The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 3 (2025)

**Received:** *October 11, 2025* | **Revisions Requested:** *November 18, 2025* | **Revision Received:** *November 26, 2025*
**Accepted:** *November 28, 2025* | **Published Online:** *December 1, 2025*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2025.3.3.22

# Щодо пріоритезації когнітивних загроз системі стратегічних комунікацій Збройних Сил України в умовах війни

**Олександр Кінь**
кандидат технічних наук, доцент
Дипломатична академія України імені Геннадія Удовенка
при Міністерстві закордонних справ
01001, вул. Велика Житомирська, Київ, Україна
email: cubalibre1972@ukr.net
ORCID: 0009-0001-2196-7515

**Олег Нечаєв**
перший заступник командувача Сил спеціальних операцій ЗС України
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: o26811650@gmail.com
ORCID: 0009-0001-2839-2830

**Олег Темний**
ад'юнкт кафедри
інформаційної боротьби інституту стратегічних комунікацій
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: o.temnyi@edu.nuou.org.ua
ORCID: 0009-0009-3173-094X

**Володимир Рахімов**
доктор філософії
заступник начальника інституту стратегічних комунікацій
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: rakhimov@edu.nuou.org.ua
ORCID: 0000-0001-9868-986X

**Ярослав Янковий**
ад'юнкт кафедри інформаційної боротьби
інституту стратегічних комунікацій
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: ya.yankovyi@gmail.com
ORCID: 0009-0007-1718-3607

**Анотація.** Система стратегічних комунікацій Збройних Сил України, попри значний розвиток, стикається з низкою викликів: надмірні інформаційні потоки під час активних фаз бойових дій, складність синхронізації комунікацій між різними суб'єктами безпекового сектору, швидкість появи нових деструктивних наративів, широке використання deepfake-технологій, а також інформаційне виснаження суспільства. У таких умовах традиційні підходи до оцінювання інформаційних загроз, які ґрунтуються на аналізі поширення окремих повідомлень чи джерел, стають недостатніми. Вони не дозволяють своєчасно визначати, які саме загрози можуть мати стратегічний ефект, які вразливості потребують негайного реагування, а які можуть бути віднесені до нижчих пріоритетів. Актуальність проблеми посилюється тим, що когнітивні загрози мають нелінійний, часто прихований характер, а їхній вплив може накопичуватися поступово, утворюючи комбінований ефект. Кожна помилка в оцінюванні важливості окремої загрози створює ризики для оперативного управління, міжнародної комунікації, підтримки партнерів та збереження мотивації особового складу. У цих умовах пріоритезація загроз стає критично необхідним процесом. Отже, розроблення методичного апарату (методики) пріоритезації когнітивних загроз системі стратегічних комунікацій Збройних Сил України є критично важливим для підвищення ефективності інформаційної та психологічної стійкості держави у війні. Такий методичний апарат забезпечить об'єктивне, системне й передбачуване оцінювання впливів, що дозволяє своєчасно реагувати на небезпечні загрози, мінімізувати наслідки інформаційних ударів та зберігати стратегічну ініціативу в когнітивній площині. Основними результатами статті є те, що в ній: проведений аналіз закордонного й українського досвіду щодо наявних підходів до пріоритезації когнітивних (інформаційно-когнітивних) загроз системі стратегічних комунікацій Збройних Сил України; сформований розширений перелік когнітивних загроз, що актуальні для системи стратегічних комунікацій Збройних Сил України; зроблено пріоритезацію когнітивних загроз системі стратегічних комунікацій Збройних Сил України за підходом ймовірність-наслідок, з наочними розрахунками методом експертного опитування. Матеріали статті можуть бути корисними для військових, аналітиків, фахівців з безпеки, науковців і стратегів, які займаються захистом інформаційного простору та реагуванням на сучасні когнітивні загрози у сфері воєнної безпеки України. Перспективними подальшими напрямами наукових досліджень у цій сфері є розвиток динамічних моделей пріоритезації когнітивних загроз із урахуванням мережевих характеристик інформаційного середовища, удосконалення алгоритмів автоматизованого моніторингу та класифікації загроз із використанням методів машинного навчання, а також формування інтегрованих систем підтримки рішень для стратегічних комунікацій, здатних працювати в режимі реального часу та адаптуватися до еволюції інформаційно-психологічних операцій противника.

**Ключові слова:** багатокритеріальні методи та моделі, збройна боротьба, когнітивні загрози, когнітивний вплив, когнітивні виклики, індекс когнітивного тиску, технології війни, метод аналізу ієрархій, національна безпека, Збройні Сили України, методи ведення війни, трансформація збройних конфліктів, реагування на когнітивні загрози, моніторинг когнітивних загроз, система стратегічних комунікацій, російсько-українська війна.

## Вступ (Introduction)

Тривала російсько-українська війна засвідчила, що супротивник робить ставку не лише на військову силу, а й на системне, багаторівневе застосування когнітивних операцій, спрямованих на підрив стійкості українського суспільства, деморалізацію військовослужбовців, спотворення сприйняття подій та делегітимізацію рішень державного і військового керівництва. Особливо значущою сферою, на яку націлено більшість когнітивних ударів, є система стратегічних комунікацій Збройних Сил України (ЗС України) (СтратКом ЗС

України), що забезпечує узгодженість інформаційних сигналів, формує довіру суспільства й партнерів, а також підтримує морально-психологічну стійкість особового складу. У цих умовах виникає нагальна потреба у створенні дієвої та науково обґрунтованої методики пріоритезації когнітивних загроз, яка дозволить оптимізувати реагування та забезпечити проактивний, а не реактивний характер стратегічних комунікацій [1–6].

російська федерація застосовує комплексну модель когнітивного впливу, яка поєднує інформаційно-психологічні операції, кібердії, психологічне маніпулювання, технології штучного інтелекту, соціальне інженерство, експлуатацію травм суспільства та використання військових успіхів чи невдач для формування деструктивних наративів. Метою таких дій є зміна поведінки цільових аудиторій, а саме: зниження готовності до оборони, підрив довіри до командування, формування помилкового сприйняття оперативно-стратегічної обстановки, поширення панічних настроїв та посилення внутрішніх конфліктів. Успішність таких операцій значною мірою залежить від здатності їх суб'єкта виявляти ключові вразливості, використовувати інформаційні вікна можливостей та завдавати ударів там, де ефект буде максимальним.

