінки пріоритетності загроз з урахуванням їхнього потенційного впливу на функціонування критичних військових комунікаційних ланцюгів.

Водночас ефективність стратегічних комунікацій як складового елементу оборонної спроможності безпосередньо впливає на здатність ЗСУ протидіяти не лише фізичній, але і ціннісно-когнітивній агресії. Відсутність адекватної методики для ідентифікації, ранжування та кількісної оцінки когнітивних загроз ускладнює прийняття управлінських рішень, оперативне реагування на виклики інформаційного простору та розвиток превентивних заходів.

Отже, розроблення методики пріоритезації та оцінювання впливу когнітивних загроз на ефективність системи стратегічних комунікацій ЗСУ є надзвичайно актуальним, оскільки сприятиме: підвищенню адаптивності та стійкості стратегічних комунікацій до інформаційних атак; формуванню принципів і механізмів вимірювання та ранжування загроз відповідно до їхнього потенційного впливу; оптимізації ресурсів інформаційної протидії в умовах високої динаміки інформаційного середовища; зміцненню ефективності комунікаційних стратегій у підтриманні морально-психологічного стану військ та суспільства. Результати такого дослідження мають практичну значущість для підвищення обороноздатності України та забезпечення інформаційної безпеки в умовах сучасної гібридної війни.

Огляд літератури

Аналіз теоретичних і практичних досліджень у сфері пріоритезації та оцінювання когнітивних загроз засвідчує [1–20], що формування науково обґрунтованої методики потребує інтеграції кількох взаємодоповнюючих математичних підходів: теоретико-ігрового моделювання, теорії ймовірностей, методу адитивної згортки та методу аналізу ієрархій тощо. Кожен із цих інструментів має власну методологічну нішу, а їх поєднання дозволяє перейти від абстрактного опису когнітивного протиборства до формалізованої процедури визначення пріоритетів загроз у системі стратегічних комунікацій.

Теоретико-ігровий підхід сформувався як інструмент моделювання стратегічної взаємодії раціональних агентів у конфліктних ситуаціях і традиційно застосовується для аналізу військово-політичного протистояння [9, 10]. У контексті когнітивної боротьби він дозволяє розглядати інформаційних акторів як гравців, що реалізують стратегії впливу, протидії, маскування або ескалації інформаційного тиску. В межах цього підходу когнітивна загроза інтерпретується як елемент стратегічної гри з неповною інформацією, де сторони приймають рішення в умовах невизначеності щодо намірів та ресурсів опонента. Практичні дослідження вказують на доцільність застосування моделей ігор з нульовою та ненульовою сумою, стохастичних ігор та моделей з неповною інформацією для опису динаміки інформаційного впливу. Водночас класичні моделі раціонального вибору потребують адаптації до особливостей когнітивного середовища, де значну роль відіграють психологічні ефекти, асиметрія сприйняття та обмежена раціональність суб’єктів.

Теорія ймовірностей забезпечує кількісне підґрунтя для оцінювання невизначеності,

притаманної когнітивним загрозам [12–14]. У дослідженнях інформаційної безпеки ймовірнісні підходи застосовуються для визначення частоти виникнення інформаційних атак, оцінки масштабу їхнього поширення та прогнозування можливих наслідків для морально-психологічного стану або довіри до інституцій. Особливе значення мають байєсівські моделі, які дозволяють оновлювати оцінки загроз у міру надходження нових даних, що є критично важливим в умовах динамічного інформаційного середовища. Практичні реалізації ймовірнісних підходів демонструють ефективність у системах моніторингу медіапростору та оцінювання ризиків, однак вони не вирішують проблеми ранжування загроз за рівнем критичності без залучення додаткових багатокритеріальних процедур.

Метод адитивної згортки є одним із базових інструментів агрегування множини критеріїв у єдиний інтегральний показник [13–18]. Його аксіоматика передбачає незалежність критеріїв та лінійність їхнього внеску до загальної оцінки. У практиці оцінювання загроз цей метод застосовується для формування індексів, що поєднують різнорідні показники: інтенсивність інформаційного впливу, рівень охоплення аудиторії, потенційний соціально-політичний ефект, стійкість цільової групи тощо. Перевагою адитивної згортки є її прозорість і простота реалізації, що дозволяє створювати формалізовані інструменти швидкої оцінки. Водночас її використання обмежується припущенням про незалежність критеріїв, тоді як у реальному когнітивному середовищі вони часто взаємопов’язані. Тому ефективність цього методу значною мірою залежить від коректного визначення вагових коефіцієнтів та попереднього аналізу кореляцій між показниками.

Метод аналізу ієрархій (MAI/AHP) розглядається як один із найбільш розвинених багатокритерійних підходів до прийняття рішень [12–18]. Він дозволяє структурувати складну проблему у вигляді ієрархії, від стратегічної мети до конкретних критеріїв і альтернатив. На основі парних порівнянь критеріїв формується матриця пріоритетів, з якої обчислюються вагові коефіцієнти через власні вектори, а також визначається показник узгодженості експертних оцінок. Практичні дослідження у військовій та інформаційній безпеці підтверджують ефективність MAI для визначення пріоритетності загроз, розподілу ресурсів та оцінювання стратегічних альтернатив. Перевагою методу є можливість інтегрувати експертні знання у формалізовану процедуру та забезпечити прозорість процесу прийняття рішень. Разом із тим MAI є чутливим до суб’єктивності оцінок і потребує ретельної перевірки узгодженості суджень, особливо в умовах високої невизначеності.

Загалом аналіз наукових джерел і практичних підходів свідчить [1–20], що ізольоване застосування кожного з розглянутих методів не забезпечує повноцінної методики пріоритезації когнітивних загроз. Теоретико-ігровий підхід надає стратегічну рамку для моделювання протиборства, теорія ймовірностей – кількісну оцінку невизначеності, адитивна згортка – механізм інтеграції показників, а MAI – структурований спосіб визначення ваг і ранжування альтернатив. Їх інтеграція в єдину методичну систему дозволяє сформувати багаторівневий інструментарій оцінювання, що поєднує стратегічний аналіз, статистичну обробку даних та експертне знання. Такий підхід створює науково обґрунтовану основу для пріоритезації когнітивних загроз і підвищує об’єктивність управлінських рішень у сфері стратегічних комунікацій в умовах сучасного інформаційного протиборства.

