УДК 351.86:316.77:323.28
DOI https://doi.org/10.32782/2312-1815/2025-22-10

Володимир Галіпчак
ORCID: 0009-0006-2501-0290

Наталія Ротар
ORCID: 0000-0002-6430-3460

ІНСТИТУЦІЙНІ ЧИННИКИ ІНФОРМАЦІЙНО-БЕЗПЕКОВОЇ ПОЛІТИКИ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ: КОНЦЕПТ ДОСЛІДЖЕННЯ

У статті розкрито концепт дослідження інституційних чинників інформаційно-безпекової політики України в умовах воєнного стану. Актуальність дослідження зумовлена посиленням інформаційних загроз у період воєнного стану та зростанням ролі інформаційної безпеки як одного з ключових чинників забезпечення національної безпеки України в умовах повномасштабної збройної агресії РФ. Проаналізовано теоретико-методологічні підходи до розуміння інформаційної безпеки як багатовимірного явища, що поєднує правові, політичні, організаційні та комунікативні компоненти. Особливу увагу приділено впливу воєнного стану на трансформацію інформаційно-безпекової політики України. Доведено, що війна стала каталізатором інституційних змін, спрямованих на підвищення стійкості інформаційного простору, розвиток стратегічних комунікацій та посилення протидії дезінформації. Водночас наголошується на необхідності дотримання балансу між безпековими імперативами та демократичними стандартами в контексті євроінтеграційного курсу України.

Зроблено висновок, що інституційні чинники не лише визначають здатність держави реагувати на актуальні інформаційні загрози, але й формують стратегічні засади інформаційно-безпекової політики в умовах воєнного стану, забезпечуючи її адаптивність та довгострокову ефективність.

Ключові слова: *інформаційна безпека, інформаційно-безпекова політика, інституційні чинники, воєнний стан, гібридна війна, національна безпека.*

Вступ. Інформаційна сфера в сучасних умовах перетворилася на один із ключових просторів протиборства між державами, політичними акторами та наддержавними утвореннями. Повномасштабна збройна агресія Російської Федерації проти України остаточно засвідчила, що інформаційна безпека більше не може розглядатися лише як допоміжний або технічний компонент національної безпеки. Вона набула стратегічного значення та стала самостійним напрямом державної політики, тісно пов'язаним із питаннями суверенітету, демократичного розвитку, стійкості суспільства й ефективності державного управління.

В умовах воєнного стану інформаційно-безпекова політика України зазнала суттєвих трансформацій. З одного боку, це пов'язано з необхідністю оперативного реагування на масовані інформаційно-психологічні операції, дезінформаційні кампанії та кібератаки з боку держави-агресора. З іншого – із потребою у збереженні балансу між безпековими імперативами та демократичними принципами функціонування публічного простору. За таких обставин особливої актуальності набуває аналіз інституційних чинників, які визначають спроможність держави формувати й реалізовувати ефективну інформаційно-безпекову політику.

Наукові дослідження у сфері інформаційної безпеки традиційно зосереджувалися на правових, технологічних або комунікаційних аспектах. Водночас інституційний вимір тривалий час залишався фрагментарно висвітленим, особливо в контексті гібридної війни

та воєнного стану. Недостатньо дослідженими залишаються питання взаємодії між органами державної влади, безпековими структурами, громадянським суспільством і міжнародними партнерами у процесі забезпечення інформаційної безпеки, а також вплив інституційних дисфункцій на ефективність відповідної політики.

Метою статті є концептуальне осмислення інституційних чинників інформаційно-безпекової політики України в умовах воєнного стану й узагальнення ключових теоретичних і практичних положень, напрацьованих у межах дисертаційного дослідження. До основних завдань належать: аналіз інституційної архітектури інформаційної безпеки; визначення ролі та функцій основних суб'єктів інформаційно-безпекової політики; окреслення специфіки інституційної взаємодії в умовах гібридної війни; формування узагальненого концепту інституційного забезпечення інформаційної безпеки держави.

