The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 3 No. 4 (2025)

Received: *January 20, 2026* | **Revisions Requested:** - | **Revision Received:** -
Accepted: *March 5, 2026* | **Published Online:** *March 21, 2026*

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

DOI: 10.62524/msj.2025.3.4.19

Рекомендації щодо впровадження технологічних та аналітичних рішень для підвищення стійкості до когнітивних впливів в умовах російських когнітивних загроз

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

Анотація. В умовах російської агресії проти України когнітивний вимір протиборства набуває все більшого значення, оскільки противник активно використовує інформаційно-психологічні операції, дезінформацію, цифрові платформи та технології штучного інтелекту для впливу на свідомість населення, військовослужбовців і міжнародної спільноти. Такі дії спрямовані на підрив довіри до державних інституцій, дестабілізацію суспільства та зниження рівня міжнародної підтримки України. У цих умовах особливої актуальності набуває розроблення ефективних технологічних та аналітичних рішень, спрямованих на підвищення стійкості держави та суспільства до когнітивних загроз. Метою статті є розроблення рекомендацій щодо впровадження технологічних та аналітичних рішень для підвищення стійкості України до когнітивних впливів в умовах російських когнітивних загроз. Проаналізовано особливості сучасних когнітивних загроз у контексті російсько-української війни та визначено основні напрями протидії. Запропоновано комплекс рекомендацій щодо впровадження технологічних і аналітичних рішень, спрямованих на моніторинг інформаційного простору, виявлення дезінформації, прогнозування когнітивних операцій та розвиток стратегічних комунікацій. Визначено основні органи, відповідальні за реалізацію таких заходів, а також здійснено порівняльне оцінювання важливості їх упровадження в умовах війни та у разі можливого її завершення. Подальші наукові дослідження доцільно спрямувати на розроблення методичного апарату кількісного оцінювання рівня когнітивної стійкості держави, створення математичних моделей прогнозування інформаційно-когнітивних операцій та дослідження можливостей використання штучного інтелекту для автоматизованого виявлення дезінформаційних кампаній. Матеріали статті можуть бути корисними для органів державної влади, що формують політику у сфері інформаційної та національної безпеки, органів сектору безпеки і оборони України, відповідальних за протидію інформаційним та психологічним операціям противника, аналітичних центрів та наукових установ, які досліджують проблематику інформаційної та когнітивної безпеки, а також освітніх і наукових закладів під час підготовки фахівців у сфері інформаційної безпеки, стратегічних комунікацій та кібербезпеки і міжнародних партнерів України, які беруть участь у розбудові системи протидії дезінформації та гібридним загрозам.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 3 No. 4 (2025)

Ключові слова: когнітивна безпека; когнітивні загрози; інформаційна війна; дезінформація; стратегічні комунікації; медіаграмотність; штучний інтелект; моніторинг інформаційного простору; прогнозування інформаційних атак; російсько-українська війна; когнітивна стійкість; цифрові платформи; інформаційна безпека держави; аналітичні системи; міжнародне співробітництво.

Вступ (Introduction)

Широкомасштабна агресія російської федерації проти України, що розпочалася у 2014 році та набула якісно нового масштабу після вторгнення 24 лютого 2022 року, супроводжується системним застосуванням когнітивних та інформаційно-психологічних операцій, які спрямовані на підрив стійкості українського суспільства, системи державного управління та сектору безпеки і оборони. У сучасних умовах війни протистояння між державами відбувається не лише у фізичному чи кіберпросторі, а й у когнітивному просторі, де об'єктом впливу стають сприйняття, цінності, поведінка та рішення людей. Саме тому російська агресія проти України характеризується широким використанням інформаційних, психологічних та когнітивних інструментів, що є ключовим елементом так званої гібридної війни [1–17].

З початку агресії росія системно застосовує комплекс технологічних когнітивних загроз, серед яких ключовими є: масовані кампанії з дезінформації та пропаганди; використання соціальних мереж, бот-мереж і тролів для формування штучних інформаційних наративів; маніпуляція інформаційним порядком денним через медіа та онлайн-платформи; поширення психологічних операцій, спрямованих на деморалізацію населення та військових; використання цифрових платформ, месенджерів і алгоритмів для масштабування пропаганди; формування хибних наративів для міжнародної аудиторії з метою підриву підтримки України.

Дослідження показують, що під час війни значну роль у поширенні російських наративів відіграють бот-мережі та координовані інформаційні кампанії, які здатні швидко масштабувати пропаганду та охоплювати мільйони користувачів соціальних мереж.

Розкриємо перебіг еволюції російських когнітивних впливів у період 2014–2021 років.

У період початку російської агресії (2014–2015 рр.) основний акцент робився на формуванні інформаційних наративів, спрямованих на легітимацію агресії та дестабілізацію України. Серед ключових інструментів: масована пропаганда через російські телевізійні канали; створення та поширення наративів "громадянської війни" в Україні; інформаційна підтримка сепаратистських рухів; активне використання "п'ятої колони" та маніпуляції громадською думкою.

У 2016–2021 роках відбулося поступове технологічне ускладнення інформаційно-когнітивних операцій. росія активно перейшла до використання цифрових платформ, соціальних мереж, інформаційних агентів впливу та алгоритмічних механізмів поширення дезінформації. У цей період зросла роль таргетованих кампаній у соціальних мережах, маніпуляцій політичними процесами та інформаційних атак на міжнародну аудиторію.

