Громадська Наталя Анатоліївна
Мизь Максим Дмитрович

Інформаційна війна в контексті національної безпеки України: загрози та виклики

УДК 323.23:[002.1:355.01(477)]]
DOI https://doi.org/10.24195/2414-9616.2025-5.5

Громадська Наталя Анатоліївна
кандидат політичних наук,
доцент кафедри журналістики
та політології
Чорноморського національного
університету імені Петра Могили
вул. 68 Десантників, 10, Миколаїв,
Україна
ORCID: 0000-0002-2310-3489

Мизь Максим Дмитрович
магістрант спеціальності «Політологія»
Чорноморського національного
університету імені Петра Могили
вул. 68 Десантників, 10, Миколаїв,
Україна
ORCID: 0009-0006-9964-7761

У статті розглядається феномен інформаційної війни в контексті національної безпеки України, її загрози та виклики. У сучасному глобалізованому світі інформаційна сфера стала стратегічним простором для реалізації політичних, економічних та військових цілей держав. Інформаційна війна перетворилася на потужний інструмент дестабілізації національної безпеки, оскільки дозволяє впливати на громадську думку, формувати суспільні настрої, змінювати політичні пріоритети та послаблювати державні інституції без прямого застосування фізичної сили. Актуальність проблеми зумовлена зростанням масштабів інформаційних загроз у сучасному світі, що стають невід'ємними складовими гібридних конфліктів. Особливо ця проблема стосується України, яка зазнає системного інформаційного впливу. Метою дослідження є аналіз сутності та специфіки інформаційної війни, визначення її впливу на систему національної безпеки України, окреслення основних загроз і викликів, а також розробка пропозицій щодо механізмів протидії. У роботі було використано метод бібліографічного аналізу літератури, аналіз, синтез, узагальнення, порівняльний та аналітичний метод. У результаті дослідження встановлено, що інформаційна війна є багатовимірним явищем, яке охоплює політичну, соціальну, економічну та культурну сфери суспільства. Вона здатна провокувати внутрішні конфлікти, підривати довіру до державних інституцій, дезорієнтувати суспільство та створювати сприятливі умови для зовнішнього впливу. Аналіз таких інструментів, як дезінформація, пропаганда, кібератаки та психологічні операції, дозволяє розкрити їхню багатовекторну спрямованість на підрив суспільної свідомості та руйнування критичної інфраструктури. Наведені можливі способи протидії інформаційним загрозам знижують можливість дестабілізації національної безпеки країни.
Ключові слова: *інформаційна війна, національна безпека, інформаційна безпека, інструменти інформаційної війни.*

Вступ. У сучасних військово-політичних реаліях важко заперечувати роль інформації в якості інструменту протистояння, що по суті є зброєю, яка може критично впливати як на перебіг війни, так й на політичний простір. На тлі становлення інформаційного суспільства та стрімкого розвитку технологій, явище інформаційної війни стало частіше згадуватися як в наукових дискурсах, так й в мас-медіа, а також серед населення. Актуальність вивчення загроз та викликів інформаційної війни в контексті національної безпеки є особливо гострою для України. Країна, яка протягом десятиліть після здобуття незалежності не виробила достатнього імунітету до гібридних інформаційних загроз, стала об'єктом агресії з боку Росії. В сучасних інформаційних війнах активно використовуються цифрові платформи, ЗМІ та соціальні мережі для створення дезінформаційного простору, спрямованого на дискредитацію уряду, формування паніки та маніпуляції суспільною думкою. З іншої сторони, відповіддю на це, є формування системи інформаційної безпеки, яка повинна протистояти викликам та загрозам.

Метою дослідження є аналіз сутності та специфіки інформаційної війни, визначення її впливу на систему національної безпеки України, окреслення основних загроз і викликів, а також розробка пропозицій щодо механізмів протидії.

Завдання дослідження:

– розкрити сутність понять «інформаційна війна», «національна безпека» та «інформаційна безпека»;

– визначити основні форми та інструменти ведення інформаційної війни;

– розглянути внутрішні та зовнішні загрози інформаційній безпеці держави;

– проаналізувати вплив інформаційної війни на систему національної безпеки України;

– окреслити ключові загрози та виклики, що постають перед державою в умовах інформаційної агресії;

– запропонувати можливі напрями та механізми підвищення ефективності інформаційної безпеки держави.