Система стратегічних комунікацій ЗС України, попри значний розвиток, стикається з низкою викликів: надмірні інформаційні потоки під час активних фаз бойових дій, складність синхронізації комунікацій між різними суб'єктами безпекового сектору, швидкість появи нових деструктивних наративів, широке використання deepfake-технологій, а також інформаційне виснаження суспільства. У таких умовах традиційні підходи до оцінювання інформаційних загроз, які ґрунтуються на аналізі поширення окремих повідомлень чи джерел, стають недостатніми [1–6]. Вони не дозволяють своєчасно визначати, які саме загрози можуть мати стратегічний ефект, які вразливості потребують негайного реагування, а які можуть бути віднесені до нижчих пріоритетів.

Актуальність проблеми посилюється тим, що когнітивні загрози мають нелінійний, часто прихований характер, а їхній вплив може накопичуватися поступово, утворюючи комбінований ефект. Кожна помилка в оцінюванні важливості окремої загрози створює ризики для оперативного управління, міжнародної комунікації, підтримки партнерів та збереження мотивації особового складу. У цих умовах пріоритезація загроз стає критично необхідним процесом, адже дозволяє:

концентрувати ресурси на найбільш небезпечних напрямах когнітивних атак;

скорочувати час реагування;

мінімізувати інформаційні втрати;

забезпечувати узгодженість між військовими та цивільними комунікаційними структурами;

формувати наративи, що превентивно нейтралізують потенційні загрози.

Однією з характерних особливостей російських операцій є їхня адаптивність: супротивник швидко перебудовує наративи залежно від розвитку ситуації на фронті, політичних рішень або внутрішніх подій в Україні. Відтак відсутність методичного апарату, що дозволяє об'єктивно оцінювати й ранжувати загрози залежно від їхнього потенційного ефекту, створює інформаційний розрив між темпом когнітивного наступу ворога та можливостями української сторони. Пріоритезація загроз є ключовою для забезпечення ієрархії реагування, визначення критичних цільових аудиторій, вибору оптимальних способів нейтралізації та коректного розподілу інформаційних ресурсів в умовах війни.

Крім того, український і міжнародний досвід демонструють, що в сучасних війнах перемога визначається не лише тактичними успіхами на полі бою, а й здатністю контролювати інформаційні та когнітивні домени. Успішна стратегічна комунікація формує образ суб'єкта, що здатен управляти війною, зберігати моральну перевагу, демонструвати стійкість і є стратегічно передбачуваним для партнерів. Водночас прорахунки у розподілі уваги між

різними когнітивними загрозами можуть призвести до зниження міжнародної підтримки, появи спотвореної репутаційної картини або невірного трактування ситуації зовнішніми акторами.

Сучасні виклики також пов'язані зі стрімким поширенням технологій генеративного штучного інтелекту, що значно спрощує створення контенту, здатного вводити в оману, і дає супротивнику інструменти масованих когнітивних атак із мінімальними витратами. Це змінює природу загроз: від поодиноких інформаційних операцій до потокової, автоматизованої дезінформації, яка потребує нових методів вимірювання небезпеки. Тому застосування формалізованих підходів до ранжування, оцінювання шкоди, визначення індексу небезпеки або рівня стратегічної значущості загроз стає не просто бажаним, а обов'язковим елементом сучасної інформаційної оборони.

Отже, розроблення методичного апарату (методики) пріоритезації когнітивних загроз системі стратегічних комунікацій ЗС України є критично важливим для підвищення ефективності інформаційної та психологічної стійкості держави у війні. Такий методичний апарат забезпечить об'єктивне, системне й передбачуване оцінювання впливів, що дозволяє своєчасно реагувати на небезпечні загрози, мінімізувати наслідки інформаційних ударів та зберігати стратегічну ініціативу в когнітивній площині.

**Матеріали та методи (Materials and Methods)**

Аналіз закордонного й українського досвіду [1–17] щодо наявних підходів до пріоритезації когнітивних (інформаційно-когнітивних) загроз системі стратегічних комунікацій ЗС України дозволяє виділити й розгорнути ключові особливості підходів та продемонструвати математичні залежності (моделі), які застосовують у практиці або, які доцільно застосувати.

По-перше, досвід Північно-атлантичного альянсу та супутні натівські доктрини підкреслюють комплексний, міждисциплінарний характер стратегічних комунікацій: StratCom має забезпечувати узгодженість дій, слідкувати за узгодженістю "слів і вчинків", інтегрувати інформаційні, публічні й кіберінструменти та працювати в циклі "спостерігай-орієнтуйся-дій-оцінюй". Це відображено в натівських військово-доктринальних документах і аналітичних матеріалах Центру стратегічних комунікацій НАТО. [11].

По-друге, американські оперативні доктрини з інформаційних операцій продовжують займатися питаннями планування, виконання та оцінювання інформаційних заходів, інтеграції OPSEC і кіберпотенціалу з операціями впливу. Ці документи виписують ризик-орієнтований підхід і підкреслюють потребу в циклічному оцінюванні результатів. [3].

По-третє, наукові та аналітичні праці останніх років концентруються на трьох важливих трендах [9–17]:

а) динамічності загроз – інформаційні кампанії – це не статичні події, а процеси, що швидко еволюціонують;

б) ролі штучного інтелекту й генеративних технологій – AI створює масштабний, дешевий контент (deepfakes, згенеровані тексти, автоматизовані ботоферми), що радикально змінює швидкість і масовість впливу;

в) необхідності кількісних метрик і динамічних моделей (мережевий аналіз, епідеміологічні моделі поширення, байєсовські оновлення й MCDM-підходи).

Ці висновки послідовно описані в провідних працях з інформаційної війни та дезінформації [4–9].

По-четверте, український досвід – офіційні концепції й доктрини стратегічних комунікацій, а також практика роботи під час широкомасштабної війни, які показують

орієнтацію на міжвідомчу координацію, оперативну готовність і необхідність адаптивних методів пріоритезації, які могли б працювати в умовах обмежених ресурсів і високої швидкості виникнення нових інформаційних загроз [9].

По-п’яте, практики і дослідження RAND, StratCom CoE та провідних міжнародних аналітичних центрів підкреслюють вагомість поєднання кількісних методів з експертними оцінками: багатокритеріальні методи ухвалення рішень (AHP, TOPSIS, Fuzzy-MCDM) для врахування стратегічного значення, мережевий аналіз для визначення вузлів впливу та потенціалу поширення, а також статистичні (байєсові) підходи для динамічного оновлення ймовірностей. Такі гібридні системи найкраще поєднують інтерпретованість для командування та адаптивність до реального часу, що підтверджується рекомендаціями центрів досліджень [11].