Розглянемо процес трансформації когнітивних загроз після 2022 року.

Після початку широкомасштабного вторгнення росії у 2022 році когнітивні операції набули системного та технологічно складного характеру. Дослідження показують, що російські дезінформаційні кампанії стали більш адаптивними, швидко реагують на події на фронті та активно використовують цифрові платформи для формування нових інформаційних наративів. Еволюція когнітивних впливів у період широкомасштабної війни може бути умовно представлена таким чином [1–5]:

2022 рік. Початок масштабних інформаційних операцій, спрямованих на: створення паніки та деморалізацію населення; поширення фейків щодо капітуляції України; дискредитацію військово-політичного керівництва держави; формування міжнародних

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 3 No. 4 (2025)

наративів про “необхідність переговорів”.

2023 рік. Розширення цифрових інструментів впливу, зокрема: масове використання бот-мереж у соціальних мережах; активізація інформаційних кампаній у глобальному інформаційному просторі; поширення маніпуляцій щодо контрнаступу та втрат України.

2024 рік. Поява нових технологічних інструментів когнітивного впливу: використання штучного інтелекту для створення фейкового контенту; застосування deepfake-технологій; посилення впливу через закриті цифрові платформи та месенджери.

2025–2026 роки. Формування комплексних когнітивних кампаній, що поєднують: інформаційні, кібернетичні та психологічні операції; автоматизовані системи поширення пропаганди; таргетовані кампанії проти військових, волонтерів та міжнародних партнерів України.

Таким чином, сучасна війна демонструє якісну трансформацію інформаційно-психологічного протиборства у когнітивну війну, де основною метою є вплив на свідомість, поведінку та стратегічні рішення суспільства, політичного керівництва і військових структур. У цих умовах особливої важливості набуває розроблення технологічних та аналітичних рішень, які дозволяють: виявляти когнітивні загрози у цифровому просторі; прогнозувати інформаційні операції противника; підвищувати стійкість державних інституцій та суспільства до дезінформації; забезпечувати ефективну протидію когнітивним операціям противника. Отже, в умовах тривалої війни росії проти України, постійного вдосконалення технологій інформаційного впливу та переходу конфлікту у когнітивний вимір розроблення рекомендацій щодо впровадження технологічних та аналітичних рішень для підвищення стійкості до когнітивних впливів є надзвичайно актуальним науковим і практичним завданням, яке безпосередньо пов’язане із забезпеченням національної та воєнної безпеки держави. Актуальність дослідження зумовлена зростанням масштабів і технологічної складності російських когнітивних операцій, що спрямовані на підрив стійкості українського суспільства та системи оборони, а також нагальною потребою у створенні ефективних технологічних та аналітичних механізмів протидії таким загрозам у сучасних умовах війни.

Матеріали та методи (Materials and Methods)

Проблематика когнітивної війни та когнітивних загроз у сучасних конфліктах набула особливої актуальності після початку російської агресії проти України. У наукових дослідженнях останніх років [1–18] активно розглядаються питання трансформації інформаційної війни у когнітивне протиборство, де об’єктом впливу стають сприйняття, переконання та поведінка суспільства. Значну кількість робіт присвячено аналізу російських інформаційних операцій, технологій поширення дезінформації, використанню цифрових платформ для маніпулювання громадською думкою, а також формуванню концепції когнітивної безпеки. У зарубіжній науковій літературі [2–6], [8], [10], [12], [18] дослідження когнітивної війни переважно здійснюється у межах безпекових студій, інформаційної безпеки та стратегічних комунікацій. Наприклад, у дослідженні “Cognitive warfare and the logic of power” [6] зазначається, що когнітивні операції розглядаються як некінетичний інструмент збільшення стратегічної сили держави, який дозволяє змінювати стратегічне середовище без прямого застосування військової сили. Автор підкреслює, що маніпуляція наративами через соціальні мережі, державні медіа та дезінформацію є ключовим інструментом російської стратегії впливу у російсько-українській війні. Інші дослідження акцентують увагу на технологічних аспектах поширення пропаганди [2–5], [10], [18]. Так, аналіз російської пропаганди у соціальних мережах показав, що значну роль у поширенні дезінформації відіграють автоматизовані акаунти. За результатами дослідження, близько 20% акаунтів, що поширювали проросійські повідомлення, були ботами, які значно посилювали охоплення пропагандистського контенту. У дослідженні, присвяченому аналізу маніпулятивних

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 3 No. 4 (2025)

наративів у когнітивній війні, доведено, що російські інформаційні кампанії активно експлуатують когнітивні упередження людей, зокрема страх, емоційні реакції та ефект підтвердження, з метою підриву довіри до державних інституцій.

У значній частині сучасних досліджень також ідеться про використання штучного інтелекту та алгоритмічних технологій в інформаційних операціях [1–2], [11], [13]. Науковці зазначають, що нові цифрові технології здатні суттєво масштабувати інформаційні операції та автоматизувати виробництво пропагандистського контенту.

Окремий напрям досліджень пов'язаний із використанням OSINT та технологій перевірки інформації для протидії дезінформації [3], [14]. У наукових роботах підкреслюється, що застосування інструментів геолокації, аналізу метаданих та архівів інтернет-контенту дозволяє ефективно виявляти фейкові повідомлення та інформаційні маніпуляції у війні. Таким чином, іноземні дослідження формують комплексне уявлення про когнітивну війну як поєднання інформаційних, психологічних та технологічних інструментів, що використовуються для впливу на свідомість людей та формування стратегічних рішень суспільства.

