УДК 351:004.738.5:316.77
JEL D83, F52, L86
DOI: https://doi.org/10.32782/2617-5940.1.2026.1

Дамір Бікулов
доктор наук з державного управління, професор,
професор кафедри менеджменту,
Запорізький національний університет
ORCID: https://orcid.org/0000-0001-9188-7310
E-mail: elcoronelnotiene1974@gmail.com

ІНСТРУМЕНТИ ІНФОРМАЦІЙНОЇ ПРОТИДІЇ В УМОВАХ РОСІЙСЬКОГО ВТОРГНЕННЯ

Анотація. *У статті здійснено комплексне дослідження сучасних механізмів інформаційної протидії в умовах повномасштабного воєнного конфлікту та трансформації цифрового інформаційного середовища. Основний акцент зроблено на виявленні ефективних інструментів нейтралізації дезінформації та підвищення стійкості суспільства до інформаційних впливів в умовах гібридної війни. Методологічною основою дослідження виступає системний підхід, що дозволяє розглядати інформаційний простір як комплексну динамічну систему. У роботі використано методи контент-аналізу цифрових платформ, порівняльного аналізу функціонування соціальних мереж і месенджерів, а також елементи інституційного та структурно-функціонального аналізу. Застосування зазначених методів дало змогу ідентифікувати ключові канали поширення дезінформації та оцінити їх вплив на суспільну свідомість. Установлено, що Російська Федерація активно використовує соціальні мережі, месенджери та цифрові платформи як інструменти ведення інформаційної війни. Визначено основні механізми впливу, зокрема функціонування анонімних каналів, використання бот-мереж, алгоритмічне просування контенту та залучення локальних агентів впливу. Доведено, що ефективність дезінформаційних кампаній значною мірою залежить від використання емоційних факторів, таких як страх, тривожність і невизначеність. Також проаналізовано обмеження доступу до цифрових платформ у Росії як інструмент централізації інформаційного контролю та визначено потенціал використання цих процесів для зворотного інформаційного впливу. Наукова новизна роботи полягає у систематизації сучасних інструментів інформаційної протидії та визначенні їх ефективності в умовах гібридних загроз. Практична цінність дослідження полягає у розробці рекомендацій щодо вдосконалення державного регулювання цифрового середовища, підвищення рівня цифрової грамотності населення та формування стійкої інформаційної політики. Отримані результати можуть бути використані при формуванні національних стратегій інформаційної безпеки та розробці практичних заходів протидії дезінформації.*

Ключові слова: *інформаційна війна, дезінформація, соціальні мережі, Telegram, державне регулювання, інформаційна безпека.*

Damir Bikulov
Doctor of Science in Public Administration, Professor,
Professor of the Department of Management,
Zaporizhzhia National University
ORCID: https://orcid.org/0000-0001-9188-7310
E-mail: elcoronelnotiene1974@gmail.com

TOOLS OF INFORMATION COUNTERACTION IN THE CONDITIONS OF RUSSIAN INVASION

Abstract. *The article provides a comprehensive study of modern mechanisms of information counteraction in the context of a full-scale military conflict and the transformation of the digital information environment. The main focus is on identifying effective tools for neutralizing disinformation and increasing the resilience of society to information influence under conditions of hybrid warfare. The methodological basis of the study is a systemic approach, which allows considering the information space as a complex dynamic system. The research applies methods of content analysis of digital platforms, comparative analysis of social networks and messaging applications, as well as elements of institutional and structural-functional analysis. The use of these methods made it possible to identify key channels of disinformation dissemination and assess their impact on public consciousness. It has been established that the Russian Federation actively uses social networks, messaging applications, and digital platforms as instruments of information warfare. The main mechanisms of influence include the operation of anonymous channels, the use of bot networks, algorithmic promotion of content, and the involvement of local actors. It is proved that the effectiveness of disinformation campaigns largely depends on the use of emotional factors such as fear, anxiety, and uncertainty. The study also analyzes the restriction of access to digital platforms in Russia as a tool of centralized information control and determines the potential for using these processes for reverse information influence. The scientific novelty of the study lies in the systematization of modern tools of information counteraction and the determination of their effectiveness under hybrid threats. The practical value consists in developing recommendations for improving state regulation of the digital environment, enhancing digital literacy, and forming a resilient information policy. The results can be used in the development of national information security strategies and practical measures to counter disinformation.*

Keywords: *information warfare, disinformation, social media, Telegram, regulation, cybersecurity.*