Нарешті, у наукових статтях із теми когнітивної війни й інформаційної безпеки підкреслюється потреба у валідації моделей (back-testing) на реальних кейсах, чутливісному аналізі ваг і параметрів, автоматизованих індикаторах (збір телеметрії зі соцмереж, OSINT, сигналів бот-активності) та створенні оперативних дашбордів для ухвалення рішень. Ці методичні висновки ґрунтуються на сучасній літературі з моделювання інформаційних каскадів і на практичних звітах про кампанії дезінформації [1–17].

*Ризик-орієнтований підхід* – простий, прозорий та зрозумілий для командування / Добре працює як оперативний фільтр (визначення критичних загроз), але недостатньо враховує мережеву динаміку поширення контенту і мультиплікаційні ефекти [2–3].

*Багатокритеріальні методи (AHP, TOPSIS, Fuzzy MCDM)* – дають формалізований підхід до ранжування із врахуванням ваг критеріїв (стратегічний вплив, швидкість поширення, масштаб аудиторії, вразливість, вартість реагування, ймовірність) і підходять для планування ресурсів та довгострокових пріоритетів.

*Мережеві й епідеміологічні моделі (SIR / SI, графові моделі)* – необхідні для оцінювання потенціалу поширення та виявлення “вузлів”, реакція на які дає мультиплікативний ефект; важливі для оперативного реагування проти бот-кампаній і масових deepfake-атак.

*Динамічні (байєсові)* підходи дозволяють оновлювати ймовірності та пріоритети у реальному часі на основі спостережень (темпи росту, коефіцієнт бот-активності, охоплення), що є критичним у швидкоплинних інформаційних кампаніях.

*Гібридна модель* – це моделі поєднання MCDM (багатокритеріальне ухвалення рішень) (AHP (метод аналізу ієрархії) / TOPSIS (метод вибору порядку переваг за подібністю до ідеального рішення) для первинного ранжування + мережевий коефіцієнт (centrality, бот-індикатор) + динамічний множник (темп росту) + байєсовське оновлення ймовірностей дає найкращий компроміс між інтерпретованістю для керівництва і адаптивністю до реального часу. Цю ідею підтримують і натівські експерти й аналітики, які радять комбінувати кількісні моделі й експертні оцінки.

У контексті триваючої, високошвидкісної та багатоканальної російсько-української війни найбільш прийнятним підходом до пріоритезації когнітивних загроз є гібридний багатоетапний підхід, що поєднує:

- багатокритеріальне первинне ранжування (AHP (метод аналізу ієрархії) для визначення ваг критеріїв; TOPSIS (метод вибору порядку переваг за подібністю до ідеального рішення) або еквівалент для ранжування загроз за зваженими показниками), а також забезпечує структуровану, прозору основу для розподілу ресурсів і політичної аргументації.

- мережеву корекцію (динамічний множник) – додавання індикаторів network-centrality, темпу приросту охоплення (growth rate) та частки автоматизованого трафіку (bot indicator) для

корекції базового рейтингу – це дозволяє пріоритезувати ті загрози, які здатні швидко “заразити” велику аудиторію.

- байєсовське або статистичне оновлення ймовірностей через регулярне оновлення ймовірності подій у часі (P(t)) на підставі нових телеметричних даних для збереження актуальності пріоритетів у реальному часі.

- експертну адаптацію й контроль шляхом періодичного збирання думок міжвідомчої експертної групи для корекції ваг AHP, валідації моделі й налаштування порогів реагування – це відповідає доктринальним вимогам НАТО і американських JP-документів щодо інтеграції людського фактора у автоматизовані рішення.

Такий гібридний підхід дає змогу поєднати інтерпретованість (щоб командування могло аргументовано віддавати пріоритети), адаптивність (щоб реагувати на швидкі “вибухові” кампанії) та ефективність розподілу обмежених ресурсів (щоб спрямовувати заходи на ті вузли (кампанії), які мають найбільший мультиплікативний ефект). Ця рекомендація узгоджується з практикою та аналітикою провідних міжнародних центрів (NATO StratCom CoE, RAND) і відповідає сучасним викликам.

**Результати (Results)**

У сучасних умовах триваючої російсько-української війни система стратегічних комунікацій ЗС України перебуває під постійним і багатовекторним тиском з боку державних, напівдержавних, проксі- та приватних акторів інформаційно-психологічного впливу противника. Ключовою особливістю цього впливу є перехід від традиційних інформаційних операцій до когнітивних операцій нового покоління, які спрямовані не лише на зміну окремих уявлень чи реакцій аудиторії, а на переорієнтацію глибинних моделей мислення, здатних впливати на поведінку військових, суспільства та міжнародних партнерів [4–9].

Відповідно, стратегічні комунікації ЗС України опиняються у ситуації, коли об’єктом атаки стають не лише інформаційні повідомлення чи канали їх поширення, а цілі когнітивні структури: цінності, емоційні патерни, довіра до інституцій, уявлення про перебіг бойових дій, морально-психологічний стан особового складу та легітимність оборонної політики держави.

Еволюція російських інформаційно-психологічних операцій демонструє тенденцію до зростання складності, інтенсивності й технологічності, що проявляється у широкому застосуванні:

штучного інтелекту для генерації контенту;

автоматизованих бот-мереж;

багатоплатформених кампаній з координацією меседжів;

deepfake-відео;

таргетованого впливу на обрані сегменти української та міжнародної аудиторій;

маніпулятивних наративів, інтегрованих у довготривалі когнітивні стратегії.

За таких умов виникає потреба у систематизації, класифікації та формалізації всього спектру загроз, що впливають на здатність стратегічних комунікацій ефективно виконувати свої функції. Ідентифікація загроз стає ключовим етапом для побудови методів пріоритезації, оскільки саме визначення природи та джерела загроз дозволяє перейти до їх кількісного оцінювання, ранжування та розроблення відповідних заходів протидії.

У цьому контексті (табл. 1) наведено розширений перелік когнітивних загроз, що актуальні для системи стратегічних комунікацій ЗС України. Таблиця охоплює: опис сутності кожної загрози, джерело її виникнення, потенційні наслідки впливу.