Українські наукові дослідження [1], [7], [9], [11], [15] здебільшого зосереджені на аналізі російської інформаційної агресії, інформаційно-психологічних операцій та когнітивної безпеки держави. У дослідженні А. Тараненко [17] розглядається концепція когнітивної безпеки як складової національної безпеки, що набуває особливого значення в умовах російської агресії проти України. Автор підкреслює, що когнітивна безпека пов'язана із захистом суспільства від маніпулятивних впливів, які можуть змінювати поведінку громадян та підривати довіру до державних інституцій. У роботах вітчизняних дослідників також підкреслюється, що сучасні конфлікти відбуваються одночасно у кількох просторах – фізичному, інформаційному, медійному та цифровому, а когнітивні операції спрямовані на руйнування суспільної єдності, дискредитацію державних інституцій та формування наративів поразки або безнадійності. Українські дослідники також приділяють увагу генезису інформаційно-когнітивної війни та її еволюції в умовах російсько-українського конфлікту, розглядаючи її як складову гібридної війни та глобальних інформаційних процесів. Крім того, у сучасних дослідженнях здійснюється аналіз технологій когнітивної війни, зокрема алгоритмічних механізмів поширення інформації, цифрових платформ, бот-мереж та інструментів інформаційного впливу.

Аналіз сучасних досліджень дає можливість визначити кілька ключових особливостей дослідження когнітивних загроз у контексті України:

по-перше – це реальний бойовий досвід когнітивної війни. Україна є однією з небагатьох держав, що перебувають у стані війни, – вона фактично перебуває у стані масштабної когнітивної війни з росією, що створює унікальний емпіричний матеріал для дослідження;

по-друге – це поєднання інформаційної, психологічної та кібернетичної складових. російські когнітивні операції здійснюються одночасно через медіа, соціальні мережі, кібероперації та дипломатичні канали;

по-третє – це масове використання цифрових платформ. Соціальні мережі, месенджери та онлайн-медіа стали ключовим середовищем поширення дезінформації та маніпуляцій;

по-четверте – це орієнтація на різні аудиторії. російські інформаційні кампанії спрямовані не лише на українське населення, а й на міжнародну аудиторію з метою зниження підтримки України.

Попри значну кількість досліджень, аналіз сучасної наукової літератури свідчить про наявність низки проблемних питань, які залишаються недостатньо дослідженими.

1. *Недосконалість комплексних методик оцінювання когнітивних загроз.* Більшість досліджень описує явище когнітивної війни на концептуальному рівні, однак методик кількісного вимірювання когнітивних впливів практично немає.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 3 No. 4 (2025)

2. *Недостатня інтеграція технологічних та аналітичних підходів.* Наукові роботи здебільшого аналізують інформаційні операції з позицій соціальних наук, тоді як поєднання аналітики даних, штучного інтелекту та когнітивних наук лише починає розвиватися.

3. *Відсутність моделей прогнозування когнітивних операцій.* Сучасні дослідження здебільшого аналізують вже проведені інформаційні кампанії, але інструменти прогнозування когнітивних атак майже не розроблено.

4. *Недостатнє дослідження військового виміру когнітивної війни.* Більшість досліджень зосереджено на медіа-просторі та політичних комунікаціях, тоді як когнітивні операції у військовому управлінні, бойових операціях та морально-психологічному забезпеченні військ досліджено значно менше.

5. *Обмежена адаптація західних концепцій до українських реалій.* Багато концепцій когнітивної війни сформовані у межах досліджень НАТО або західних університетів і не завжди враховують специфіку російсько-української війни, яка характеризується поєднанням традиційних бойових дій та масштабних інформаційних операцій.

Таким чином, аналіз сучасних наукових досліджень виявив, що проблематика когнітивної війни та когнітивних загроз активно розвивається як у зарубіжній, так і в українській науковій літературі. Дослідники приділяють значну увагу аналізу інформаційних операцій, дезінформації, маніпулятивних наративів та технологій їх поширення.

Водночас, є низка важливих аспектів, які залишаються недостатньо дослідженими, зокрема методики оцінювання когнітивних загроз, аналітичні системи виявлення когнітивних операцій, моделі прогнозування інформаційних атак та практичні механізми підвищення стійкості держави до когнітивних впливів.

Саме ці наукові прогалини визначають необхідність подальших досліджень та розроблення технологічних і аналітичних рішень для підвищення стійкості до когнітивних впливів, що є особливо актуальним в умовах тривалої російської агресії проти України.

Results (Результати)

Сучасна російсько-українська війна демонструє, що поряд із традиційними військовими операціями дедалі більшого значення набуває когнітивний вимір протиборства, у межах якого основною метою противника є вплив на сприйняття, переконання та поведінку населення, військовослужбовців і політичного керівництва держави. російська федерація активно застосовує інформаційно-психологічні операції, дезінформацію, маніпулятивні наративи, технології штучного інтелекту, бот-мережі, а також алгоритмічні механізми поширення інформації для формування необхідного інформаційного середовища.

У цих умовах підвищення стійкості держави до когнітивних впливів потребує системного впровадження технологічних та аналітичних рішень, які дозволяють своєчасно виявляти, аналізувати та нейтралізувати когнітивні операції противника.

На основі аналізу сучасних загроз та міжнародного досвіду доцільно визначити кілька ключових напрямів впровадження відповідних рішень (рис. 1).