Вступ. В умовах повномасштабного вторгнення Російської Федерації інформаційний простір став одним із ключових театрів бойових дій. Сучасні цифрові технології дозволяють здійснювати масовий вплив на суспільну свідомість, формувати панічні настрої, підривати довіру до державних інституцій ініціювати та координувати деструктивну діяльність. Якщо 10–15 років потому акцент інформаційного впливу на суспільство був сконцентрований на телебаченні, зараз існує великий прошарок громадян, які його ігнорують. Саме такі громадяни є переважно рушійною силою більшості суспільних процесів. Особливу роль у цьому відіграють популярні соціальні мережі та месенджери, зокрема Telegram і WhatsApp, які використовуються як інструменти поширення дезінформації та пропаганди. Існує необхідність протидії в українському інформаційному просторі, включаючи тематичні локальні його підрозділи.

Літературний огляд. Питання інформаційної безпеки та протидії дезінформації досліджувалися в роботах українських і зарубіжних науковців, зокрема у сфері гібридних загроз, кібербезпеки та стратегічних комунікацій. Разом з тим, в умовах повномасштабної війни зростає потреба у дослідженні нових інструментів інформаційного впливу, які базуються на використанні цифрових платформ і алгоритмів поширення контенту. Проблематика інформаційної війни, дезінформації та стратегічних комунікацій активно досліджується українськими та зарубіжними науковцями в контексті гібридних загроз і цифровізації суспільства.

Серед українських дослідників вагомий внесок у розвиток теорії інформаційної безпеки зробив В. Горбулін, який обґрунтовує концепцію гібридної війни як комплексного поєднання військових, інформаційних та економічних інструментів впливу [1]. Г. Почепцов розглядає інформаційні війни як системний інструмент управління масовою свідомістю через наративи, символи та медіа, підкреслюючи роль соціальних мереж у поширенні дезінформації [2].

О. Литвиненко акцентує увагу на необхідності формування державної інформаційної політики та розвитку стратегічних комунікацій як ключового інструменту протидії зовнішнім інформаційним загрозам [3]. У дослідженнях Н. Карпчук та О. Дубаса розглядаються механізми функціонування інформаційних операцій у цифровому середовищі та роль новітніх медіа у формуванні громадської думки [4].

Сучасні українські дослідження також приділяють значну увагу впливу соціальних мереж і месенджерів. Зокрема, в роботах О. Кучмія доведено, що Telegram та інші цифрові платформи стали ключовими каналами інформаційно-психологічного впливу, які дозволяють масштабувати дезінформацію та маніпулювати суспільними настроями [5].

Серед зарубіжних науковців значний внесок у дослідження інформаційного суспільства зробив М. Кастельс, який розглядає владу як функцію контролю над інформаційними потоками в мережевому суспільстві [6]. Дослідження F. Splidsboel Hansen доводять, що російська федерація використовує дезінформацію як системний інструмент гібридної війни, спрямований на підрив демократичних інститутів [7].

Аналітичні матеріали NATO Strategic Communications Centre of Excellence підтверджують, що інформаційні операції є невід'ємною частиною сучасних військових стратегій, а соціальні мережі використовуються як платформи для координації інформаційного впливу [8]. Європейська служба зовнішніх дій у межах проєкту EUvsDisinfo задокументувала тисячі випадків поширення проросійської дезінформації, що свідчить про системний характер таких кампаній [9].

Крім того, сучасні емпіричні дослідження демонструють значний рівень автоматизації інформаційних операцій. Зокрема, дослідження Bradshaw та Howard показують, що бот-мережі відіграють ключову роль у поширенні політичної пропаганди та можуть формувати штучний інформаційний порядок денний і відповідні соціальні установки [10].

Таким чином, аналіз сучасних досліджень свідчить про високий рівень наукового опрацювання проблематики інформаційної війни, однак актуальним залишається питання розробки практичних інструментів протидії дезінформації в умовах повномасштабного вторгнення та адаптації державної політики до нових цифрових викликів ворога.

Метою статті є дослідження механізмів інформаційного впливу Російської Федерації та розробка інструментів ефективної інформаційної протидії в Україні.

Методологія. У дослідженні використано методи системного аналізу, контент-аналізу соціальних мереж, порівняльного аналізу, а також елементи інституційного підходу.

Основна частина. Російська інформаційна кампанія, яка передувала повномасштабному вторгненню та продовжується в умовах війни, базується на комплексі взаємопов'язаних механізмів інформаційного впливу, спрямованих на формування необхідних соціально-психологічних установок у суспільстві [3; 4]. Основною метою таких дій є дестабілізація інформаційного простору, зниження довіри до державних інституцій та формування викривленої картини реальності.