Методи дослідження. У роботі було використано метод бібліографічного аналізу літератури (для загальної характеристики стану інформаційної безпеки України), аналіз, синтез та узагальнення (для характеристики основних уявлень про інформаційну безпеку та інформаційні війни); порівняльний метод (для аналізу основних теоретичних підходів до розуміння суті поняття «інформаційна війна»); аналітичний метод (при характеристиці існуючих загальних уявлень про інструменти та методи ведення інформаційної війни).

Результати. Національна безпека є фундаментальною категорією, що визначає стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів від реальних та потенційних загроз. Наприклад, закон «Про національну безпеку», підписаний президентом США Г. Труменом у 1947 році, трактує національну безпеку як об'єднання аспектів внутрішньої, зовнішньої та військової політики з метою формування збалансованого підходу до вирішення питання про застосування Сполученими Штатами різноманітних інструментів – як військових, так і невійськових – у зовнішній політиці для захисту власної безпеки. Відтак, у цьому визначенні сутності національної безпеки акцент робиться на зовнішніх діях США [8, с. 80]. Згідно зі статтею 1 Закону України «Про національну безпеку України», загрози визначаються як «явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України» [4]. А в статті 17 Конституції України згадується, що «захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави». Тому складовою національної безпеки можна визнати інформаційну безпеку [6].

Інформаційна безпека визначається захистом ключових інтересів індивіда, суспільства та держави від ризиків в інформаційному середовищі. У Сполучених Штатах та державах Європейського Союзу під цим терміном розуміють рівень захисту інформації та інформаційних мереж від несанкціонованого втручання, експлуатації, змін, обмеження доступу, руйнування, пошкодження цілісності тощо. В Україні застосовують ширше тлумачення, що охоплює, зокрема, аспекти політичної безпеки, пов'язані з роботою медійного простору [5]. В чинній стратегії інформаційної безпеки України, окрім питання захисту інформації, зазначається й «…існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій...» [12].

Таким чином, інформаційна безпека є ключовою складовою національної безпеки, що забезпечує захист від загроз та реагування на виклики в інформаційному просторі.

Наразі термін «інформаційна війна» має переважно публіцистичне забарвлення і ще не набув сталого визначення. Це підтверджують постійні дискусії стосовно справжнього змісту цього поняття, а також дебати щодо його коректності та практичної корисності.

Вперше поняття «інформаційна війна» застосував Т. Рон у доповіді «Системи озброєння та інформаційна війна», яку він підготував у 1976 році. У документі було наголошено, що інформаційна інфраструктура становить основний елемент американської економіки, водночас перетворюючись на потенційно вразливу ціль як у період війни, так і в мирний час [9, с. 77].

Серед поглядів дослідників, які займаються питаннями інформаційних війн, можна виділити декілька підходів до цього визначення, деякі з яких можна представити наступним чином [9, с. 78–81]:

– перший – психологічний підхід, який розглядає інформаційну війну як прихований вплив інформації на свідомість окремих людей, груп і мас у цілому за допомогою пропаганди, дезінформації та маніпуляцій, спрямований на формування нових уявлень про соціально-політичний устрій суспільства через зміну ціннісних орієнтацій та базових переконань особистості;

– другий – геополітичний підхід, що трактує інформаційну війну як міждержавне протиборство, спрямоване на досягнення зовнішньополітичних цілей не через фізичну силу, військову техніку або зброю, а за допомогою витончених технологій примусового контролю, що зовні проявляються у дипломатичних формах;

– третій – соціально-комунікативний підхід, який розуміє інформаційну війну як комунікаційну технологію, що спрямована на здобуття інформаційної переваги в рамках національної стратегії, де ключову роль відіграє інформація, яка впливає на когнітивні орієнтації.

– четвертий – системний підхід, де інформаційну війну розглядають як динамічний процес, що протікає в складній самоорганізованій системі з великою кількістю елементів, взаємозв'язки між якими мають імовірнісний, а не детермінований характер.