1. *Створення національної системи моніторингу когнітивного простору.* Одним із ключових елементів протидії когнітивним загрозам є створення інтегрованої системи моніторингу інформаційного та когнітивного середовища. Така система має забезпечувати постійний аналіз інформаційних потоків у соціальних мережах, медіа, цифрових платформах та інших інформаційних каналах з метою своєчасного виявлення дезінформаційних кампаній та маніпулятивних наративів.

Основними елементами такої системи можуть бути: автоматизовані системи аналізу великих даних (Big Data); алгоритми машинного навчання для виявлення бот-мереж; системи аналізу інформаційних наративів; інструменти раннього попередження про інформаційні атаки.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 3 No. 4 (2025)

Основні виконавці: Рада національної безпеки і оборони України; Служба безпеки України; Міністерство оборони України; Міністерство цифрової трансформації України; аналітичні центри та наукові установи.



Рисунок 1. Модель взаємозв'язку технологічних рішень, інституцій впровадження та результатів підвищення когнітивної стійкості держави

2. *Використання технологій штучного інтелекту для виявлення дезінформації.* З огляду на зростання обсягів інформації у цифровому середовищі, ефективна протидія дезінформації неможлива без використання технологій штучного інтелекту. Алгоритми машинного навчання здатні автоматично виявляти фейкові новини, маніпулятивні повідомлення та координовані інформаційні кампанії.

До основних технологічних рішень належать: системи автоматичного аналізу текстів та медіаконтенту; інструменти виявлення deepfake-контенту; системи аналізу інформаційних мереж та поширення наративів; алгоритми визначення координованої поведінки у соціальних мережах.

Основні виконавці: Міністерство цифрової трансформації України; Сили безпеки і оборони України; науково-дослідні установи; IT-компанії та стартапи у сфері штучного інтелекту.

3. *Формування системи аналітичної підтримки ухвалення рішень.* Ефективна протидія когнітивним операціям потребує створення системи аналітичної підтримки управлінських рішень. Такі системи повинні забезпечувати комплексний аналіз інформаційного середовища та прогнозування можливих інформаційних операцій противника.

Основними функціями таких систем мають бути: моделювання сценаріїв інформаційних атак; прогнозування розвитку інформаційних кампаній; оцінювання впливу дезінформації на суспільство; підтримка стратегічних комунікацій держави.

Основні виконавці: Рада національної безпеки і оборони України; Генеральний штаб Збройних Сил України; урядові аналітичні центри; наукові установи сектору безпеки і оборони.

4. *Розвиток системи стратегічних комунікацій держави.* Ефективна протидія когнітивним загрозам неможлива без активної комунікаційної політики держави. Система стратегічних комунікацій повинна забезпечувати формування достовірного інформаційного

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 3 No. 4 (2025)

середовища та оперативне реагування на інформаційні атаки противника.

Основними заходами у цьому напрямі є: координація інформаційної політики державних органів; оперативне спростування дезінформації; формування позитивних національних наративів; посилення міжнародних інформаційних кампаній на підтримку України.

Основні виконавці: Кабінет Міністрів України; Міністерство культури та інформаційної політики; Міністерство закордонних справ України; Центр стратегічних комунікацій та інформаційної безпеки.

5. *Підвищення когнітивної стійкості суспільства.* Одним із ключових елементів протидії когнітивним загрозам є формування високого рівня критичного мислення та медіаграмотності населення.

Основними заходами роботи у цьому напрямі є: впровадження програм медіаграмотності у систему освіти; проведення інформаційно-просвітницьких кампаній; розвиток громадських ініціатив із протидії дезінформації.

Основні виконавці: Міністерство освіти і науки України; громадські організації; наукові установи; міжнародні партнери.

З огляду на поточні умови війни та можливі сценарії її завершення, доцільно оцінити пріоритетність впровадження запропонованих рішень щодо підвищення когнітивної стійкості суспільства у короткостроковій та середньостроковій перспективі з урахуванням триваючої війни та у разі її можливого закінчення (табл. 1).

Таблиця 1. Щодо пріоритетності впровадження запропонованих рішень стосовно підвищення когнітивної стійкості суспільства

Напрям	Під час війни	Після можливого завершення війни
Система моніторингу когнітивного простору	критично важлива	дуже важлива
Технології штучного інтелекту для аналізу дезінформації	критично важлива	дуже важлива
Аналітичні системи прогнозування інформаційних атак	дуже важлива	критично важлива
Система стратегічних комунікацій	критично важлива	важлива
Підвищення медіаграмотності населення	важлива	критично важлива

Під час війни першочергового значення набувають технологічні системи оперативного виявлення інформаційних атак, тоді як у довгостроковій перспективі ключову роль відіграватиме підвищення когнітивної стійкості суспільства та розвиток аналітичних інструментів прогнозування загроз.