Одним із ключових інструментів є анонімні Telegram-канали, що дозволяють створювати розгалужені мережі без чіткої ідентифікації джерела інформації [5]. Такі канали активно використовуються для поширення фейкових повідомлень, маніпуляцій суспільною думкою, а також для здійснення оперативної комунікації між різними елементами інформаційної інфраструктури. Крім того, Telegram застосовується як інструмент вербування агентів, координації дій, збору розвідувальної інформації та організації підривної діяльності [2; 7].

З березня–квітня 2026 року в Російській Федерації почали спостерігатися тенденції до обмеження доступу до глобальних месенджерів, зокрема Telegram, що пов'язано з прагненням держави централізувати інформаційні потоки та посилити контроль над цифровим середовищем [6]. Натомість активно впроваджуються внутрішні цифрові платформи (VK, Max), функціонування яких повністю контролюється державними структурами.

Другим за важливістю інструментом інформаційного впливу є ботоферми – спеціалізовані програмні комплекси, що забезпечують масове розповсюдження однотипних повідомлень з метою створення ефекту «суспільної підтримки» або «суспільного невдоволення» [7]. Такі механізми активно використовуються в соціальних мережах, під час голосувань та в інформаційних кампаніях.

Важливу роль відіграють також агенти впливу – реальні особи (блогери, псевдоексперти, медіа), які ретранслюють необхідні наративи та формують громадську думку [4]. Особливістю їх діяльності є використання фрагментарної інформації та емоційного контенту, що базується на страху, паніці та невизначеності [8]. Саме емоційний компонент значною мірою підвищує ефективність інформаційних операцій.

Окремим напрямом є здійснення кібероперацій та хакерських атак на цифрову інфраструктуру України та країн-союзників, що призводить до втрати інформації, порушення роботи інформаційних систем та створення додаткового психологічного тиску на населення [2; 9].

Водночас варто відзначити, що ефективність зазначених інформаційних стратегій змінюється з часом. На початковому етапі війни вони демонстрували високий рівень впливу, що підтверджується значною підтримкою агресивної політики всередині Росії та активністю інформаційних агентів у глобальному інформаційному просторі. Проте на 4–5 рік війни спостерігається поступове зниження їх ефективності, що пов'язано зі зростанням рівня критичного мислення, інформаційної обізнаності та цифрової грамотності населення [10].

Важливим аспектом є державне регулювання цифрового середовища. Показовим є досвід Китайської Народної Республіки, де функціонує система «Великий китайський файрвол» (Great Firewall), яка забезпечує комплексний контроль інформаційних потоків [11]. Ця система поєднує технічні (DNS-блокування, DPI, фільтрація трафіку), правові та адміністративні механізми впливу, що дозволяє державі ефективно контролювати цифровий простір.

В Україні регулювання інформаційного середовища здійснюється такими органами, як Національна рада з питань телебачення і радіомовлення, Служба безпеки України, кіберполіція та Міністерство цифрової трансформації [1;2]. У контексті інформаційної війни актуалізується питання доцільності застосування обмежувальних заходів, зокрема блокування деструктивного контенту та співпраці з міжнародними цифровими платформами.

Альтернативним підходом до протидії інформаційним загрозам є створення якісного контенту, підвищення рівня цифрової грамотності населення та розвиток стратегічних комунікацій [10; 12]. Саме комплексне поєднання цих заходів дозволяє забезпечити ефективну інформаційну безпеку в умовах сучасних викликів.

Висновки. Інформаційна війна в сучасних умовах виступає невід'ємною складовою збройних конфліктів і набуває системного характеру, поєднуючи технологічні, соціально-психологічні та комунікаційні інструменти впливу. Проведене дослідження підтверджує, що Російська Федерація активно використовує цифрові платформи, соціальні мережі та месенджери як ключові інструменти реалізації інформаційно-психологічних операцій, спрямованих на дестабілізацію суспільства, формування викривленої картини реальності та підрив довіри до державних інституцій.

Встановлено, що ефективність інформаційного впливу забезпечується за рахунок комплексного використання анонімних каналів, бот-мереж, агентів впливу та емоційно насиченого контенту, який апелює до страху, невизначеності та соціальної напруги. Водночас динаміка інформаційного протистояння свідчить про поступове зниження результативності хаотичних інформаційних стратегій противника, що пов'язано зі зростанням рівня критичного мислення, цифрової грамотності та адаптаційних можливостей українського суспільства.