Також існують поняття, які акцентують увагу на військовому протистоянні, де інформаційна війна є частиною загальних військових заходів.

Крім того, привертає увагу дослідження П. Шпиги та Р. Рудника, в якому виділяються чотири підходи до тлумачення цього поняття [13, с. 328].

Інформаційна війна може включати такі дії: збір тактичної інформації, перевірку її достовірності, поширення пропаганди та дезінформації з метою деморалізації або маніпулювання опонентом і громадськістю, підрив якості інформації опонента та обмеження його здатності збирати дані. Можна побачити, що інформаційна війна ведеться як на ворожий суб'єкт (державу, групу тощо), так і населення [7, с. 239].

Таким чином, інформаційна війна націлена на ослаблення моральних і матеріальних (інформаційних) ресурсів супротивника та посилення власних через пропагандистський та технічний вплив.

Таблиця 1

Підходи до «інформаційної війни» П. Шпиги та Р. Рудника

Підхід	Опис
Перший	Інформаційна війна як комплекс політико-правових, соціально-економічних і психологічних дій, спрямованих на контроль інформаційного простору, усунення противника, руйнування його комунікацій та обмеження доступу до засобів передачі повідомлень.
Другий	Найгостріша форма протистояння в інформаційному просторі, де ключовими є безкомпромісність, висока інтенсивність суперечки та короткі періоди активного конфлікту.
Третій	Інформаційна війна як спосіб підтримки військових дій через сучасні електронні засоби, такі як цифрові випромінювачі, супутникові передавачі та інші технології.
Четвертий	Інформаційна війна ототожнюється з кібернетичною війною, тобто протистоянням між технічними системами.

Джерело: сформовано автором на основі [13]

На відміну від збройних конфліктів, інформаційна війна не спричиняє безпосередніх руйнувань або жертв, проте наслідки таких воєн у сфері психології особистості та суспільства можуть перевищувати ефекти від реальних бойових дій.

Наглядними для розуміння є окреслені національні загрози та виклики в Стратегії інформаційної безпеки України, які безпосередньо стосуються небезпеки інформаційних війн для держави [12]:

– інформаційне домінування держави-агресора на тимчасово окупованих територіях України;

– обмежені можливості реагувати на дезінформаційні кампанії;

– несформованість системи стратегічних комунікацій;

– недосконалість регулювання відносин у сфері інформаційної діяльності та захисту професійної діяльності журналістів;

– спроби маніпуляції свідомістю громадян України щодо європейської та євроатлантичної інтеграції України;

– недостатній рівень інформаційної культури та медіаграмотності в суспільстві для протидії маніпулятивним та інформаційним впливам.

Вищезгадані загрози вказують на те, що для України явище інформаційної війни є актуальним та критичним. Тому важливо розглянути прояви інформаційної війни в контексті агресії з боку Росії.

Певні прояви інформаційних операцій по відношенню до України можна побачити ще під час президентських виборів 2004 року, де російські медіа та політичні діячі відкрито протистояли одному кандидату (В. Ющенко) та підтримували іншого (В. Януковича). Також російські інформаційні кампанії намагалися знизити міжнародний імідж України під час «газових війн» 2005 року. Крім цього, в різні часи змінювався перелік провідних тем, таких як проблеми Чорноморського флоту, проблематика паливно-енергетичного комплексу, проблеми Криму і кримських татар, а також діяльність екстремістських політичних організацій [10, с. 19].

Окремо також потрібно виділити висвітлення російськими ЗМІ подій Євромайдану в агресивно-пропагандистському світлі, де подальші події показали вразливість українського населення до інформаційно-пропагандистських атак [11, с. 239].

Є. Магда виділяє п'ять основних методів інформаційної агресії Росії проти України до початку широкомасштабного вторгнення: дезінформацію та маніпуляції, пропаганду, перекручування громадської думки, психологічний і психотропний тиск, а також поширення чуток. [11, с 239].