Таким чином, ефективна протидія російським когнітивним загрозам потребує комплексного підходу, який поєднує технологічні, аналітичні та організаційні інструменти. Запропоновані рекомендації дозволяють сформувати цілісну систему підвищення когнітивної стійкості держави, що охоплює як технологічні механізми моніторингу інформаційного середовища, так і заходи щодо формування критичного мислення у суспільстві. Упровадження таких рішень сприятиме підвищенню ефективності протидії інформаційним операціям противника, зміцненню національної безпеки та формуванню стійкого інформаційного середовища в Україні як у період війни, так і у післявоєнний період. З метою визначення пріоритетності впровадження запропонованих рекомендацій щодо підвищення когнітивної стійкості України було проведено експертне оцінювання їх практичної важливості. Оцінювання здійснювалося за десятибальною шкалою, де 1 бал відповідає мінімальній важливості, а 10 балів – максимально критичній важливості для забезпечення національної

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 3 No. 4 (2025)

безпеки. Результати узагальненого експертного опитування дали змогу визначити порівняну значущість кожного блоку рекомендацій та провести їх порівняльне оцінювання у відсотковому вимірі. Узагальнені результати оцінювання подано у табл. 2.

Таблиця 2. Практична оцінка важливості впровадження рекомендацій щодо підвищення когнітивної стійкості України (методом експертного опитування)

№	Блок рекомендацій	Основний зміст заходів	Основні відповідальні органи	Очікуваний результат	Оцінка важливості (1–10)
1	Національна система моніторингу когнітивного простору	Створення інтегрованих платформ аналізу медіа, соцмереж, месенджерів, виявлення інформаційних атак	РНБО, СБУ, Міноборони, Мінцифри	Раннє виявлення інформаційних операцій противника	10
2	Використання штучного інтелекту для виявлення дезінформації	AI-аналіз інформаційних потоків, виявлення бот-мереж, deepfake, координації інформаційних кампаній	Мінцифри, СБУ, аналітичні центри, IT-сектор	Автоматизоване виявлення дезінформаційних кампаній	9
3	Аналітичні системи прогнозування когнітивних операцій	Моделювання інформаційних атак, аналіз наративів, прогнозування інформаційних кампаній	РНБО, Генеральний штаб ЗСУ, наукові установи	Прогнозування та запобігання інформаційним операціям	8
4	Розвиток системи стратегічних комунікацій держави	Координація державної інформаційної політики, оперативне спростування дезінформації	Кабінет Міністрів, МКІП, МЗС	Формування стійкого інформаційного середовища	9
5	Підвищення медіаграмотності населення	Освітні програми, навчання критичному мисленню, просвітницькі кампанії	МОН, громадські організації, медіа	Підвищення стійкості суспільства до маніпуляцій	8
6	Інтеграція міжнародних систем протидії дезінформації	Обмін даними з партнерами, інтеграція з системами ЄС і НАТО	МЗС, РНБО, міжнародні партнери	Підвищення ефективності міжнародної протидії пропаганді	7
7	Формування єдиної державної системи когнітивної безпеки	Інституційна координація усіх структур протидії когнітивним загрозам	РНБО, Кабінет Міністрів, сектор безпеки і оборони	Системна протидія когнітивним операціям	10

Аналіз результатів експертного оцінювання свідчить про високий рівень важливості більшості запропонованих напрямів підвищення когнітивної стійкості держави (рис. 2). Найвищі оцінки – 10 балів, що відповідає 100% максимальної важливості, – отримали два напрями: створення національної системи моніторингу когнітивного простору та формування єдиної державної системи когнітивної безпеки. Це свідчить про те, що експерти розглядають ці заходи як базові елементи інституційного та технологічного забезпечення протидії когнітивним загрозам, без яких неможливе ефективне функціонування всієї системи захисту інформаційного середовища держави. Дещо нижчі, але також високі показники отримали використання технологій штучного інтелекту для виявлення дезінформації та розвиток

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 3 No. 4 (2025)

системи стратегічних комунікацій держави, які були оцінені у 9 балів (90% максимальної важливості). Це підкреслює значення сучасних цифрових технологій та ефективної інформаційної політики держави для своєчасного виявлення та нейтралізації інформаційних атак противника. Середній рівень пріоритетності отримали аналітичні системи прогнозування когнітивних операцій та заходи з підвищення медіаграмотності населення, які отримали 8 балів (80% максимальної важливості). Експерти відзначили, що ці напрями мають важливе стратегічне значення для формування довгострокової стійкості суспільства до інформаційних маніпуляцій, хоча їхній ефект здебільшого проявляється у середньостроковій та довгостроковій перспективі. Найнижчу оцінку серед представлених напрямів отримала інтеграція міжнародних систем протидії дезінформації, яка була оцінена у 7 балів (70% максимальної важливості). Попри порівняно нижчий показник, цей напрям також залишається важливим елементом протидії когнітивним загрозам, оскільки забезпечує обмін інформацією з міжнародними партнерами та доступ до сучасних технологічних рішень у сфері боротьби з дезінформацією. Узагальнюючи результати експертного оцінювання, можна відзначити, що середнє значення важливості всіх запропонованих заходів становить близько 8,7 бала, або 87% від максимально можливого рівня, що підтверджує високий рівень актуальності впровадження комплексної системи підвищення когнітивної стійкості України. Порівняльний аналіз отриманих результатів показує, що першочергового значення набувають інституційні та технологічні механізми моніторингу інформаційного простору та координації державної політики у сфері когнітивної безпеки, тоді як освітні та міжнародні напрями є важливими доповнювальними елементами формування стійкості суспільства до інформаційних впливів.