Результати

Методика пріоритезації та оцінювання впливу когнітивних загроз на ефективність системи стратегічних комунікацій Збройних Сил України (далі – Методика) призначена для формалізованого аналізу, систематичного ранжування та кількісного оцінювання деструктивного впливу когнітивних загроз різного типу на функціонування системи стратегічних комунікацій (далі – ССК) ЗС України.

Методика забезпечує науково обґрунтований інструментарій для підтримки прийняття

управлінських рішень щодо протидії когнітивним загрозам в інформаційному просторі на стратегічному та оперативному рівнях управління. Застосування методики дозволяє перейти від якісних експертних оцінок до кількісних показників, що підвищує об'єктивність та відтворюваність результатів аналізу.

Методика може застосовуватися як самостійний аналітичний інструмент, так і як складова частина системи комплексного оцінювання інформаційної безпеки ЗС України. Вона орієнтована на використання фахівцями підрозділів стратегічних комунікацій, аналітичних підрозділів розвідки (J2), підрозділів інформаційних операцій, а також науково-дослідних установ Міністерства оборони України.

Основна мета методики – забезпечити кількісну основу для визначення пріоритетів протидії когнітивним загрозам та оцінювання їх сукупного впливу на ключові показники ефективності ССК ЗС України в умовах інформаційного протиборства.

Досягнення мети передбачає розв'язання двох взаємопов'язаних задач:

по-перше, визначення того, які саме когнітивні загрози є найбільш небезпечними для ССК (задача пріоритезації);

по-друге, кількісне оцінювання того, наскільки ці загрози знижують ефективність ССК за різними показниками (задача оцінювання впливу).

Поєднання цих двох задач забезпечує цілісне уявлення про стан когнітивної безпеки ССК та дозволяє обґрунтовано розподіляти обмежені ресурси протидії.

Методика розв'язує такі основні завдання:

1) ідентифікація та класифікація когнітивних загроз системі стратегічних комунікацій ЗС України за типами, джерелами та механізмами впливу;

2) формалізація процесу пріоритезації когнітивних загроз на основі теоретико-ігрового підходу, що моделює конфліктну взаємодію між раціональним противником та системою протидії ССК;

3) кількісне оцінювання впливу кожного типу когнітивних загроз на кожний ключовий показник ефективності ССК з урахуванням ймовірностей реалізації загроз та ефективності наявних засобів протидії;

4) формування інтегрального показника впливу когнітивних загроз на ефективність ССК із застосуванням адитивної згортки з науково обґрунтованими вагами;

5) визначення критичних порогових значень та умов переходу системи у стан зниженої або критичної ефективності;

6) проведення аналізу чутливості результатів до зміни вхідних параметрів для оцінки робастності висновків;

7) обґрунтування рекомендацій щодо пріоритетних напрямів посилення протидії когнітивним загрозам та раціонального розподілу ресурсів.

У методиці розглядаються три основних типи когнітивних загроз, що становлять найбільшу небезпеку для ССК ЗС України у 2024–2026 рр.:

T_1 – дезінформаційні кампанії (ІПСО, наративи рф). Організований, системний вплив на інформаційний простір з метою формування хибних уявлень про стан справ, дискредитації командування ЗС України, підриву довіри до офіційних джерел інформації. Включає координовані операції впливу через традиційні ЗМІ, телеграм-канали, закриті месенджери. Характеризується високим рівнем організованості, довгостроковою стратегією, значними ресурсами противника та глибоким розумінням культурного контексту цільових аудиторій.

T_2 – Deepfake та AI-генерований контент. Створення та поширення фальсифікованого аудіо-, відео- та текстового контенту з використанням технологій штучного інтелекту (генеративних змагальних мереж, великих мовних моделей). Загроза характеризується стрімким зростанням якості фальсифікатів, зниженням порогу входу для створення deepfake-контенту, складністю виявлення та спростування, а також високим емоційним впливом на

аудиторію.

T_3 – маніпуляції в соціальних мережах (боти, тролі). Систематичне використання автоматизованих облікових записів (ботів), координованих мереж тролів та астротурфінгу для штучного формування суспільної думки, посилення поляризації, поширення панічних настроїв. Включає маніпуляції з алгоритмами рекомендацій, створення штучних трендів, координовані атаки на офіційні акаунти ЗС України та провокування конфліктів між різними групами аудиторії.

Розглянемо ключові показники ефективності (KPI) ССК. Ефективність ССК ЗС України оцінюється за чотирма ключовими показниками:

E_1 – рівень довіри цільових аудиторій. Відображає ступінь довіри населення, особового складу ЗС України, міжнародної спільноти та інших цільових аудиторій до офіційної комунікації ЗС України. Вимірюється через соціологічні дослідження, аналіз залученості в офіційних каналах комунікації, моніторинг медіапростору. Є фундаментальним показником, оскільки від рівня довіри залежить ефективність усіх інших комунікаційних зусиль.

E_2 – наративне домінування в інформаційному просторі. Характеризує здатність ССК формувати та підтримувати домінуючі наративи в інформаційному просторі, визначати порядок денний дискусії. Оцінюється через частку проукраїнських наративів у медіапросторі, швидкість поширення офіційних повідомлень порівняно з дезінформацією, рівень цитування офіційних джерел.

E_3 – швидкість реагування на інформаційні загрози. Відображає здатність ССК оперативно виявляти, аналізувати та протидіяти інформаційним загрозам. Вимірюється середнім часом від виявлення загрози до публікації офіційної реакції, часткою загроз, на які було надано своєчасну відповідь, ефективністю систем раннього попередження.

E_4 – стійкість системи до когнітивного впливу противника. Інтегральна характеристика здатності ССК зберігати функціональність та ефективність в умовах масованого когнітивного впливу. Включає технічну стійкість (захищеність інфраструктури), організаційну стійкість (наявність резервних каналів, процедур кризового реагування), когнітивну стійкість (медіаграмотність цільових аудиторій).

До основних припущень та обмежень можна віднести те, що Методика базується на таких припущеннях:

1) противник діє раціонально, обираючи стратегії когнітивного впливу, що максимізують шкоду ССК (припущення раціональності гравця у теоретико-ігровій моделі);

2) типи когнітивних загроз є достатньо розрізненими для окремого аналізу, хоча на практиці вони можуть реалізовуватися одночасно (припущення незалежності загроз);

3) експертні оцінки, що використовуються як вхідні дані, є результатом колективного аналізу кваліфікованих фахівців і відображають узгоджену позицію експертної групи;

4) ключові показники ефективності ССК є адитивно незалежними, що дозволяє застосовувати адитивну згортку;

5) характер когнітивних загроз може суттєво змінюватися з часом, тому методика потребує регулярного оновлення вхідних даних.