Також інші дослідники виділяли (до широкомасштабного вторгнення), що Росія діяла в таких напрямках ведення інформаційної війни [10, с. 21]:

– зниження міжнародного авторитету України для послаблення її геополітичного значення;

– спотворення та фрагментування інформації з метою дестабілізації країни та впровадження «керованого хаосу»;

– створення стереотипу меншовартості українців і руйнування національної самосвідомості;

– поширення російської мови та культури для утвердження російської ідентичності при витісненні української.

Серед інструментів інформаційної війни, які використовуються донині, на нашу думку, можна відзначити такі:

– широке використання підконтрольних ЗМІ (телебачення, радіо, інтернет) для пропаганди та здійснення спрямованого інформаційно-психологічного впливу на українців з метою дезінформації, нагнітання, виправдання агресії та деморалізації патріотично налаштованих верств суспільства;

– використання методів контрінформаційної боротьби, включно з блокуванням загальнодержавних українських телеканалів і радіостанцій на окупованих територіях, а також контролем регіональних та місцевих ЗМІ;

– застосування пропагандистських підрозділів та «лідерів думок» у соціальних мережах та онлайн-платформах.

Вразливість України до інформаційних атак відмічається, з однієї сторони – несформованістю і недостатньою визначеністю системи цінностей та інтересів суспільства, а також наявністю численних протиріч між інтересами різних соціальних спільнот і професійних груп, що, з однієї сторони,

спричиняє політичну та соціальну нестабільність, а з іншої – недосконалість системи національної інформаційної безпеки [2, с. 106].

Тому для захисту та запобігання від вищеназваних загроз потрібні чіткі цілі та завдання, спрямовані на протидію таким загрозам. В Україні основою інформаційної безпеки є «Стратегія інформаційної безпеки України» від 2021 року. Цей документ чітко окреслює внутрішні та зовнішні загрози та виклики та надає план розвитку та удосконалення системи національної інформаційної безпеки [12].

Серед стратегічних цілей особливо виділяються задачі, які повинні бути направлені на підвищення медіаграмотності та забезпечення розвитку української культури, що повинно підвищити захищеність населення від ворожих інформаційно-психологічних атак.

Серед іншого, пріоритетним напрямком повинна стати присутність України в світі та підвищення її іміджу, бо, як демонструють результати опитування TNS, проведеного 3–8 вересня 2015 року у восьми країнах ЄС (Великобританія, Іспанія, Італія, Нідерланди, Німеччина, Польща, Франція, Швеція) 53% опитаних європейців вважають, що на сході України триває громадянська війна [3, с. 240]. Таким чином, для ефективного входження України до світового інформаційного простору важливо спиратися на міжнародний досвід, розвивати сучасну нормативно-правову базу, забезпечувати доступ до глобальних інформаційних ресурсів та впроваджувати світові стандарти роботи з інформацією. Не менш значущими є використання іноземних інформаційних продуктів для формування власних ресурсів, підтримка їх актуальності, розширення української присутності в глобальному середовищі, а також активна участь у міжнародних програмах і проєктах, що стосуються новітніх інформаційних технологій. Важливою умовою залишається постійний моніторинг методів інформаційного впливу, що дозволить Україні зміцнити свої позиції на світовій арені.

В цілому, на нашу думку, Україна повинна зосередитися на наступних напрямках в сфері інформаційної безпеки:

– забезпечення інформаційного суверенітету та розробка ефективних механізмів, спрямованих на розвиток українського суспільства на засадах національної гідності та з дотриманням прав і свобод громадян у інформаційній сфері;

– формування системної координаційної системи інформаційної безпеки та впорядкування інформаційної діяльності для налагодженої взаємодії органів влади з громадськістю;

– протидія загрозам та удосконалення заходів щодо нейтралізації шкідливих інформаційних впливів через наповнення медіапростору якісним контентом і підвищення інформаційної культури населення;

– гармонізація законодавства за допомогою реформування нормативно-правової бази у сфері обігу інформації з обмеженим доступом відповідно до вимог міжнародного права ЄС та НАТО;

– удосконалення кібербезпеки, що передбачає створення ефективної системи захисту кіберпростору, включаючи моніторинг загроз, захист критичної інфраструктури та розробку необхідної законодавчої бази.