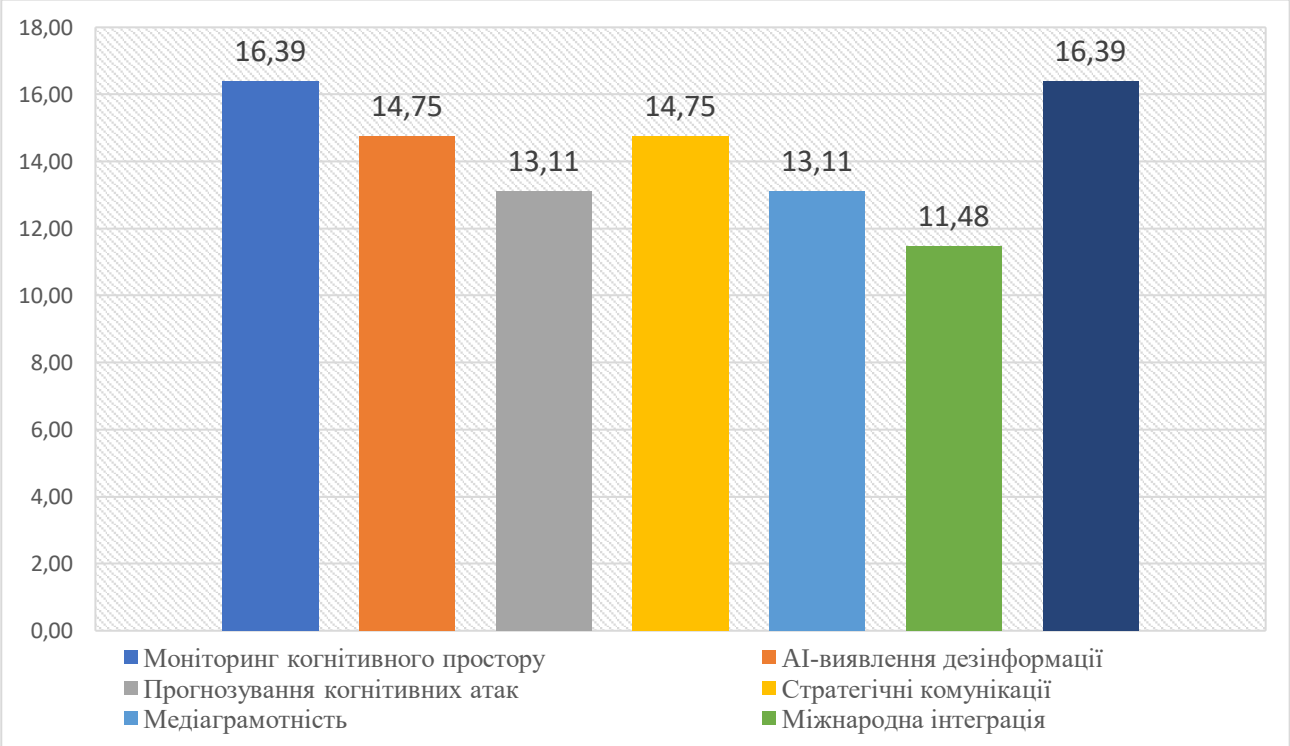


Рисунок 2. Оцінка пріоритетності рекомендацій щодо підвищення когнітивної стійкості України (методом експертного опитування)

Висновок (Conclusion)

Проведене дослідження дозволило узагальнити сучасні підходи до протидії когнітивним

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 3 No. 4 (2025)

загрозам у контексті російсько-української війни та сформувати практичні рекомендації щодо впровадження технологічних і аналітичних рішень, спрямованих на підвищення стійкості держави та суспільства до інформаційно-когнітивних впливів.

Встановлено, що сучасний етап російської агресії характеризується системним застосуванням когнітивних операцій, які реалізуються через інформаційні, психологічні, технологічні та соціальні механізми впливу. Основною метою таких операцій є формування необхідного інформаційного середовища, маніпулювання суспільною свідомістю, підрив довіри до державних інституцій, деморалізація цивільного населення та військовослужбовців, а також зниження рівня міжнародної підтримки України.

Аналіз сучасних технологічних тенденцій показав, що російські когнітивні операції активно використовують цифрові платформи, соціальні мережі, бот-мережі, алгоритмічні механізми поширення інформації, а також інструменти штучного інтелекту для створення маніпулятивного інформаційного контенту. У зв'язку із цим протидія таким загрозам потребує комплексного поєднання технологічних, аналітичних та організаційних механізмів.

У статті обґрунтовано доцільність формування системного підходу до підвищення когнітивної стійкості держави, який передбачає впровадження таких ключових напрямів: створення національної системи моніторингу когнітивного простору, використання технологій штучного інтелекту для виявлення дезінформації, розвиток аналітичних систем прогнозування когнітивних операцій, посилення стратегічних комунікацій держави, а також підвищення рівня медіаграмотності та критичного мислення населення.

Запропоновані рекомендації передбачають чітке визначення основних суб'єктів їх реалізації, серед яких ключову роль відіграють органи сектору безпеки і оборони України, центральні органи виконавчої влади, науково-дослідні установи, аналітичні центри, IT-сектор та міжнародні партнери України. Такий підхід дозволяє сформувати інтегровану систему протидії когнітивним загрозам, здатну ефективно функціонувати як у період активної фази війни, так і у післявоєнний період.

Порівняльне оцінювання важливості впровадження запропонованих рекомендацій свідчить про те, що в умовах війни першочергового значення набувають технологічні системи моніторингу інформаційного простору, автоматизовані інструменти виявлення дезінформації та механізми стратегічних комунікацій. У довгостроковій перспективі, зокрема у разі можливого завершення активної фази війни, ключову роль відіграватиме розвиток систем прогнозування інформаційних загроз, формування інституційної системи когнітивної безпеки та підвищення когнітивної стійкості суспільства.