Обмеження методики:

не враховується синергетичний ефект одночасної реалізації кількох типів загроз (ефект мультиплікації);

якість результатів залежить від якості експертних оцінок вхідних параметрів;

модель не враховує динаміку зміни стратегій противника в реальному часі (статична модель з дискретним оновленням).

Методика має дворівневу архітектуру, що відображає логіку аналізу когнітивних загроз: спочатку визначається, які загрози є найнебезпечнішими (пріоритезація), а потім оцінюється, наскільки ці загрози знижують ефективність ССК (оцінювання впливу). Результати першого

рівня (ваги пріоритетності) безпосередньо використовуються як вхідні дані другого рівня, що забезпечує системну цілісність методики.

Здійснено опис основних етапів та їх взаємозв'язок.

Часткова методика I (4 етапи):

Етап 1.1. Формування платіжної матриці – побудова моделі конфліктної взаємодії "противник – ССК".

Етап 1.2. Аналіз матричної гри за критеріями оптимальності – визначення оптимальних стратегій за Вальдом, Гурвіцем, Севіджем.

Етап 1.3. Розв'язок ЗЛП для змішаних стратегій – пошук оптимального розподілу ймовірностей стратегій противника.

Етап 1.4. Визначення ваг пріоритетності загроз – формування нормалізованого вектора ваг w_i^T (вага пріоритетності і-ї когнітивної загрози).

Таблиця 1: Архітектура Методики

Рівень	Часткова методика	Математичний апарат	Вхідні дані	Результат
I	Пріоритезація когнітивних загроз	Теорія ігор (матричні ігри, ЗЛП, критерії оптимальності)	Платіжна матриця (експертні оцінки шкоди)	Ваги пріоритетності загроз w_i^T
II	Оцінювання впливу когнітивних загроз	Теорія ймовірностей, MAI, адитивна згортка, аналіз чутливості	Ймовірності, матриця впливу, ваги з рівня I	Інтегральний показник I_{xek}, залишкова ефективність $E_{зал}$

Джерело: *розроблено автором.*

Часткова методика II (6 етапів):

Етап 2.1. Оцінювання ймовірностей реалізації загроз – визначення $P(T_i)$ з урахуванням протидії.

Етап 2.2. Визначення ваг KPI методом MAI – побудова матриці парних порівнянь, розрахунок w_j^E (вага значущості *j*-го KPI).

Етап 2.3. Оцінювання часткових показників впливу – формування матриці впливу, розрахунок I_{ij} (показник впливу когнітивних загроз).

Етап 2.4. Адитивна згортка – обчислення інтегральних показників I_i, I_{xek} (загальний інтегральний показник впливу когнітивних загроз), $E_{зал}$ (показник залишкової ефективності ССК).

Етап 2.5. Аналіз чутливості – дослідження впливу варіації параметрів на результат.

Етап 2.6. Порогові значення та зворотний зв'язок – класифікація стану ССК, ітеративне коригування.

Взаємозв'язок між частковими методиками реалізується через вектор ваг пріоритетності w_i^T, що передається з виходу Часткової методики I на вхід Етапу 2.4 Часткової методики II. Зворотний зв'язок реалізується через ітеративний цикл: якщо результат $E_{зал}$ не відповідає прийнятному рівню, коригуються коефіцієнти протидії η_i та повторюються Етапи 2.1–2.4.

Часткова методика I базується на математичному апараті теорії ігор та призначена для визначення ваг пріоритетності когнітивних загроз з урахуванням раціональної поведінки противника. Методика моделює когнітивне протиборство як антагоністичну матричну гру двох осіб з нульовою сумою.

4.1. Етап 1.1. Формування платіжної матриці

На цьому етапі будується формальна модель конфліктної взаємодії у вигляді платіжної матриці.

Гравці:

Гравець 1 (противник) – суб'єкт когнітивного впливу, що обирає тип когнітивної загрози для реалізації.

Гравець 2 (ССК) – система стратегічних комунікацій ЗС України, що обирає стратегію протидії.

Стратегії гравця 1 (типи загроз): T_1 – дезінформаційні кампанії (ІПСО, наративи рф); T_2 – Deepfake та AI-генерований контент; T_3 – маніпуляції в соціальних мережах (боти, тролі).

Стратегії гравця 2 (варіанти протидії ССК): S_1 – активна протидія: превентивні наративи, контрпропаганда, проактивне інформування цільових аудиторій, формування порядку денного; S_2 – реактивна протидія: оперативне спростування, факт-чекінг, швидке реагування на виявлені фейки та маніпуляції; S_3 – посилення стійкості: програми медіаграмотності, зміцнення довіри до офіційних джерел, розвиток резервних каналів комунікації; S_4 – комбінована протидія: поєднання активних інформаційних заходів із технічним захистом (детекція ботів, AI-верифікація контенту, блокування джерел дезінформації).

Платіжна матриця:

$$A = ||a_{ij}||,\ i = 1,\dots,m;\ j = 1,\dots,n;\ m = 3,\ n = 4$$

де a_{ij} – рівень шкоди ССК (в балах від 0 до 10) при реалізації загрози T_i за умови застосування стратегії протидії S_j.

Значення a_{ij} визначаються методом експертного оцінювання. Експертна група (не менше 5 фахівців) незалежно оцінює кожний елемент матриці. Підсумкове значення визначається як медіана експертних оцінок. Шкала: 0 – шкода відсутня, 1–3 – незначна шкода, 4–6 – помірна шкода, 7–8 – значна шкода, 9–10 – критична шкода.

4.2. Етап 1.2. Аналіз матричної гри за критеріями оптимальності

Застосування кількох критеріїв оптимальності забезпечує робастність результатів та дозволяє оцінити загрози з різних позицій.

4.2.1. Критерій Вальда (максимін)

Критерій Вальда визначає гарантований результат для кожної стратегії – найгірший можливий результат, на який може розраховувати гравець. Для противника це мінімальна шкода, яку він гарантовано завдасть ССК незалежно від обраної стратегії протидії:

$$\alpha_i = min_{j=1}^{\ n}\ a_{ij}, i = 1, \dots m$$

де α_i – гарантований мінімальний виграш (шкода ССК) при застосуванні загрози T_i.