**Таблиця 1.** Когнітивні загрози системі стратегічних комунікацій ЗС України

| № | Когнітивна загроза | Опис загрози | Джерело виникнення | Можливий наслідок впливу |
|---|---|---|---|---|
| 1 | Дезінформація противника | Цілеспрямоване поширення неправдивих повідомлень, створених для введення в оману особового складу, населення та партнерів | Ворожі ІПСО, закордонні ЗМІ, бот-мережі | Порушення довіри до офіційної інформації, деморалізація, помилкові рішення |
| 2 | Інформаційні вкиди для провокування паніки | Масове поширення “сенсацій” про поразки, зради, втрати | Ворог, внутрішні деструктивні групи | Порушення стабільності в тилу, зниження бойового духу |
| 3 | Маніпуляція емоціями | Використання страху, гніву, втоми суспільства для зміни його поведінки й ставлення до ЗСУ | Противник, проросійські медіа, соцмережі | Емоційне виснаження, міжгрупові конфлікти, нерозуміння рішень командування |
| 4 | Підміна контексту | Викривлення окремих елементів правди з метою хибної інтерпретації ситуації | Фейкові “аналітики”, псевдоекспертні платформи | Створення альтернативної інформаційної реальності |
| 5 | Підрив довіри до командування | Поширення фейків про рішення лідерів, внутрішні конфлікти, “зраду” | Ворог, агенти впливу, анонімні Telegram-канали | Зниження дисципліни, розкол між військовими і суспільством |
| 6 | Підміна бренду “ЗСУ” ворожими меседжами | Використання стилістики, оформлення та термінології ЗСУ у фейкових повідомленнях | Професійні ІПСО-центри рф | Дискредитація сил оборони, збільшення кількості успішних фейків |
| 7 | Інформаційне перевантаження | Надмірний потік повідомлень, що ускладнює відокремлення важливого від другорядного | Соцмережі, “інфошум”, неконтрольовані канали | Зниження спроможності до критичного мислення, помилки в оцінці ситуації |
| 8 | “Повзуча нормалізація” втрат та загроз | Поступове притуплення чутливості суспільства до небезпеки | Втома від війни, інформаційна апатія | Зниження мобілізаційної готовності, байдужість до ключових рішень |
| 9 | Викривлення меседжів СтратКому внутрішніми суб’єктами | Неправильне тлумачення повідомлень пресслужб, штабу, Міноборони | Профільні комунікатори, ЗМІ, блогери | Некоректне розуміння намірів держави та ЗСУ |
| 10 | Несинхронність комунікації між відомствами | Різні або суперечливі меседжі різних органів влади | Міноборони, ГШ, інші ЦОВВ | Втрата довіри, підрив цілісності інформаційної платформи оборони |
| 11 | Витоки службової інформації | Поширення чуток, неофіційних деталей операцій, втрат, планів | Військовослужбовці, волонтери, цивільні | Створення інфоприводів для ворога, загроза операціям |
| 12 | Deepfake-атаки | Створення фальшивих відео з голосами чи обличчями військових та керівництва | ІПСО противника, ШІ-генератори | Провокації, хаос, дискредитація керівництва |
| 13 | Мета-маніпуляція (маніпуляція сенсами) | Зміна ключових понять: “мир”, “поразка”, “перемога”, “справедливість” | Ідеологічні центри, ворожі аналітичні структури | Переорієнтація цілей суспільства, підрив стійкості |
| 14 | Когнітивна ерозія внаслідок тривалої війни | Хронічна втома, зниження здатності споживати інформацію критично | Повсякденний стрес, втрати | Підвищення сприйнятливості до фейків та маніпуляцій |
| 15 | Успішне використання супротивником інфлюенсерів | Залучення популярних осіб до поширення потрібних меседжів | Дезінформаційні центри рф, корисні “ідіоти” | Легітимізація фейків через “авторитетних” осіб |
| 16 | Атаки на символи й національні наративи | Розмивання значень героїзму, боротьби, перемоги | Противник, проросійські культурні проєкти | Підрив національної ідентичності, демотивація |
| 17 | Соціальна поляризація через інформаційні впливи | Створення протиставлень: військові/цивільні, фронт/тил, влада/суспільство | Ворожі ботоферми, внутрішні маніпулятори | Послаблення єдності та обороноздатності |
| 18 | Радикалізація суспільних дискусій | Розкачування крайніх позицій, формування атмосфери конфлікту | Telegram-канали, ворожі тролі | Зниження спроможності суспільства до мобілізації та співпраці |
| 19 | Спотворення образу українських військових | Поширення історій про “некомпетентність”, “жорстокість” | Ворог, інформаційні операції за кордоном | Послаблення міжнародної підтримки |
| 20 | Системна атака на репутацію конкретних бойових підрозділів | Створення фейкових “скандалів” | рф, агенти, псевдоблогери | Погіршення морального стану особового складу, розкол між підрозділами |

Наведений перелік є узагальненим результатом аналізу сучасних інформаційних операцій противника, оцінки технологічних трендів, досвіду ведення стратегічних комунікацій під час масштабної війни та практики роботи керівництва Сил оборони України у сфері інформаційної протидії.

Зробимо пріоритезацію за підходом *ймовірність (P) × наслідок (I)*, з наочними розрахунками в табл. 2. Для уніфікації нормалізуємо ризиковий бал:

$$R_i = Pi * Ii \rightarrow S_i = R_i \ / \ 25, \ S_i \text{€}\{0;1]. \quad (1)$$

Відповідно до розрахунків кожній загрозі призначені числові оцінки, а саме: *P* (ймовірність) – 1…5 (1 – дуже низька … 5 – дуже висока). *I* (наслідок) – 1..5 (1 – незначний … 5 – критичний) та далі обчислюємо ризиковий бал. Далі за значенням *S* можна оперативно задавати пороги реагування (табл. 2, рис. 1).

Проведемо інтерпретацію отриманих результатів розрахунків, які проведені за допомогою групи експертів із 8 осіб. Проведений аналіз дав можливість визначити структуру ризиків та рівні їх критичності для системи стратегічних комунікацій ЗС України. Результати показують чітку стратифікацію загроз за рівнем пріоритетності, яка має безпосередній вплив на планування заходів реагування, розподіл ресурсів і побудову системи моніторингу.

До категорії абсолютної критичності увійшли три загрози (найвищий пріоритет (S=1): № 1 – дезінформація, № 2 – інформаційні вкиди для паніки, №5 – підрив довіри до командування. Ці загрози поєднують максимальну ймовірність виникнення та найвищі можливі наслідки. Вони мають потенціал одночасно впливати на внутрішню стійкість особового складу, суспільну ситуацію в тилу та оперативну діяльність командування. Висока швидкість їх поширення у поєднанні з низьким порогом довіри у стресових ситуаціях формують критичну комбінацію. Саме ці загрози мають бути об’єктом безперервного моніторингу, оперативного реагування, контрнаративної роботи, а також партнерської взаємодії із ЗМІ та платформами.