Висновки. Інформаційна війна є одним із ключових інструментів гібридної агресії, що підриває політичну стабільність, маніпулює суспільною свідомістю та послаблює національну безпеку. На прикладі України показано, як інформаційна агресія може призвести до загроз різного масштабу та критичності, а також продемонстровано, наскільки важливим є один із ключових елементів національної безпеки – інформаційна безпека. Ефективна стратегія протидії інформаційним загрозам повинна бути комплексною і включати правове регулювання, кіберзахист, медіаграмотність та міжнародну співпрацю.

Особливо потрібно звертати увагу на підвищення рівня інформаційної культури населення, що дозволяє громадянам критично оцінювати отриману інформацію та розпізнавати дезінформацію, пропаганду й маніпулятивні медіатехнології. В умовах постійного інформаційного тиску саме свідоме й медіаграмотне суспільство здатне протистояти зовнішньому впливу та не ставати інструментом у руках агресора. Крім того, державі слід активно розвивати власний інформаційний простір, підтримувати незалежні медіа, удосконалювати механізми стратегічних комунікацій та забезпечувати оперативне інформування громадян. Важливою складовою є і зміцнення кіберінфраструктури, адже кібератаки нерідко поєднуються з інформаційними операціями, формуючи єдину систему гібридного впливу.

Отже, у сучасних умовах інформаційна безпека стає не лише питанням державної політики, а й фактором національної стійкості. Успішна протидія інформаційним війнам можлива лише за умови об'єднання зусиль держави, суспільства та міжнародних партнерів, адже саме інформація сьогодні є одним із головних ресурсів, що визначає безпечний розвиток держави та її майбутнє.

ЛІТЕРАТУРА:

1. Khoroshko V., Khokhlachova Y., Pirtskhalava T., Ivanchenko I. Information weapons as a tool of information warfare. Ukrainian Information Security Research Journal. 2022. Vol. 24, No 2 (Information protection). DOI: 10.18372/2410-7840.24.16930. URL: https://jrnl.nau.edu.ua/index.php/ZI/article/view/16930 (дата звернення: 22.09.2025);

2. Горулько В. В. Роль і місце інформаційної безпеки в загальній системі національної без-

пеки держави. *Вісник* Харківського національного університету імені В. Н. Каразіна, серія «Право». 2022. Вип. 34. С. 104–109. URL: https://periodicals.karazin.ua/law/article/view/21301/20766 (дата звернення: 21.09.2025).

3. Дмитренко М. А. Проблемні питання інформаційної безпеки України. Міжнародні відносини. Серія Політичні науки. 2017. № 17. С. 236–243;

4. Закон України «Про національну безпеку України» від 21.06.2018 р. *Відомості Верховної Ради України*, № 31, 241. URL: «https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text» (дата звернення: 21.09.2025);

5. Інформаційна безпека / О. В. Литвиненко // Енциклопедія Сучасної України [Електронний ресурс] / редкол. : І. М. Дзюба, А. І. Жуковський, М. Г. Железняк [та ін.] ; НАН України, НТШ. – Київ: Інститут енциклопедичних досліджень НАН України, 2011. URL: https://esu.com.ua/article-12457. (дата звернення: 22.08.2025);

6. Конституція України від 26.06.1996 р. *Відомості Верховної Ради України*, №30, 141. URL: «https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text» (дата звернення: 20.09.2025);

7. Марценко М. С. Поняття та види інформаційних війн // Матеріали VI Міжнародної науково-практичної конференції «Російсько-українська війна: право, безпека, світ» (29–30 квітня 2022 р.). – Тернопіль, 2022. URL: http://confuf.wunu.edu.ua/index.php/confuf/article/view/943 (дата звернення: 20.09.2025).

8. Національна безпека в контексті європейської інтеграції України: підручник / Г. П. Ситник, М. Г. Орел; за ред. Г. П. Ситника. Київ: Міжрегіональна Академія управління персоналом, 2021. 372 с.

9. Проноза І. І. (2018). Інформаційна війна: сутність та особливості прояву. Актуальні проблеми політики, Вип. 61, 76–84.