Обґрунтовано, що ефективна інформаційна протидія потребує комплексного підходу, який має поєднувати державне регулювання цифрового середовища, розвиток технологічних інструментів моніторингу та протидії дезінформації, а також системне підвищення рівня медіаграмотності населення. Важливим є баланс між заходами контролю та дотриманням демократичних принципів, зокрема свободи слова та доступу до інформації.

Особливу увагу доцільно приділити використанню вразливостей інформаційної політики противника, зокрема обмежень доступу до глобальних цифрових платформ, що створює додаткові можливості для здійснення цілеспрямованого інформаційного впливу на аудиторію в середині Російської Федерації. У цьому контексті перспективним напрямом є розвиток альтернативних каналів комунікації, використання технологій обходу обмежень та формування якісного конкурентного інформаційного контенту.

Таким чином, формування стійкої системи інформаційної безпеки потребує консолідації зусиль держави, суспільства та приватного сектору, а також постійної адаптації до нових викликів цифрового середовища. Практична реалізація запропонованих підходів сприятиме підвищенню ефективності протидії гібридним загрозам та зміцненню інформаційного суверенітету України.

Список використаних джерел:

1. Горбулін В. П. Світова гібридна війна: український фронт. Київ: НІСД, 2017. 496 с.
2. Почепцов Г. Г. Інформаційні війни. Київ: Видавничий дім «Києво-Могилянська академія», 2015. 496 с.
3. Литвиненко О. В. Інформаційна безпека України: теорія і практика. Київ: НІСД, 2014. 256 с.
4. Карпчук Н. П., Дубас О. П. Інформаційні операції в сучасному цифровому середовищі. Київ: НАДУ, 2020. 210 с.
5. Кучмій О. П. Соціальні мережі як інструмент інформаційного впливу. *Вісник інформаційної безпеки.* 2021. №3. С. 45–52.
6. Castells M. The Rise of the Network Society. Oxford: Blackwell, 2010. 597 p.
7. Splidsboel Hansen F. Russian Hybrid Warfare: A Study of Disinformation. Copenhagen: DIIS, 2017. 36 p.
8. NATO Strategic Communications Centre of Excellence. Social Media as a Tool of Hybrid Warfare. Riga, 2022. URL: https://stratcomcoe.org
9. EUvsDisinfo. Disinformation Cases Database. URL: https://euvsdisinfo.eu (дата звернення: 2026).
10. Bradshaw S., Howard P. Computational Propaganda. Oxford: Oxford University Press, 2018. 302 p.
11. Закон України «Про основні засади забезпечення кібербезпеки України» №2163-VIII від 05.10.2017.
12. Доктрина інформаційної безпеки України: Указ Президента України №47/2017 від 25.02.2017.

References:

1. Horbulin V. P. (2017). Svitova hibrydna viina: ukrainskyi front [World hybrid war: Ukrainian front]. Kyiv: NISS.
2. Pocheptsov H. H. (2015). Informatsiini viiny [Information wars]. Kyiv: Kyiv-Mohyla Academy Publishing House.
3. Lytvynenko O. V. (2014). Informatsiina bezpeka Ukrainy: teoriia i praktyka [Information security of Ukraine: theory and practice]. Kyiv: NISS.
4. Karpchuk N. P. & Dubas O. P. (2020). Informatsiini operatsii v suchasnomu tsyfrovomu seredovyshchi [Information operations in the modern digital environment]. Kyiv: NADU.
5. Kuchmii O. P. (2021). Social media as a tool of information influence. *Visnyk informatsiinoi bezpeky,* no. 3, pp. 45–52.
6. Castells M. (2010). The rise of the network society. Oxford: Blackwell.
7. Splidsboel Hansen F. (2017). Russian hybrid warfare: A study of disinformation. Copenhagen: DIIS.
8. NATO StratCom COE. (2022). Social media as a tool of hybrid warfare. Available at: https://stratcomcoe.org
9. EUvsDisinfo. (2026). Disinformation cases database. Available at: https://euvsdisinfo.eu
10. Bradshaw S. & Howard P. (2018). Computational propaganda. Oxford: Oxford University Press.
11. Zakon Ukrainy “Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy” [Law of Ukraine on cybersecurity]. (2017).
12. Doktryna informatsiinoi bezpeky Ukrainy [Information security doctrine of Ukraine]. (2017).

Дата надходження статті: 25.03.2026
Дата прийняття статті: 15.04.2026
Дата публікації статті: 24.06.2026