Другу групу становлять загрози, які мають високий пріоритет (S=0,8): № 11 – витоки службової інформації, № 12 – deepfake-атаки, № 13 – мета-маніпуляція сенсами. Ці загрози мають дещо нижчу ймовірність, але їх потенційний наслідок залишається критичним. Йдеться про загрози, які можуть призвести до втрати операційної безпеки, руйнування довіри до керівництва або зміни фундаментальних ціннісних орієнтирів суспільства. Для цієї групи домінують технічні та процедурні шляхи протидії: контроль доступу, системи попередження витоків, інструменти детекції deepfake, а також проактивні стратегічні комунікації.

Третя група когнітивних загроз – це загрози, які мають середній–високий пріоритет (S=0,64): № 6, 10, 17, 19, 20 – підміна бренду “ЗСУ”, несинхронність комунікацій, соціальна поляризація, спотворення образу військових, атаки на бойові підрозділи. Ця категорія не має максимальної небезпеки в кожному окремому пункті, але її сила полягає у системному характері впливу. Несинхронність комунікацій та інформаційна поляризація створюють “вікна вразливості”, через які ворог може масштабувати інші загрози. Підміна бренду “ЗСУ” та атаки на конкретні підрозділи впливають на міжнародне сприйняття, престиж служби та єдність армії. Ці загрози потребують міжвідомчої координації, уніфікації меседжів, стандартів комунікацій, взаємодії з міжнародними партнерами та платформами.

До групи когнітивних загроз середнього пріоритету (S=0,60): № 3 – маніпуляція емоціями, № 7 – інформаційне перевантаження, № 14 – когнітивна ерозія внаслідок тривалої війни. Ці загрози діють на рівні культурно-психологічної стійкості аудиторій та мають кумулятивний характер. Вони рідко дають миттєві наслідки, проте поступово формують втомленість, зниження критичності сприйняття та емоційну нестабільність. Протидія полягає

у розбудові стійкості – освітні ініціативи, інформаційна гігієна, психологічна підтримка військових і цивільних, комунікаційна ясність.

**Таблиця 2.** Результати пріоритезації когнітивних загроз системі стратегічних комунікацій ЗС України

| № | Когнітивна загроза (скорочено) | P | I | R = P×I | Оцінка S (0–1) |
|---|---|---|---|---|---|
| 1 | Дезінформація противника | 5 | 5 | 25 | 1 |
| 2 | Інфовкиди для паніки | 5 | 5 | 25 | 1 |
| 3 | Маніпуляція емоціями | 5 | 3 | 15 | 0,60 |
| 4 | Підміна контексту | 3 | 3 | 9 | 0,36 |
| 5 | Підрив довіри до командування | 5 | 5 | 25 | 1 |
| 6 | Підміна бренду “ЗСУ” | 4 | 4 | 16 | 0,64 |
| 7 | Інформаційне перевантаження | 5 | 3 | 15 | 0,60 |
| 8 | Повзуча нормалізація | 3 | 3 | 9 | 0,36 |
| 9 | Викривлення меседжів | 3 | 3 | 9 | 0,36 |
| 10 | Несинхронність комунікації між відомствами | 4 | 4 | 16 | 0,64 |
| 11 | Витоки службової інформації | 4 | 5 | 20 | 0,80 |
| 12 | Deepfake-атаки | 4 | 5 | 20 | 0,80 |
| 13 | Мета-маніпуляція (сенси) | 4 | 5 | 20 | 0.80 |
| 14 | Когнітивна ерозія | 5 | 3 | 15 | 0,60 |
| 15 | Використання інфлюенсерів | 3 | 3 | 9 | 0,36 |
| 16 | Атаки на наративи / символи | 3 | 3 | 9 | 0,36 |
| 17 | Соціальна поляризація | 4 | 4 | 16 | 0,64 |
| 18 | Радикалізація дискусій | 3 | 3 | 9 | 0,36 |
| 19 | Спотворення образу ЗС України за кордоном | 4 | 4 | 16 | 0,64 |
| 20 | Атаки на репутацію підрозділів | 4 | 4 | 16 | 0,64 |

Понижений, але релевантний пріоритет (S=0,36) мають когнітивні загрози № 4, 8, 9, 15, 16, 18 – підміна контексту, нормалізація небезпеки, внутрішнє спотворення меседжів, інфлюенсери, атаки на символи, радикалізація дискусій. Це загрози з помірною ймовірністю та обмеженою силою впливу, які все ж можуть посилювати інші загрози, якщо їх не контролювати. Вони потребують регламентних, але не кризових заходів: регулярного моніторингу, характеристики ризиків у звітах, інформаційно-роз’яснювальної роботи.

Практичну інтерпретацію індексу *S* (порогова шкала) можна представити таким чином: $S \geq 0{,}90$ – критичний рівень: негайні дії, кризове реагування, 24/7 моніторинг; $0{,}70 \leq S < 0{,}90$ – високий рівень: пріоритети штабу, виділення ресурсів, контроль виконання; $0{,}50 \leq S < 0{,}70$ – середній рівень: планові заходи, підвищена увага; $S < 0.50$ – низький (помірний): моніторинг і профілактика.

У контексті цієї оцінки до критичних когнітивних загроз можна віднести № 1, № 2, № 5, до високих – № 11, № 12, № 13, до середніх та важливих належать № 3, № 6, № 7, № 10, № 14, № 17, № 19, № 20, до помірних належить решта.

Метод “ймовірність×наслідок” відображає лише поточний стан і не враховує динамічності інформаційної війни та змін у ворожих кампаніях. Оцінювання *P* та *I* значною мірою залежить від досвіду експертів; можливі зміщення, різна інтерпретація, відсутність консенсусу. Поширення загроз залежить від центральності інфлюенсерів, алгоритмів платформ, бот-мереж та швидкості росту охоплення – ці фактори не включені в базову модель.