Максимінна стратегія противника:

$$T^* = \arg max_i[\alpha_i]$$

$$V^- = max_i[\alpha_i] = min_i\left[min_j\left(a_{ij}\right)\right]$$

де V^- – нижня ціна гри;
T^* – оптимальна стратегія за критерієм Вальда.

Інтерпретація: загроза T^* є найнебезпечнішою в песимістичному сценарії – навіть за найкращої протидії ССК вона гарантовано завдає максимальну мінімальну шкоду.

4.2.2. Критерій мінімаксу

Для ССК (гравець 2) критерій мінімаксу визначає стратегію, що мінімізує найгірший можливий результат:

$$\beta_j = max_{j=1}^{m} a_{ij}, j = 1, \dots n$$

де β_j – максимальна шкода ССК при застосуванні стратегії протидії S_j

$$S^* = \arg\min_j [\beta_j]$$

$$V^+ = \min_j [\beta_j] = \min_j [\max_i (a_{ij})]$$

де V^+ – верхня ціна гри;
S^* – оптимальна стратегія протидії.

Перевірка наявності сідлової точки: якщо $V^- = V^+ = V$, то гра має розв'язок у чистих стратегіях з ціною гри V. Якщо $V^- < V^+$, необхідний перехід до змішаних стратегій (Етап 1.3).

4.2.3. Критерій Гурвіца

Компромісний критерій, що враховує як оптимістичний, так і песимістичний сценарії з параметром оптимізму λ ∈ [0, 1]:

$$H_i = \lambda \cdot \max_j(a_{ij}) + (1 - \lambda) \cdot \min_j(a_{ij}), \ i = 1, \dots, m$$

де H_i – оцінка i-ї стратегії (загрози) за критерієм Гурвіца;
λ – коефіцієнт оптимізму противника: λ = 1 відповідає абсолютному оптимізму (критерій максимаксу), λ = 0 – абсолютному песимізму (критерій Вальда);
$\max_j(a_{ij})$ – найкращий можливий результат при застосуванні загрози T_i;
$\min_j(a_{ij})$ – найгірший можливий результат при застосуванні загрози T_i.

Для моделювання агресивного противника (рф) рекомендується значення λ = 0.6, що відповідає помірно-оптимістичній поведінці з урахуванням досвіду та ресурсів противника.

4.2.4. Критерій Севіджа (мінімакс жалю)

Критерій мінімізує максимальний "жаль" – різницю між фактичним виграшем та найкращим можливим виграшем у даних умовах.

Крок 1. Побудова матриці ризиків (жалю) R = $||r_{ij}||$:

$$r_{ij} = \max_k(a_{kj}) - a_{ij}, \ i = 1,\dots,m; \ j = 1,\dots,n$$

де r_{ij} – величина жалю при обранні стратегії T_i, коли ССК застосовує стратегію S_j;
$\max_k(a_{kj})$ – максимальна шкода по j-му стовпцю.

Крок 2. Визначення максимального жалю для кожної загрози:

$$S_i = \max_j(r_{ij}), \ i = 1, \dots, m$$

Крок 3. Оптимальна стратегія за Севіджем:

$$T^* = \arg\min_i [S_i] = \arg\min_i [\max_j(r_{ij})]$$

Інтерпретація: загроза з найменшим максимальним жалем є найбільш "універсальною" – вона забезпечує стабільно високу шкоду незалежно від дій ССК.

4.3. Етап 1.3. Розв'язок ЗЛП для змішаних стратегій

Для визначення оптимальної змішаної стратегії противника задача формулюється як задача лінійного програмування (ЗЛП). Це центральний математичний етап Часткової методики І.

4.3.1. Формулювання ЗЛП

Противник шукає змішану стратегію $p = (p_1, p_2, p_3)$, що максимізує гарантований виграш: Максимізувати V за обмежень:

$$p_1 a_{11} + p_2 a_{21} + p_3 a_{31} \geq V \quad (\text{стратегія } S_1)$$
$$p_1 a_{12} + p_2 a_{22} + p_3 a_{32} \geq V \quad (\text{стратегія } S_2)$$
$$p_1 a_{13} + p_2 a_{23} + p_3 a_{33} \geq V \quad (\text{стратегія } S_3)$$
$$p_1 a_{14} + p_2 a_{24} + p_3 a_{34} \geq V \quad (\text{стратегія } S_4)$$
$$p_1 + p_2 + p_3 = 1$$
$$p_1, p_2, p_3 \geq 0, \ V - \text{не обмежено}$$

4.3.2. Зведення до стандартної форми ЗЛП

Виконується заміна змінних: $x_i = p_i / V$ (при V > 0, що забезпечується додаванням достатньо великої константи до всіх елементів матриці, якщо є від'ємні елементи). Задача набуває стандартної форми:

Мінімізувати $Z = x_1 + x_2 + x_3$

за обмежень:

$$a_{11}x_1 + a_{21}x_2 + a_{31}x_3 \geq 1$$
$$a_{12}x_1 + a_{22}x_2 + a_{32}x_3 \geq 1$$
$$a_{13}x_1 + a_{23}x_2 + a_{33}x_3 \geq 1$$
$$a_{14}x_1 + a_{24}x_2 + a_{34}x_3 \geq 1$$
$$x_1, x_2, x_3 \geq 0$$

4.3.3. Симплекс-метод розв'язку

Для розв'язку ЗЛП застосовується симплекс-метод Данціга. Алгоритм складається з таких кроків:

Крок 1. Введення додаткових змінних s_j для перетворення нерівностей у рівності:

$$a_{1j}x_1 + a_{2j}x_2 + a_{3j}x_3 - s_j = 1, \ s_j \geq 0, \ j = 1,\ldots,4$$

Крок 2. Формування початкової симплекс-таблиці з базисними та вільними змінними.

Крок 3. Вибір ведучого стовпця (змінна з найбільшим коефіцієнтом у цільовому рядку).

Крок 4. Вибір ведучого рядка (мінімальне відношення вільного члена до елемента ведучого стовпця серед додатних елементів).

Крок 5. Жорданові перетворення (виключення) для формування нового базису.