Результати дослідження переконують у тому, що впровадження запропонованих технологічних і аналітичних рішень здатне значно підвищити ефективність протидії інформаційним операціям противника, забезпечити своєчасне виявлення когнітивних атак та зміцнити інформаційну і когнітивну стійкість держави.

Подальші наукові дослідження доцільно спрямувати на: розроблення методичного апарату кількісного оцінювання рівня когнітивної стійкості держави; створення математичних моделей прогнозування інформаційно-когнітивних операцій; дослідження можливостей використання штучного інтелекту для автоматизованого виявлення дезінформаційних кампаній; розроблення інтегрованих аналітичних платформ для моніторингу інформаційного середовища; дослідження впливу когнітивних операцій на процеси військового управління та морально-психологічний стан військ.

Таким чином, запропоновані у статті рекомендації та аналітичні підходи можуть бути використані як теоретична та практична основа для формування ефективної системи підвищення когнітивної стійкості України в умовах сучасних безпекових викликів.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 3 No. 4 (2025)

Рекомендації (Recommendations)

Матеріали статті можуть бути корисними для: органів державної влади, що формують політику у сфері інформаційної та національної безпеки; органів сектору безпеки і оборони України, відповідальних за протидію інформаційним та психологічним операціям противника; аналітичних центрів та наукових установ, які досліджують проблематику інформаційної та когнітивної безпеки; освітніх і наукових закладів під час підготовки фахівців у сфері інформаційної безпеки, стратегічних комунікацій та кібербезпеки; міжнародних партнерів України, які беруть участь у розбудові системи протидії дезінформації та гібридним загрозам.

Конфлікт інтересів (Conflict of Interest)

Автори заявляють, що у них немає конкуруючих інтересів за тематикою статті.

Використані джерела

1. Pomerantsev, P. (2022). *Information war and the Russian invasion of Ukraine*. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/information-war-and-the-russian-invasion-of-ukraine/
2. Singer, P. W., & Brooking, E. (2018). *LikeWar: The weaponization of social media*. Houghton Mifflin Harcourt. https://www.hmhbooks.com/shop/books/LikeWar/9781328695740
3. Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux. https://us.macmillan.com/books/9780374287268/activemeasures
4. Helmus, T., Bodine-Baron, E., & Radin, A. (2018). *Russia's hostile measures in Europe: Understanding Russian influence operations*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR2539.html
5. Atlantic Council. (2023). *Undermining Ukraine: How Russia widened its global information war in 2023*. https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023/
6. NATO Innovation Hub. (2021). *Cognitive warfare*. NATO Allied Command Transformation. https://www.innovationhub-act.org/sites/default/files/2021-01/20210122_CW%20Final.pdf
7. Баранов, О. А. (2020). Когнітивна безпека держави як складова національної безпеки. *Стратегічні пріоритети, 2*, 43–52. https://niss.gov.ua/sites/default/files/2020-06/strateg-priority-2-2020.pdf
8. Benkler, Y., Faris, R., & Roberts, H. (2018). *Network propaganda: Manipulation, disinformation, and radicalization in American politics*. Oxford University Press. https://global.oup.com/academic/product/network-propaganda-9780190923623
9. Дубов, Д. В. (2017). *Інформаційна безпека України в умовах гібридної війни*. НІСД. https://niss.gov.ua/sites/default/files/2017-05/InfoSecurity_Dubov.pdf
10. Rid, T. (2013). *Cyber war will not take place*. Oxford University Press. https://global.oup.com/academic/product/cyber-war-will-not-take-place-9780199330637
11. Почепцов, Г. Г. (2015). *Інформаційні війни: новий інструмент політики*. Києво-Могилянська академія. https://ekmair.ukma.edu.ua/items/2f77e0f7-4a41-4e4e-bdf4-7a8f7c9b96e5
12. Zuboff, S. (2019). *The age of surveillance capitalism*. PublicAffairs. https://www.publicaffairsbooks.com/titles/shoshana-zuboff/the-age-of-surveillance-capitalism/9781610395694/
13. Ліпкан, В. А. (2016). *Інформаційна безпека України*. КНТ. https://elar.naiau.kiev.ua/handle/123456789/17063
14. European Union Institute for Security Studies. (2022). *Cognitive warfare: The new battlefield*. https://www.iss.europa.eu/content/cognitive-warfare-new-battlefield
15. Горбулін, В. П. (2017). *Світова гібридна війна: український фронт*. НІСД. https://niss.gov.ua/sites/default/files/2017-02/Gorbulin_hybrid_war.pdf

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 3 No. 4 (2025)

16. Segal, A. (2016). *The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age*. PublicAffairs. https://www.publicaffairsbooks.com/titles/adam-segal/the-hacked-world-order/9781610394161/
17. Тараненко, А. О. (2021). Когнітивна безпека як новий вимір інформаційної безпеки держави. *Інформація і право, 3* (38), 95–103. https://doi.org/10.37750/2616-6798.2021.3(38).244528
18. Schmidt, E., & Cohen, J. (2013). *The new digital age: Transforming nations, businesses, and our lives*. Knopf. https://www.penguinrandomhouse.com/books/310766/the-new-digital-age-by-eric-schmidt-and-jared-cohen/