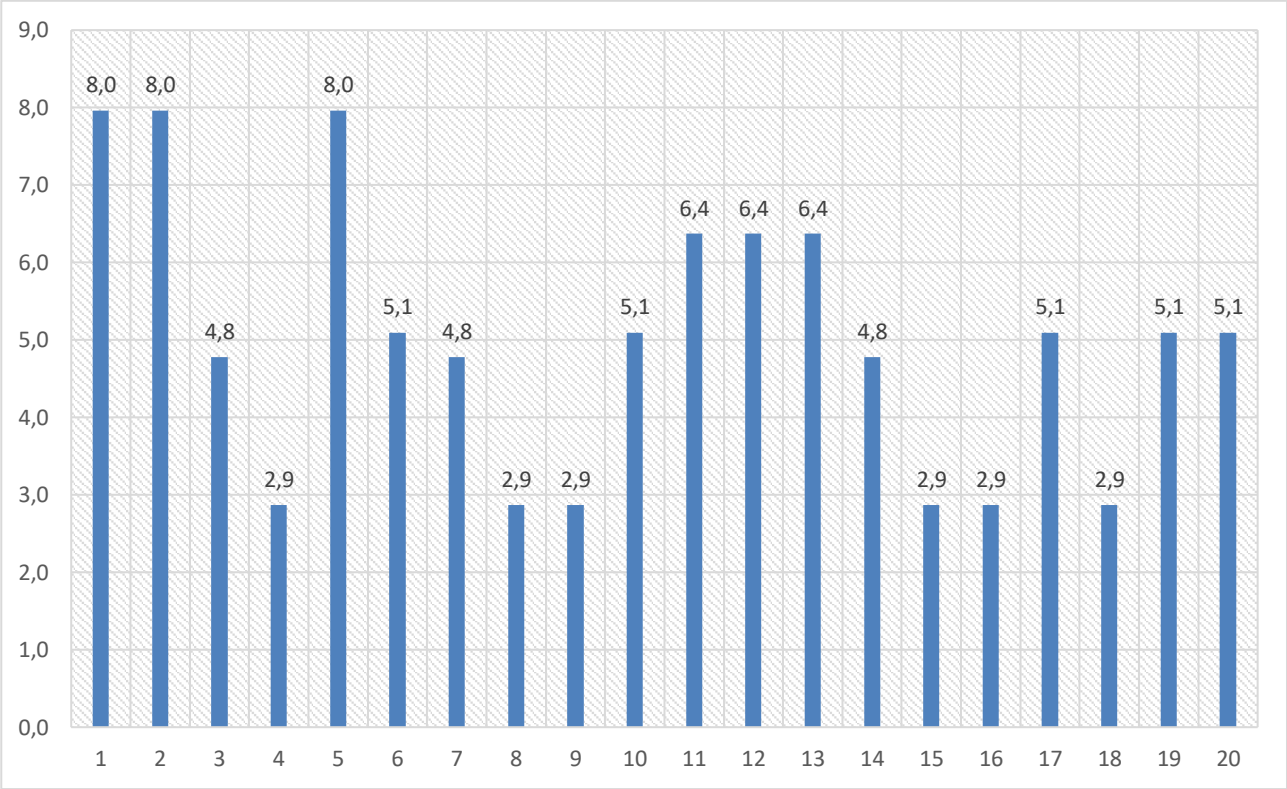



**Рисунок 1.** Нормовані оцінки впливу когнітивних загроз на систему стратегічних комунікацій в Збройних Силах України (табл. 2)

Запровадження коефіцієнтів, які відповідають за темп поширення, бот-активність, центральність джерел підвищує точність і оперативність оцінки.

Використання методу аналізу ієрархій для обґрунтування ваг критеріїв та TOPSIS (Метод вибору порядку переваг за подібністю до ідеального рішення) для багатовимірного ранжування дозволяє створити комплексну модель, що враховує стратегічний вплив, вартість реагування, уразливість аудиторій та інші аспекти.

Регулярний аналіз реальних кейсів дезінформаційних атак, оцінка точності моделі, перевірка впливу зміни ваг та параметрів.

Для загроз із найвищим пріоритетом необхідно створити практичні алгоритми реагування та чеклісти (оперативні, технічні, юридичні, організаційні).

Методика оцінювання когнітивних загроз за підходом “ймовірність×наслідок” забезпечує швидкий і зрозумілий індекс пріоритетності ($S$) у шкалі 0–1. За отриманими результатами критичними є загрози дезінформації, панічних вкидів та підриву довіри до командування (S=1). Високими залишаються витоки інформації, deepfake-атаки та мета-маніпуляції (S=0,80).

Проте для комплексної роботи зі стратегічними комунікаціями необхідно доповнити цю модель динамічними індикаторами та багатокритеріальними методами (AHP, TOPSIS), що забезпечить точнішу, адаптивну та стратегічно релевантну оцінку загроз у сучасному інформаційному середовищі.

**Висновок (Conclusion)**

Проведений аналіз підходів до пріоритезації когнітивних загроз у системі стратегічних комунікацій ЗС України показав, що у сучасних умовах російсько-української війни домінує

потреба у використанні кількісних, об'єктивних, прозорих і відтворюваних методів, які здатні врахувати як динамічність інформаційного середовища, так і багатовимірність впливів на поведінку особового складу, суспільства та міжнародних партнерів. Порівняння різних моделей, а саме: експертних, ризик-орієнтованих, багатокритеріальних, мережевих і прогностичних, доводить, що найбільш ефективними є підходи, які поєднують структуровану експертну оцінку (AHP) із методами багатокритеріального вибору (TOPSIS). Такі моделі дозволяють не тільки визначити силу та ймовірність загроз, але й створити ранжований список пріоритетів, що може бути інтегрований у процеси оперативного та стратегічного планування.

Результати аналізу підтверджують, що когнітивні загрози проти ЗС України мають системний і цілеспрямований характер, а їх структура відповідає ключовим компонентам російської інформаційно-психологічної кампанії: деморалізація військових, фрагментація суспільної підтримки, дискредитація командування, підрив довіри партнерів і створення альтернативної реальності через дезінформаційні наративи. Найбільш небезпечними виявилися загрози, які одночасно характеризуються високою ймовірністю реалізації та високими наслідками для бойової стійкості, національної волі та міжнародної позиції України. До них насамперед належать: масштабні інформаційно-психологічні операції рф, спрямовані на ЗС України; високоточні, персоналізовані атаки з використанням соціальних медіа; вплив через AI-генеративний контент та дипфейки; підрив легітимності військово-політичного керівництва; а також операції з моделювання паніки, взаємної недовіри або невпевненості у власних спроможностях.

Результати аналізу показують, що росія активно застосовує принципи когнітивної війни, у якій інформаційний вплив поєднується зі штучним інтелектом, великими даними, соціальною інженерією та психологічними операціями. Саме тому традиційні методи оцінювання загроз, такі як якість каналів комунікації, кількість інформаційних атак, спостереження за інформаційними трендами, вже не дають змоги формувати повну картину загроз. У сучасних умовах найбільш прийнятним підходом для пріоритезації загроз є ризик-орієнтована модель із використанням багатокритеріального оцінювання (MCDM), де інтегруються методи MAI та багатокритеріального оцінювання. Такий підхід одночасно враховує думки експертів, статистичні дані, контекстні чинники, швидкість розвитку подій та інтенсивність інформаційних впливів. Він дозволяє оперативно оновлювати пріоритети загроз відповідно до змін на фронті, у внутрішньополітичній та міжнародній площині, а також моделювати сценарії їхнього розвитку.