Крок 6. Повторення кроків 3–5 до досягнення оптимальності (всі коефіцієнти у цільовому рядку ≤ 0 для задачі мінімізації).

Після отримання оптимального розв'язку $x^* = (x_1^*, x_2^*, x_3^*)$ відновлюються оптимальні ймовірності змішаної стратегії:

$$V = 1 / Z^* = 1 / (x_1^* + x_2^* + x_3^*)$$

$$p_i^* = x_i^* / Z^* = x_i^* \cdot V, \ i = 1, 2, 3$$

де V – ціна гри у змішаних стратегіях.

Примітка: для гри розміром 3×4 можливе також застосування графічного методу або прямого розв'язку системи лінійних рівнянь для активних стратегій.

4.4. Етап 1.4. Визначення ваг пріоритетності загроз

Ваги пріоритетності когнітивних загроз формуються на основі синтезу результатів теоретико-ігрового аналізу. Застосовується комплексний підхід, що інтегрує оцінки за кількома критеріями:

Метод 1: На основі змішаних стратегій.

$$w_i^{T_i} = p_i^*$$

Ваги безпосередньо визначаються оптимальними ймовірностями змішаної стратегії противника.

Метод 2: Комплексний показник за критеріями.

Для підвищення робастності формується комплексний показник, що враховує результати всіх критеріїв:

$$K_i = \gamma_1 \cdot \tilde{\alpha}_i + \gamma_2 \cdot \tilde{H}_i + \gamma_3 \cdot \tilde{M}_i$$

де K_i – комплексний показник пріоритетності загрози T_i; $\tilde{\alpha}_i = \alpha_i / \sum\alpha_k$ – нормалізована оцінка за Вальдом;
$\tilde{H}_i = H_i / \sum H_k$ – нормалізована оцінка за Гурвіцем;
$\tilde{M}_i = M_i / \sum M_k$ – нормалізоване середнє значення шкоди ($M_i = (1/n)\sum_j a_{ij}$);
$\gamma_1, \gamma_2, \gamma_3$ – ваги критеріїв ($\gamma_1 + \gamma_2 + \gamma_3 = 1$);
$\gamma_1 = 0.4$, $\gamma_2 = 0.3$, $\gamma_3 = 0.3$. – рекомендовані значення.

Підсумкові ваги пріоритетності (нормалізація):

$$w_i^{T_i} = K_i / \sum_k K_k, \ \sum w_i^T = 1$$

Узгодження методів. Якщо обидва методи дають подібні результати (різниця ваг < 0.05), це підтверджує робастність оцінок. У разі суттєвих розбіжностей рекомендується переглянути вхідні дані платіжної матриці.

Часткова методика II базується на математичному апараті теорії ймовірностей та адитивної згортки. Вона використовує ваги пріоритетності загроз w_i^T, отримані в Частковій методиці 1, та формує інтегральний показник впливу когнітивних загроз на ефективність ССК.

5.1. Етап 2.1. Оцінювання ймовірностей реалізації загроз

Для кожної когнітивної загрози T_i визначається результуюча ймовірність її успішної реалізації з урахуванням потенціалу противника та наявних засобів протидії.

Формула результуючої ймовірності:

$$P(T_i) = P_o(T_i) \cdot (1 - \eta_i), \ i = 1, ..., m$$

де $P(T_i)$ – результуюча ймовірність успішної реалізації загрози T_i, $P(T_i) \in [0, 1]$;
$P_o(T_i)$ – базова ймовірність реалізації загрози T_i за відсутності протидії;
η_i – коефіцієнт ефективності протидії загрозі T_i, $\eta_i \in [0, 1]$.

Базова ймовірність $P_o(T_i)$ визначається експертним шляхом з урахуванням: ресурсного потенціалу противника (фінансові, технічні, людські ресурси), історичних даних (частота та успішність попередніх атак), технологічної готовності (наявність відповідних засобів та технологій), мотивації (інтенсивність інформаційного протиборства на поточному етапі).

Коефіцієнт ефективності протидії η_i характеризує здатність ССК нейтралізувати відповідний тип загрози та визначається з урахуванням: наявності спеціалізованих технічних засобів (детектори deepfake, системи моніторингу ботів), кваліфікації особового складу, розвиненості процедур реагування, рівня міжвідомчої координації.

5.2. Етап 2.2. Визначення ваг KPI методом аналізу ієрархій (MAI)

Для визначення ваг значущості ключових показників ефективності w_j^E застосовується метод аналізу ієрархій за алгоритмом, описаним у п. 2.4.

Крок 1. Побудова матриці парних порівнянь.

Експертна група проводить попарне порівняння КРІ за шкалою Сааті (1–9 балів). Формується квадратна матриця $C = ||C_{jk}||$ розміром 4×4:

$$C = || C_{jk} ||, \; c_{jj} = 1, \; c_{kj} = 1/c_{jk}$$

Елемент c_{jk} показує, у скільки разів КРІ E_j важливіший за КРІ E_k з точки зору забезпечення ефективності ССК.

Крок 2. Обчислення вектора пріоритетів.

Метод середнього геометричного по рядках:

$$g_j = (c_{j1} \cdot c_{j2} \cdot c_{j3} \cdot c_{j4})^{\wedge}(1/4), \; j = 1, ..., 4$$

Нормалізація:

$$w_j^E = g_j / (g_1 + g_2 + g_3 + g_4), \; \sum w_j^E = 1$$

Крок 3. Перевірка узгодженості.

Обчислення λ_max (максимальне власне число матриці С):

$$\lambda_max = (1/k) \cdot \sum_{j=1}^{k} [(C \cdot w_j / w_j]$$

де $(C \cdot w)_j$ – j-й елемент вектора-добутку матриці C на вектор ваг w.

$$IУ = (\lambda_\max - k) / (k - 1)$$

$$ВУ = IУ / BI, \; \text{для } k = 4: BI = 0{,}90$$

Критерій узгодженості: ВУ ≤ 0.10. Якщо ВУ > 0.10 – необхідний перегляд матриці парних порівнянь.

5.3. Етап 2.3. Оцінювання часткових показників впливу

Формується матриця впливу $D = ||d_{ij}||$, де d_{ij} – нормалізований показник деструктивного впливу загрози T_i на КПЕ E_j:

$$D = ||d_{ij}||, \; d_{ij} \in [0, 1], \; i = 1,...,m; \; j = 1,...,k$$

де $d_{ij} = 0$ – означає відсутність впливу, $d_{ij} = 1$ – повне руйнування відповідного КПЕ.