Матеріал і методи дослідження. Методологічну основу дослідження становить комплекс загальнонаукових і спеціальних методів пізнання, що дали змогу всебічно проаналізувати інституційні чинники інформаційно-безпекової політики України в умовах воєнного стану. Вихідною теоретико-методологічною позицією є системний підхід, за якого інформаційна безпека розглядається як багаторівнева та динамічна підсистема національної безпеки, функціонування якої визначається взаємодією політичних, правових, інституційних і комунікативних чинників.

У процесі дослідження застосовано інституційний підхід, що дав змогу проаналізувати структуру, функції та взаємодію основних суб'єктів формування й реалізації інформаційно-безпекової політики. Особлива увага приділялася виявленню ролі державних інституцій, безпекових органів, органів публічної влади, а також недержавних акторів і міжнародних партнерів у протидії інформаційним загрозам в умовах збройної агресії.

Для осмислення трансформацій інформаційно-безпекової політики використано порівняльний метод, який дав можливість зіставити інституційні моделі забезпечення інформаційної безпеки в довоєнний період та в умовах воєнного стану. Нормативно-правовий аналіз застосовувався для дослідження правових засад функціонування інформаційної сфери, особливостей правового режиму воєнного стану та його впливу на регулювання інформаційних відносин.

Метод структурно-функціонального аналізу використано з метою виявлення ключових інституційних механізмів забезпечення інформаційної безпеки, а також факторів, що знижують ефективність інформаційно-безпекової політики. Узагальнення й інтерпретація результатів здійснювалися з урахуванням сучасних наукових підходів до дослідження гібридних конфліктів і інформаційних війн.

Результати та обговорення. Під час дослідження встановлено, що інституційні чинники виступають системоутворювальним елементом інформаційно-безпекової політики України та визначають її спроможність функціонувати в умовах воєнного стану. Аналіз теоретичних підходів до розуміння інформаційної безпеки як складової національної безпеки засвідчив, що сучасні інформаційні загрози мають комплексний характер і не обмежуються суто технологічним, правовим або військовим виміром. Вони формуються на перетині політичних, інформаційних, соціальних і комунікативних процесів, що суттєво ускладнює механізми їх ідентифікації та нейтралізації [1; 3].

Отримані результати дали змогу обґрунтувати доцільність розгляду інформаційно-безпекової політики як багаторівневої системи, у межах якої поєднуються правові, політичні, організаційні та комунікативні компоненти. У дисертації доведено, що саме інституційна спроможність держави забезпечує узгодженість зазначених компонентів, їхню взаємодію і адаптацію до умов гібридної війни та воєнного стану [4]. У цьому контексті інформаційна безпека постає не лише як сфера реагування на загрози, а як окремий напрям стратегічного державного управління, що потребує цілісного бачення, довгострокового планування та стабільної інституційної підтримки.

У межах дослідження інституційного виміру інформаційно-безпекової політики визначено ключові суб'єкти її формування та реалізації, зокрема органи державної влади, сектор безпеки й оборони, регуляторні інституції у сфері інформації та комунікацій, а також інститути громадянського суспільства та медіасередовище. Встановлено, що недостатня координація між цими інститутами знижує ефективність протидії інформаційним загрозам, особливо в умовах кризових ситуацій та воєнного протистояння [2]. Водночас обґрунтовано, що саме налагоджена інституційна взаємодія виступає передумовою формування стійкого інформаційного простору та підвищення загальної інформаційної резильєнтності держави.

Особливу увагу в дослідженні приділено аналізу нормативно-правових засад інформаційної безпеки. Встановлено, що в умовах воєнного стану відбувається посилення ролі держави в регулюванні інформаційного простору, зокрема шляхом обмеження деструктивних інформаційних впливів, протидії дезінформації та інформаційно-психологічним операціям [6; 7]. Разом із тим наголошується, що надмірна концентрація регуляторних повноважень без належних інституційних запобіжників може створювати ризики для демократичного розвитку, що зумовлює необхідність збереження балансу між імперативами безпеки та дотриманням прав і свобод людини. Такий баланс розглядається як ключова умова реалізації євроінтеграційного курсу України та її відповідності європейським стандартам у сфері інформаційної політики [5].