Шляхи протидії найбільш небезпечним когнітивним загрозам мають поєднувати технологічні, організаційні та соціально-психологічні інструменти, формуючи багаторівневу систему стійкості. Одним із ключових напрямів є розвиток інституційної спроможності стратегічних комунікацій, зокрема розширення аналітичних центрів, підсилення системи моніторингу, удосконалення процедур швидкого реагування та міжвідомчої координації. Не менш важливим є запровадження автоматизованих систем виявлення інформаційних атак, включно з детекторами дезінформації та дипфейків, що використовують машинне навчання.

У протидії персоналізованим інформаційним атакам особливу роль відіграє психологічна стійкість особового складу, яка забезпечується системною підготовкою, регулярними тренінгами, впровадженням етичного та адаптивного лідерства, розвитком внутрішніх каналів комунікації та забезпеченням контрольованого інформаційного середовища на рівні підрозділів. Паралельно необхідно підсилювати оперативну інформаційну підтримку бойових дій, створювати конкурентні інформаційні наративи, розвивати партнерську взаємодію з медіа, аналітичними центрами та міжнародними структурами НАТО й ЄС.

Серед рекомендацій варто виділити потребу у створенні динамічної доктринальної моделі, що забезпечуватиме адаптацію стратегічних комунікацій до нових типів когнітивних

загроз; формування багаторівневої системи оцінювання загроз із використанням алгоритмів MCDM; інтеграцію AHP / TOPSIS у процеси планування операцій; систематичне проведення аудиту інформаційного простору, а також побудову комплексної системи освітньої підготовки фахівців зі стратегічних комунікацій та інформаційної безпеки. Важливо також запровадити державно-військову систему раннього попередження про когнітивні атаки, що дозволить зменшувати потенційний вплив противника на ухвалення рішень та психологічний стан персоналу.

Отже, найбільш ефективним підходом у російсько-українській війні є інтегрована модель пріоритезації загроз, що поєднує метод аналізу ієрархій для визначення ваг критеріїв і метод вибору порядку переваг за подібністю до ідеального рішення, для побудови рангу загроз, оскільки вона відповідає особливостям сучасних інформаційних операцій, швидкості змін середовища та комплексності впливів противника. Її застосування дозволяє формувати адаптивну, науково-обґрунтовану та оперативно актуальну систему захисту стратегічних комунікацій ЗС України, забезпечуючи підвищення стійкості, керованості та ефективності інформаційної політики держави в умовах триваючої агресії.

Перспективними подальшими напрямами наукових досліджень у цій сфері є розвиток динамічних моделей пріоритезації когнітивних загроз із урахуванням мережевих характеристик інформаційного середовища, удосконалення алгоритмів автоматизованого моніторингу та класифікації загроз із використанням методів машинного навчання, а також формування інтегрованих систем підтримки рішень для стратегічних комунікацій, здатних працювати в режимі реального часу та адаптуватися до еволюції інформаційно-психологічних операцій противника.

**Рекомендації (Recommendations)**

Результати цієї статті можуть бути корисними для науковців у сфері воєнних наук, фахівців зі стратегічного планування, аналітиків сектору безпеки та оборони, а також для державних органів, які працюють над розробленням або адаптацією до когнітивних загроз системі стратегічних комунікацій ЗС України.

**Конфлікт інтересів (Conflict of Interest)**

Автори заявляють, що у них немає конфлікту інтересів.

**Використані джерела**

1. NATO Standardization Office. (2022). *AJP-10: Allied joint doctrine for strategic communications*. NATO. https://nso.nato.int/nso/
2. U.S. Department of Defense. (2022). *Joint Publication 3-13: Information operations*. https://www.jcs.mil/Doctrine/
3. U.S. Department of Defense. (2020). *Joint Publication 3-13.3: Operations security (OPSEC)*. https://www.jcs.mil/Doctrine/
4. Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The weaponization of social media*. Houghton Mifflin Harcourt.
5. Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.
6. Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war*. W. W. Norton & Company.
7. NATO Strategic Communications Centre of Excellence. (2018–2024). *Publications on disinformation, narrative warfare, and capability assessment*. https://stratcomcoe.org/

8. Helmus, T., Bodine-Baron, E., Radin, A., et al. (2018). *Russian social media influence: Understanding Russian propaganda in social media ecosystems* (RR-2237). RAND Corporation. https://www.rand.org/pubs/research_reports/RR2237.html
9. Міністерство оборони України. (2023). *Доктрина стратегічних комунікацій Збройних Сил України (ВКП 10-00(49).01)*. https://www.mil.gov.ua/
10. Kostyrev, A. G. (2021). *NATO–Ukraine strategic communications: Theory and practice*. NISS. https://niss.gov.ua/
11. NATO Strategic Communications Centre of Excellence. (2023). *AI and the future of information integrity: Detection, manipulation, and resilience*. https://stratcomcoe.org/
12. Bjola, C., & Pamment, J. (2019). *Digital diplomacy and international organisations: Autonomy, legitimacy and contestation*. Routledge.
13. Fridman, O., Kabernik, V. V., & Pearce, K. E. (2021). *Hybrid conflicts and information warfare in the post-Soviet space*. Routledge.
14. Giles, K. (2016). *Handbook of Russian information warfare*. NATO Defense College. https://www.ndc.nato.int/download/downloads.php?icode=506
15. Brantly, A. F. (2020). *Cyber and information warfare: Threats and responses*. Rowman & Littlefield.
16. European Centre of Excellence for Countering Hybrid Threats. (2019–2024). *Handbooks on disinformation, strategic foresight, and narrative manipulation*. https://www.hybridcoe.fi/
17. Banaszewska, A., & Pikulicka-Wilczewska, A. (2022). Cognitive warfare and algorithmic propaganda in the contemporary security environment. *Journal of Information Warfare, 21*(3), 1–18. https://jinfowar.com