Значення d_{ij} визначаються експертним шляхом із урахуванням механізму впливу конкретної загрози на конкретний КПЕ.

Частковий показник впливу загрози T_i на КПЕ E_j з урахуванням ймовірності реалізації:

$$I_{ij} = P(T_i) \cdot d_{ij}, \; I_{ij} \in [0, 1]$$

де I_{ij} – частковий показник впливу, що характеризує очікувану шкоду КПЕ E_j від загрози T_i;

$P(T_i)$ – результуюча ймовірність реалізації загрози (з Етапу 2.1);

d_{ij} – ступінь деструктивного впливу (з матриці впливу D).

5.4. Етап 2.4. Адитивна згортка

На цьому етапі формуються інтегральні показники впливу когнітивних загроз за допомогою дворівневої адитивної згортки.

5.4.1. Перший рівень: інтегральний вплив кожної загрози

$$I_i = \sum_{j=1}^{k} w_j^E \cdot I_{ij} = \sum_{j=1}^{k} w_j^E \cdot P(T_i) \cdot d_{ij}, \; i = 1, ..., m$$

де I_i – інтегральний показник впливу загрози T_i на ССК, $I_i \in [0, 1]$;

w_j^E – вага значущості j-го КРІ (з Етапу 2.2, метод МАІ);

I_{ij} – частковий показник впливу (з Етапу 2.3).

5.4.2. Другий рівень: загальний інтегральний показник

$$I_{xek} = \sum_{i=1}^{m} w_i^T \cdot I_i = \sum_{i=1}^{m} w_i^T \cdot [\sum_{j=1}^{k} w_j^E \cdot P(T_i) \cdot d_{ij}]$$

де I_{xek} – загальний інтегральний показник впливу когнітивних загроз на ефективність ССК;
w_i^T – вага пріоритетності і-ї загрози (з Часткової методики І);
I_i – інтегральний вплив і-ї загрози (з першого рівня згортки).

5.4.3. Показник залишкової ефективності ССК

$$E_{зал} = 1 - I_{xek}, \quad E_{зал} \in [0, 1]$$

де $E_{зал}$ – показник залишкової ефективності ССК після впливу когнітивних загроз. Значення Езал = 1 відповідає повній ефективності (відсутність впливу), Езал = 0 – повній втраті ефективності.

5.5. Етап 2.5. Аналіз чутливості

Аналіз чутливості є обов'язковим етапом методики, що забезпечує оцінку робастності результатів до зміни вхідних параметрів. Проводиться дослідження впливу варіації ключових параметрів на інтегральний показник I_{xek} та залишкову ефективність $E_{зал}$.

5.5.1. Параметри для аналізу чутливості

Аналіз проводиться за такими параметрами:

1) ваги пріоритетності загроз w_i^T – варіація ±10% від базового значення;
2) ваги КПЕ w_j^E – варіація ±15% від базового значення;
3) коефіцієнти ефективності протидії η_i – варіація ±20% від базового значення;
4) базові ймовірності $P_o(T_i)$ – варіація ±10% від базового значення.

5.5.2. Методика проведення аналізу чутливості

Для кожного параметра ϑ_k проводиться:

1) Однофакторний аналіз: послідовна зміна одного параметра при фіксованих інших. Для кожного значення параметра обчислюється $I_{xek}(\vartheta_k)$.

2) Обчислення коефіцієнта чутливості:

$$S_k = |\Delta I_{xek} / \Delta \vartheta_k| \cdot (\vartheta_k^o / I_{xek}^o)$$

де S_k – безрозмірний коефіцієнт чутливості до параметра ϑ_k;
ΔI_{xek} – зміна інтегрального показника;
$\Delta\theta_k$ – зміна параметра;
ϑ_k^o, I_{xek}^o – базові значення параметра та інтегрального показника.

Якщо $S_k > 1$, зміна параметра призводить до більш ніж пропорційної зміни результату – параметр є критичним і потребує особливо точного визначення.

5.6. Етап 2.6. Порогові значення та зворотний зв'язок

5.6.1. Класифікація стану ССК

Визначаються три порогові рівні залишкової ефективності ССК (табл. 2).

Зворотний зв'язок реалізується через ітеративний цикл коригування коефіцієнтів ефективності протидії:

1. Якщо $E_{зал}$ потрапляє у жовту або червону зону – ініціюється процедура коригування.
2. Визначаються загрози з найбільшим внеском у I_{xek} (тобто з найбільшим добутком $w_i^T \cdot I_i$).
3. Для пріоритетних загроз моделюється підвищення η_i на задану величину $\Delta\eta$.
4. Перераховується $P(T_i)$, I_{ij}, I_i, I_{xek}, $E_{зал}$ з оновленими параметрами.
5. Цикл повторюється до досягнення $E_{зал} \geq 0.70$ або вичерпання можливостей підвищення η_i.

Таблиця 2: Порогові рівні залишкової ефективності ССК

Зона	Умова	Стан ССК	Управлінське рішення
Зелена	Езал ≥ 0.70	Прийнятна ефективність	Моніторинг, планова протидія, профілактичні заходи
Жовта	0.40 ≤ Езал < 0.70	Знижена ефективність	Посилення заходів протидії, перерозподіл ресурсів, підвищення готовності
Червона	Езал < 0.40	Критична ефективність	Негайне реагування, кризове управління, мобілізація додаткових ресурсів

Джерело: *розроблено автором.*

5.6.2. Механізм зворотного зв'язку

Формула *k*-ї ітерації:

$$E_{зал}^{(k)} = 1 - \sum_i w_i^T \cdot \sum_j w_j^E \cdot P_0(T_i) \cdot (1 - \eta_i^{(k)}) \cdot d_{ij}$$

де $\eta_i^{(k)}$ – коефіцієнт протидії на *k*-й ітерації.

Обговорення

Отримані результати підтверджують доцільність застосування інтегрованого математико-аналітичного підходу для оцінювання когнітивних загроз у системі стратегічних комунікацій Збройних Сил України. Запропонована методика поєднує інструментарій теорії ігор, теорії ймовірностей, методу аналізу ієрархій та адитивної згортки, що дозволяє формалізувати процес пріоритезації загроз та кількісно оцінити їх вплив на ефективність системи стратегічних комунікацій.