10. Сасин Г. В. Інформаційна війна: сутність, засоби реалізації, результати та можливості протидії (на прикладі російської експансії в український простір) / Г. В. Сасин // *Грані*. 2015. № 3. С. 18–23. URL: http://nbuv.gov.ua/UJRN/Grani_2015_3_5 (дата звернення 19.08.2025);

11. Стрільчук, Л. (2023). Інформаційна війна як складова сучасних гібридних воєн (на прикладі Грузії та України). *Літопис Волині*, (28), 235–239. URL: https://doi.org/10.32782/2305-9389/2023.28.33 (дата звернення 18.08.2025);

12. Указ Президента України №685/2021 «Про рішення Ради національної безпеки і оборони України від 15 жовтня 20121 року «Про Стратегії інформаційної безпеки». URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення 18.08.2025);

13. Шпига П. С., Рудник Р. М. Основні технології та закономірності інформаційної війни. Проблеми міжнародних відносин. 2014. Вип. 8. С. 326-339.

REFERENCES:

1. Khoroshko V., Khokhlachova Y., Pirtskhalava T., Ivanchenko I. (2022). Informacijna zbroja jak instrument informacijnoji vijny [Information weapons as a tool of information warfare]. *Ukrainian Information Security Research Journal* (electronic journal), vol. 24, no. 2 pp. 50–58. DOI: 10.18372/2410-7840.24.16930. Retrieved from: https://jrnl.nau.edu.ua/index.php/ZI/article/view/16930 [in Ukrainian].

2. Horulko V. V. (2022). Rolj i misce informacijnoji bezpeky v zaghaljnij systemi nacionaljnoji bezpeky derzhavy [The role and place of information security in the overall system of national security of the state]. *Visnyk Kharkivsjkogho nacionaljnogho universytetu imeni V. N. Karazina, serija «Pravo»* [Bulletin of V. N. Karazin Kharkiv National University, series «Law»] (electronic journal), vol. 34, pp. 104–109. Retrieved from: https://periodicals.karazin.ua/law/article/view/21301/20766 [in Ukrainian].

3. Dmytrenko M. A. (2017). Problemni pytannja informacijnoji bezpeky Ukrajiny [Problematic issues of information security in Ukraine]. *Mizhnarodni vidnosyny, serija Politychni nauky*, №17, pp. 236–243 [in Ukrainian].

4. Verkhovna Rada Ukrainy (2018). Zakon Ukrainy «Pro natsionalnu bezpeku Ukrainy» vid 21.06.2018 roku [Law of Ukraine «On National Security of Ukraine» dated 21.06.2018.]. Retrieved from: «https://zakon.rada.gov.ua/laws/show/254k/96-vr#Text» [in Ukrainian].

5. Lytvynenko O. V. (2011). Informatsiina bezpeka [Information security]. *Encyklopedija Suchasnoji Ukrajiny*. Retrieved from: https://esu.com.ua/article-12457.

6. Verkhovna Rada Ukrainy (1996). Konstytutsiia Ukrainy vid 26.06.1996 roku [Constitution of Ukraine of June 26, 1996]. Retrieved from: https://zakon.rada.gov.ua/laws/show/254k/96-vr#Text [in Ukrainian].

7. Martsenko M. S. (2022). Ponjattja ta vydy informacijnykh vijn [Concept and types of information warfare]. *Proceedings of the Mizhnarodnoji naukovo-praktychnoji konferenciji «Rosijsjko-ukrajinsjka vijna: pravo, bezpeka, svit»* (Ukraine, Ternopil, April 29–30 2022), Ternopil pp. 239-242. Retrieved from: http://confuf.wunu.edu.ua/index.php/confuf/article/view/943 [in Ukrainian].

8. Sytnyk H. P., Orel M. H. (2021). Natsionalna bezpeka v konteksti yevropeiskoi intehratsii Ukrainy [National security in the context of Ukraine's European integration]. Kyiv: *Mizhreghionaljna Akademija upravlinnja personalom*, 372 p. [in Ukrainian].