**References**

1. NATO Standardization Office. (2022). *AJP-10: Allied joint doctrine for strategic communications*. NATO. https://nso.nato.int/nso/
2. U.S. Department of Defense. (2022). *Joint Publication 3-13: Information operations*. https://www.jcs.mil/Doctrine/
3. U.S. Department of Defense. (2020). *Joint Publication 3-13.3: Operations security (OPSEC)*. https://www.jcs.mil/Doctrine/
4. Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The weaponization of social media*. Houghton Mifflin Harcourt.
5. Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.
6. Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war*. W. W. Norton & Company.
7. NATO Strategic Communications Centre of Excellence. (2018–2024). *Publications on disinformation, narrative warfare, and capability assessment*. https://stratcomcoe.org/
8. Helmus, T., Bodine-Baron, E., Radin, A., et al. (2018). *Russian social media influence: Understanding Russian propaganda in social media ecosystems* (RR-2237). RAND Corporation. https://www.rand.org/pubs/research_reports/RR2237.html
9. Ministry of Defence of Ukraine. (2023). *Strategic Communications Doctrine of the Armed Forces of Ukraine (VKP 10-00(49).01).* https://www.mil.gov.ua/
10. Kostyrev, A. G. (2021). *NATO–Ukraine strategic communications: Theory and practice*. NISS. https://niss.gov.ua/
11. NATO Strategic Communications Centre of Excellence. (2023). *AI and the future of information integrity: Detection, manipulation, and resilience*. https://stratcomcoe.org/
12. Bjola, C., & Pamment, J. (2019). *Digital diplomacy and international organisations: Autonomy, legitimacy and contestation*. Routledge.

13. Fridman, O., Kabernik, V. V., & Pearce, K. E. (2021). *Hybrid conflicts and information warfare in the post-Soviet space*. Routledge.
14. Giles, K. (2016). *Handbook of Russian information warfare*. NATO Defense College. https://www.ndc.nato.int/download/downloads.php?icode=506
15. Brantly, A. F. (2020). *Cyber and information warfare: Threats and responses*. Rowman & Littlefield.
16. European Centre of Excellence for Countering Hybrid Threats. (2019–2024). *Handbooks on disinformation, strategic foresight, and narrative manipulation*. https://www.hybridcoe.fi/
17. Banaszewska, A., & Pikulicka-Wilczewska, A. (2022). Cognitive warfare and algorithmic propaganda in the contemporary security environment. *Journal of Information Warfare*, *21*(3), 1–18. https://jinfowar.com

## On the Prioritisation of Cognitive Threats to the Strategic Communications System of the Armed Forces of Ukraine under Wartime Conditions

**Oleksandr Kin**
PhD in Technical Sciences, Associate Professor
Hennadii Udovenko Diplomatic Academy of Ukraine
under the Ministry of Foreign Affairs
01001, Velyka Zhytomyrska Street, Kyiv, Ukraine
e-mail: cubalibre1972@ukr.net
ORCID: 0009-0001-2196-7515

**Oleh Nechaiev**
First Deputy Commander
of the Special Operations Forces of the Armed Forces of Ukraine
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl Avenue, 28 B, Kyiv, Ukraine
e-mail: o26811650@gmail.com
ORCID: 0009-0001-2839-2830

**Oleh Temnyi**
Doctoral candidate of the Department of Information Warfare,
Institute of Strategic Communications
National Defence University of Ukraine
03049, Povitrianykh Syl Avenue, 28 B, Kyiv, Ukraine
e-mail: o.temnyi@edu.nuou.org.ua
ORCID: 0009-0009-3173-094X

**Volodymyr Rakhimov**
PhD in Military Sciences
Deputy Head of the Institute of Strategic Communications
National Defence University of Ukraine
03049, Povitrianykh Syl Avenue, 28 B, Kyiv, Ukraine
e-mail: rakhimov@edu.nuou.org.ua
ORCID: 0000-0001-9868-986X

The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 3 No. 3 (2025)

**Yaroslav Yankovyi**
Adjunct of the Department of Information Warfare
of the Institute of Strategic Communications
National Defense University of Ukraine
03049, Povitrianykh Syl Avenue, 28 B, Kyiv, Ukraine
e-mail: ya.yankovyi@gmail.com
ORCID: 0009-0007-1718-3607

**Abstract.** The Strategic Communications System of the Armed Forces of Ukraine, despite its significant development, faces a number of challenges: excessive information flows during active phases of hostilities, the complexity of synchronising communications among various actors within the security and defence sector, the rapid emergence of new destructive narratives, the widespread use of deepfake technologies, and the informational fatigue of society. Under such conditions, traditional approaches to assessing information threats — primarily based on analysing the dissemination of individual messages or sources are becoming insufficient. They do not enable the timely identification of which specific threats may have a strategic effect, which vulnerabilities require immediate response, and which may be assigned lower priority. The urgency of the problem is heightened by the fact that cognitive threats are nonlinear and often covert in nature, and their impact may accumulate gradually, producing a combined effect. Any error in assessing the significance of a particular threat creates risks for operational management, international communication, partner support, and maintaining the motivation of personnel. In these circumstances, the prioritisation of threats becomes a critically necessary process. Therefore, the development of a methodological framework for the prioritisation of cognitive threats to the Strategic Communications System of the Armed Forces of Ukraine is essential for strengthening the state's informational and psychological resilience during wartime. Such a framework will ensure an objective, systematic, and predictable assessment of impacts, enabling timely responses to dangerous threats, minimisation of the consequences of information attacks, and the preservation of strategic initiative in the cognitive domain. The main results of the article are as follows: it analyses foreign and Ukrainian experience regarding existing approaches to prioritising cognitive (information-cognitive) threats to the Strategic Communications System of the Armed Forces of Ukraine; formulates an expanded list of cognitive threats relevant to the system; and conducts the prioritisation of cognitive threats using a probability – impact approach supported by demonstrative calculations based on expert elicitation. The findings may be useful for military personnel, analysts, security specialists, scholars, and strategists engaged in protecting the information environment and responding to contemporary cognitive threats within the sphere of Ukraine's defence and military security. Promising directions for further scientific research in this field include the development of dynamic models for prioritising cognitive threats that account for the network characteristics of the information environment; the improvement of algorithms for automated monitoring and classification of threats using machine-learning methods; and the creation of integrated decision-support systems for strategic communications capable of operating in real time and adapting to the evolution of the adversary's information-psychological operations.

**Keywords:** multicriteria methods and models; armed struggle; cognitive threats; cognitive influence; cognitive challenges; cognitive pressure index; warfare technologies; Analytic Hierarchy Process (AHP); national security; Armed Forces of Ukraine; methods of warfare; transformation of armed conflicts; response to cognitive threats; cognitive threat monitoring; strategic communications system; russian-Ukrainian war.