Використання теоретико-ігрового підходу забезпечує моделювання когнітивного протиборства як конфліктної взаємодії між суб'єктом когнітивного впливу та системою стратегічних комунікацій. Такий підхід дозволяє визначити відносну небезпечність різних типів когнітивних загроз і сформувати ваги їх пріоритетності з урахуванням стратегічної поведінки противника.

Застосування ймовірнісних методів і методу аналізу ієрархій забезпечує визначення ваг ключових показників ефективності системи стратегічних комунікацій та створює основу для інтегрального оцінювання впливу загроз. Подальше використання адитивної згортки дозволяє агрегувати різнорідні показники у єдиний інтегральний індикатор та визначити показник залишкової ефективності системи стратегічних комунікацій.

Разом з тим запропонована методика має певні обмеження. Вона базується на припущенні раціональної поведінки противника та адитивної незалежності показників ефективності, а також значною мірою залежить від якості експертних оцінок вхідних параметрів. Крім того, модель має статичний характер і не враховує можливу динамічну зміну стратегій когнітивного впливу в інформаційному середовищі.

Отримані результати можуть бути використані як аналітична основа для підтримки управлінських рішень у сфері стратегічних комунікацій та визначення пріоритетних напрямів протидії когнітивним загрозам.

Висновки

У статті обґрунтовано доцільність інтеграції теоретико-ігрового підходу, інструментарію теорії ймовірностей, методу адитивної згортки та методу аналізу ієрархій (AHP) в єдину комплексну методику пріоритезації та оцінювання впливу когнітивних загроз на ефективність системи стратегічних комунікацій Збройних Сил України в умовах триваючої російсько-української

війни. Доведено, що теоретико-ігрове моделювання забезпечує стратегічну формалізацію когнітивного протиборства як взаємодії суб'єктів у середовищі неповної інформації та дозволяє визначати ймовірні сценарії розвитку інформаційних атак і критичні точки вразливості комунікаційної системи. Показано, що використання положень теорії ймовірностей, зокрема механізмів байєсівського оновлення оцінок, створює кількісну основу для вимірювання невизначеності, прогнозування поширення деструктивних наративів та оцінювання ризику їх впливу на цільові аудиторії. Встановлено, що метод адитивної згортки забезпечує можливість агрегування різнорідних показників когнітивних загроз у єдиний інтегральний індекс за умови коректного визначення вагових коефіцієнтів і перевірки незалежності критеріїв. Обґрунтовано ефективність методу аналізу ієрархій (AHP) для структурованого визначення ваг критеріїв, формалізації експертних оцінок і ранжування загроз за рівнем їх критичності для функціонування стратегічних комунікацій. Доведено, що комплексне поєднання зазначених математичних процедур підвищує об'єктивність управлінських рішень, сприяє оптимізації розподілу ресурсів інформаційної протидії та формує прозорий механізм визначення пріоритетів реагування на когнітивні атаки.

Сформована методика має практичну значущість для підвищення стійкості системи стратегічних комунікацій ЗСУ, збереження морально-психологічної стабільності особового складу та підтримання суспільної довіри в умовах інтенсивного інформаційного протиборства. Перспективами подальших досліджень є розроблення динамічних стохастичних моделей когнітивного протиборства з урахуванням часової еволюції загроз, інтеграція нечітких множин (Fuzzy AHP) для зменшення впливу експертної невизначеності, створення програмного інструментарію автоматизованої підтримки прийняття рішень на основі запропонованої методики, а також її емпірична верифікація на матеріалах реальних інформаційних операцій періоду російсько-української війни.

Результати дослідження можуть використовуватися у сфері стратегічних комунікацій, інформаційної безпеки, морально-психологічного забезпечення, інформаційно-аналітичної діяльності та оборонного планування, а їх практичне впровадження є доцільним в органах військового управління стратегічного й оперативного рівнів, у структурах Генерального штабу Збройних Сил України, підрозділах стратегічних комунікацій та інформаційних операцій, органах планування сил оборони, а також у системі підготовки військових кадрів і науково-дослідних установах сектору безпеки і оборони України.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Barabanov, M. *Lessons and Implications from Russia's Invasion of Ukraine (2022–2023)*. London: RUSI Reports, 2023. URL: https://rusi.org/explore-our-research/publications/rusi-reports/lessons-and-implications-russias-invasion-ukraine-2022-23
2. Gates, S., & Sanchez-Casares, T. *Disinformation and Geopolitical Conflict: Russia's Ukraine Campaign* // Journal of Strategic Security. 2023. Vol. 16, № 2. С. 12–29. https://doi.org/10.5038/1944-0472.16.2.1925.
3. Lucas, E. *The New Cold War: Russia's Information War in Ukraine* // Journal of International Affairs. 2023. Vol. 76, № 1. С. 101–120. http://jia.sipa.columbia.edu.
4. Mendel, T. *Russia's Information Warfare Against Ukraine and the West*. Tallinn: ICDS, 2022. URL: https://icds.ee/en/russias-information-warfare-against-ukraine-and-the-west