References

1. Pomerantsev, P. (2022). *Information war and the Russian invasion of Ukraine*. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/information-war-and-the-russian-invasion-of-ukraine/
2. Singer, P. W., & Brooking, E. (2018). *LikeWar: The weaponization of social media*. Houghton Mifflin Harcourt. https://www.hmhbooks.com/shop/books/LikeWar/9781328695740
3. Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux. https://us.macmillan.com/books/9780374287268/activemeasures
4. Helmus, T., Bodine-Baron, E., & Radin, A. (2018). *Russia's hostile measures in Europe: Understanding Russian influence operations*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR2539.html
5. Atlantic Council. (2023). *Undermining Ukraine: How Russia widened its global information war in 2023*. https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023/
6. NATO Innovation Hub. (2021). *Cognitive warfare*. NATO Allied Command Transformation. https://www.innovationhub-act.org/sites/default/files/2021-01/20210122_CW%20Final.pdf
7. Baranov, O. A. (2020). *Cognitive security of the state as a component of national security*. *Strategic Priorities, 2*, 43–52. https://niss.gov.ua/sites/default/files/2020-06/strateg-priority-2-2020.pdf
8. Benkler, Y., Faris, R., & Roberts, H. (2018). *Network propaganda: Manipulation, disinformation, and radicalization in American politics*. Oxford University Press. https://global.oup.com/academic/product/network-propaganda-9780190923623
9. Dubov, D. V. (2017). *Information security of Ukraine in conditions of hybrid war*. NISS. https://niss.gov.ua/sites/default/files/2017-05/InfoSecurity_Dubov.pdf
10. Rid, T. (2013). *Cyber war will not take place*. Oxford University Press. https://global.oup.com/academic/product/cyber-war-will-not-take-place-9780199330637
11. Pocheptsov, G. G. (2015). *Information wars: A new instrument of politics*. Kyiv-Mohyla Academy. https://ekmair.ukma.edu.ua/items/2f77e0f7-4a41-4e4e-bdf4-7a8f7c9b96e5
12. Zuboff, S. (2019). *The age of surveillance capitalism*. PublicAffairs. https://www.publicaffairsbooks.com/titles/shoshana-zuboff/the-age-of-surveillance-capitalism/9781610395694/
13. Lipkan, V. A. (2016). *Information security of Ukraine*. KNT. https://elar.naiau.kiev.ua/handle/123456789/17063
14. European Union Institute for Security Studies. (2022). *Cognitive warfare: The new battlefield*. https://www.iss.europa.eu/content/cognitive-warfare-new-battlefield
15. Horbulin, V. P. (2017). *World hybrid war: The Ukrainian front*. NISS. https://niss.gov.ua/sites/default/files/2017-02/Gorbulin_hybrid_war.pdf
16. Segal, A. (2016). *The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age*. PublicAffairs. https://www.publicaffairsbooks.com/titles/adam-segal/the-hacked-world-order/9781610394161/

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 3 No. 4 (2025)

17. Taranenko, A. O. (2021). *Cognitive security as a new dimension of state information security*. *Information and Law, 3* (38), 95–103. https://doi.org/10.37750/2616-6798.2021.3(38).244528
18. Schmidt, E., & Cohen, J. (2013). *The new digital age: Transforming nations, businesses, and our lives*. Knopf. https://www.penguinrandomhouse.com/books/310766/the-new-digital-age-by-eric-schmidt-and-jared-cohen/

Recommendations for implementing technological and analytical solutions to increase resilience to cognitive influences in the face of Russian cognitive threats

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

Abstract. In the context of Russian aggression against Ukraine, the cognitive dimension of the confrontation is becoming increasingly important, as the enemy is actively using information and psychological operations, disinformation, digital platforms and artificial intelligence technologies to influence the consciousness of the population, military personnel and the international community. Such actions are aimed at undermining trust in state institutions, destabilizing society and reducing the level of international support for Ukraine. In these conditions, the development of effective technological and analytical solutions aimed at increasing the resilience of the state and society to cognitive threats is of particular relevance. The purpose of the article is to develop recommendations for the implementation of technological and analytical solutions to increase Ukraine's resilience to cognitive influences in the context of Russian cognitive threats. The article analyzes the features of modern cognitive threats in the context of the Russian-Ukrainian war and identifies the main directions for countering them. A set of recommendations is proposed for the implementation of technological and analytical solutions aimed at monitoring the information space, detecting disinformation, forecasting cognitive operations and developing strategic communications. The main bodies responsible for the implementation of such measures are identified, and a comparative assessment of the importance of their implementation in war conditions and in the event of its possible termination is also carried out. Further scientific research should be directed at developing a methodological apparatus for quantitatively assessing the level of cognitive stability of the state, creating mathematical models for forecasting information and cognitive operations and studying the possibilities of using artificial intelligence for automated detection of disinformation campaigns. The materials of the article may be useful for state authorities that form policy in the field of information and national security, security and defense sector bodies of Ukraine responsible for countering information and psychological operations of the enemy, analytical centers and scientific institutions that study the issues of information and cognitive security, as well as educational and scientific institutions during the training of specialists in the field of information security, strategic communications and cybersecurity, and international partners of Ukraine that participate in the development of a system for countering disinformation and hybrid threats.

Keywords: cognitive security; cognitive threats; information warfare; disinformation; strategic communications; media literacy; artificial intelligence; monitoring of the information space; forecasting information attacks; Russian-Ukrainian war; cognitive resilience; digital platforms; information security of the state; analytical systems; international cooperation.