9. Pronoza I. I. (2018). Informacijna vijna: sutnistj ta osoblyvosti projavu [Information warfare: essence and features of manifestation]. *Aktualjni problemy polityky* [Current problems of politics] (electronic journal), vol. 61, pp. 76–84. Retrieved from: http://app.nuoua.od.ua/archive/61_2018/9.pdf [in Ukrainian].

10. Sasyn H. V. (2015). Informacijna vijna: sutnistj, zasoby realizaciji, rezuljtaty ta mozhlyvosti protydiji (na prykladi rosijsjkoji ekspansiji v ukrajinsjkyj prostir) [Information warfare: essence, means of implementation, results and possibilities of counteraction (using the example of Russian expansion into Ukrainian space)]. *Hrani*, № 3. pp. 18–23. Retrieved from: http://nbuv.gov.ua/UJRN/Grani_2015_3_5 [in Ukrainian].

11. Strilchuk L. (2023). Informacijna vijna jak skladova suchasnykh ghibrydnykh vojen (na prykladi Ghruziji ta Ukrajiny) [Information warfare as a component of modern hybrid wars (using the example of Georgia and Ukraine)]. *Litopys Volyni*, (28), pp. 235–239. Retrieved from: https://doi.org/10.32782/2305-9389/2023.28.33 [in Ukrainian].

12. Prezydent Ukrainy (2021). Ukaz Prezydenta Ukrainy № 685/2021 «Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku «Pro Stratehii informatsiinoi bezpeky» [Decree of the President of Ukraine No. 685/2021 "On the Decision of the National Security and Defense Council of Ukraine of October 15, 20121 «On Information Security Strategies»]. Retrieved from: https://zakon.rada.gov.ua/laws/show/685/2021#Text [in Ukrainian].

13. Shpyha P. S., Rudnyk R. M. (2014) Osnovni tekhnolohii ta zakonomirnosti informatsiinoi viiny [Basic technologies and patterns of information warfare]. *Problemy mizhnarodnykh vidnosyn*, vol. 8, pp. 326–339. [in Ukrainian].

Information warfare in the context of Ukraine's national security: threats and challenges

Hromadska Natalia Anatoliivna

PhD in Political Science,
Associate Professor at the Department of Journalism and Political Sciences
Petro Mohyla Black Sea National University
68 Desantnykiv str., 10, Mykolaiv, Ukraine
ORCID: 0000-0002-2310-3489

Myz Maksym Dmytrovych

Master's Student in Political Science
Petro Mohyla Black Sea National University
68 Desantnykiv str., 10, Mykolaiv, Ukraine
ORCID: 0009-0006-9964-7761

The article examines the phenomenon of information warfare in the context of Ukraine's national security, its threats, and challenges. In today's globalized world, the information sphere has become a strategic domain for achieving political, economic, and military objectives of states. Information warfare has evolved into a powerful tool for destabilizing national security, as it allows influencing public opinion, shaping social attitudes, altering political priorities, and weakening state institutions without the direct use of physical force. The relevance of this issue is determined by the growing scale of information threats in the modern world, which have become integral components of hybrid conflicts. This problem is particularly significant for Ukraine, which is subject to systemic information influence.

The purpose of the study is to analyze the essence and specific features of information warfare, to determine its impact on Ukraine's national security system, to outline the main threats and challenges, and to develop proposals for counteraction mechanisms. The research employed methods of bibliographic literature analysis, analysis, synthesis, generalization, as well as comparative and analytical methods.

The results of the study show that information warfare is a multidimensional phenomenon encompassing the political, social, economic, and cultural spheres of society. It can provoke internal conflicts, undermine trust in state institutions, disorient society, and create favorable conditions for external influence. The analysis of such tools as disinformation, propaganda, cyberattacks, and psychological operations reveals their multidirectional impact aimed at undermining public consciousness and destroying critical infrastructure. The proposed ways of counteracting information threats help reduce the likelihood of destabilization of the country's national security.

Key words: *information warfare, national security, information security, instruments of information warfare.*

Дата першого надходження рукопису до видання: 21.10.2025
Дата прийнятого до друку рукопису після рецензування: 18.11.2025
Дата публікації: 15.12.2025