5. Pomeranzev, P., & Weiss, M. *The Menace of Unreality: How the Kremlin Weaponizes Information* // Institute of European, Russian and Eurasian Studies. Georgetown University, 2014. URL: https://www.sais-berkeley.edu/sites/default/files/menace_of_unreality_pomeranzev_weiss.pdf
6. *Russia's Offensive Campaign Assessment — Ukraine* // Institute for the Study of War (ISW), 2022–2024. (серія аналітичних оновлень). URL: https://www.understandingwar.org/project/russian-offensive-campaign-assessment
7. Дрозд, О. *Інформаційно-психологічна війна в умовах російсько-української війни* // Вісник Національної академії наук України. 2023. № 4. С. 45–60.
8. Олександр Кінь, Олег Нечаєв, Олег Темний, Володимир Рахімов, Ярослав Янковий (2025) Щодо пріоритезації когнітивних загроз системі стратегічних комунікацій Збройних Сил України в умовах війни. Міжнародний науковий журнал «Military Science». Том 3 № 3. С. 273-287. https://doi.org/10.62524/msj.2025.3.3.
9. von Neumann, J., & Morgenstern, O. *Theory of Games and Economic Behavior*. Princeton: Princeton University Press, 1944. Перевидання 2007. ISBN: 978-0691130613
10. Nash, J. *Non-Cooperative Games* // Annals of Mathematics. 1951. Vol. 54, № 2. С. 286–295. JSTOR: https://www.jstor.org/stable/1969529.
11. Schelling, T. *The Strategy of Conflict*. Cambridge, MA: Harvard University Press, 1960. ISBN: 978-0674840317
12. Savage, L.J. *The Foundations of Statistics*. New York: Wiley, 1954. ISBN: 978-0471082589
13. Bayes, T. *An Essay towards Solving a Problem in the Doctrine of Chances* // Philosophical Transactions of the Royal Society. 1763. Vol. 53. С. 370–418. https://www.jstor.org/stable/107215
14. Raiffa, H. *Decision Analysis: Introductory Lectures on Choices under Uncertainty*. Reading, MA: Addison-Wesley, 1968. ISBN: 978-0201021663
15. Keeney, R.L., & Raiffa, H. *Decisions with Multiple Objectives: Preferences and Value Trade-Offs*. New York: Wiley, 1976. ISBN: 978-0471094697
16. Saaty, T.L. *The Analytic Hierarchy Process*. New York: McGraw-Hill, 1980. ISBN: 978-0070543713
17. Saaty, T.L. *Decision Making with the Analytic Hierarchy Process* // International Journal of Services Sciences. 2008. Vol. 1, № 1. С. 83–98. https://doi.org/10.1504/IJSSCI.2008.017590.
18. Vargas, L.G. *An Overview of the Analytic Hierarchy Process and its Applications* // European Journal of Operational Research. 1990. Vol. 48. С. 2–8. https://doi.org/10.1016/0377-2217(90)90030-M.
19. Belton, V., & Stewart, T. *Multiple Criteria Decision Analysis: An Integrated Approach*. Dordrecht: Kluwer Academic Publishers, 2002. ISBN: 978-1402004083
20. Triantaphyllou, E. *Multi-Criteria Decision Making Methods: A Comparative Study*. Dordrecht: Kluwer, 2000. ISBN: 978-0792377010

References

1. Barabanov, M. Lessons and Implications from Russia's Invasion of Ukraine (2022–2023). London: RUSI Reports, 2023. URL: https://rusi.org/explore-our-research/publications/rusi-reports/lessons-and-implications-russias-invasion-ukraine-2022-23.
2. Gates, S., & Sanchez-Casares, T. Disinformation and Geopolitical Conflict: Russia's Ukraine Campaign // Journal of Strategic Security. 2023. Vol. 16, No. 2. P. 12–29. https://doi.org/10.5038/1944-0472.16.2.1925.
3. Lucas, E. The New Cold War: Russia's Information War in Ukraine // Journal of International Affairs. 2023. Vol. 76, No. 1. P. 101–120. http://jia.sipa.columbia.edu
4. Mendel, T. Russia's Information Warfare Against Ukraine and the West. Tallinn: ICDS, 2022. URL: https://icds.ee/en/russias-information-warfare-against-ukraine-and-the-west

5. Pomeranzev, P., & Weiss, M. The Menace of Unreality: How the Kremlin Weaponizes Information // Institute of European, Russian and Eurasian Studies. Georgetown University, 2014. URL: https://www.sais-berkeley.edu/sites/default/files/menace_of_unreality_pomeranzev_weiss.pdf
6. Russia's Offensive Campaign Assessment — Ukraine // Institute for the Study of War (ISW), 2022–2024. (a series of analytical updates). URL: https://www.understandingwar.org/project/russian-offensive-campaign-assessment
7. Drozd, O. Information and psychological warfare in the context of the Russian-Ukrainian war // Bulletin of the National Academy of Sciences of Ukraine. 2023. No. 4. P. 45–60.
8. Oleksandr Kin, Oleg Nechayev, Oleg Temnyi, Volodymyr Rakhimov, Yaroslav Yankovy (2025) On the prioritization of cognitive threats to the strategic communications system of the Armed Forces of Ukraine in wartime. International scientific journal "Military Science". Vol. 3 No. 3 (2025). P. 273-287. https://doi.org/10.62524/msj.2025.3.3.
9. von Neumann, J., & Morgenstern, O. Theory of Games and Economic Behavior. Princeton: Princeton University Press, 1944. Reprint 2007. ISBN: 978-0691130613
10. Nash, J. Non-Cooperative Games // Annals of Mathematics. 1951. Vol. 54, No. 2. P. 286–295. JSTOR: https://www.jstor.org/stable/1969529
11. Schelling, T. The Strategy of Conflict. Cambridge, MA: Harvard University Press, 1960. ISBN: 978-0674840317
12. Savage, L.J. The Foundations of Statistics. New York: Wiley, 1954. ISBN: 978-0471082589
13. Bayes, T. An Essay towards Solving a Problem in the Doctrine of Chances // Philosophical Transactions of the Royal Society. 1763. Vol. 53. P. 370–418. https://www.jstor.org/stable/107215.
14. Raiffa, H. Decision Analysis: Introductory Lectures on Choices under Uncertainty. Reading, MA: Addison-Wesley, 1968. ISBN: 978-0201021663
15. Keeney, R.L., & Raiffa, H. Decisions with Multiple Objectives: Preferences and Value Trade-Offs. New York: Wiley, 1976. ISBN: 978-0471094697
16. Saaty, T.L. The Analytic Hierarchy Process. New York: McGraw-Hill, 1980. ISBN: 978-0070543713
17. Saaty, T.L. Decision Making with the Analytic Hierarchy Process // International Journal of Services Sciences. 2008. Vol. 1, No. 1. P. 83–98. https://doi.org/10.1504/IJSSCI.2008.017590.
18. Vargas, L.G. An Overview of the Analytic Hierarchy Process and its Applications // European Journal of Operational Research. 1990. Vol. 48. P. 2–8. https://doi.org/10.1016/0377-2217(90)90030-M.
19. Belton, V., & Stewart, T. Multiple Criteria Decision Analysis: An Integrated Approach. Dordrecht: Kluwer Academic Publishers, 2002. ISBN: 978-1402004083
20. Triantaphyllou, E. Multi-Criteria Decision Making Methods: A Comparative Study. Dordrecht: Kluwer, 2000. ISBN: 978-0792377010

This is an open access journal and all published articles are licensed under a Creative Commons «Attribution» 4.0.