Окрему увагу приділено впливу воєнного стану на трансформацію інформаційно-безпекової політики. Доведено, що з початком повномасштабної агресії Російської Федерації інформаційна безпека набула статусу стратегічного пріоритету державної політики та була інтегрована в загальну систему національної безпеки [8]. Війна виступила каталізатором глибоких інституційних змін, спрямованих на підвищення стійкості інформаційного простору, вдосконалення механізмів державної комунікації, розвиток стратегічних комунікацій і зміцнення інформаційного суверенітету України.

Результати дослідження також підтверджують зростання ролі стратегічних комунікацій і суспільних наративів у забезпеченні інформаційної безпеки. Формування стійкого інформаційного середовища неможливе без урахування рівня довіри громадян до державних інститутів, а також без активної політичної та комунікативної участі суспільства. В умовах тривалого воєнного протистояння стратегічні комунікації виконують не лише інформативну, а й консолідаційну функцію, сприяючи збереженню соціальної єдності та підтримці легітимності державних рішень [10].

Узагальнюючи результати дослідження, можна стверджувати, що інституційні чинники не лише визначають здатність держави оперативно реагувати на інформаційні загрози, але й формують стратегічні засади інформаційно-безпекової політики України в умовах воєнного стану. Саме інституційна спроможність забезпечує адаптивність, стійкість і довгострокову ефективність цієї політики, а також її відповідність сучасним безпековим викликам і європейським стандартам [9].

Висновки. За результатами проведеного дослідження встановлено, що інформаційно-безпекова політика України в умовах воєнного стану формується під визначальним впливом інституційних чинників, які забезпечують її стійкість, адаптивність та спроможність реагувати на сучасні виклики. Інформаційна безпека в умовах російської агресії набула системного характеру та трансформувалася з окремого напряму державної політики у ключовий елемент загальної системи національної безпеки.

Доведено, що ефективність інформаційно-безпекової політики безпосередньо залежить від рівня інституційної взаємодії між органами державної влади, сектором безпеки й оборони, регуляторними структурами у сфері інформації та комунікацій, а також інститутами громадянського суспільства й медіасередовищем. Недостатня узгодженість дій між цими суб'єктами знижує здатність держави протидіяти інформаційним загрозам, тоді як

скоординована інституційна модель сприяє формуванню стійкого та контрольованого інформаційного простору.

Обґрунтовано, що воєнний стан став каталізатором інституційних змін у сфері інформаційної безпеки, зумовивши посилення ролі держави в регулюванні інформаційних процесів, розвитку стратегічних комунікацій та протидії дезінформації. Водночас актуалізується проблема збереження балансу між безпековими імперативами та демократичними стандартами, що має принципове значення для реалізації євроінтеграційного курсу України.

Встановлено, що інформаційно-безпекова політика в умовах війни виходить за межі суто технічних або нормативно-правових механізмів і дедалі більше спирається на соціально-політичні чинники, зокрема рівень довіри громадян до державних інститутів, ефективність суспільних комунікацій та здатність формувати стійкі національні наративи. Саме ці аспекти визначають довгострокову стійкість інформаційного простору й інформаційного суверенітету держави.

Загалом результати дослідження підтверджують, що інституційні чинники є ключовою передумовою формування ефективної інформаційно-безпекової політики України в умовах воєнного стану. Перспективи подальших наукових розвідок вбачаються в поглибленому аналізі інституційних механізмів стратегічних комунікацій, розвитку міжнародної співпраці у сфері інформаційної безпеки, а також у дослідженні ролі політичної участі та громадянського суспільства у зміцненні інформаційної стійкості держави.

Література:

1. Біленчук П. Д., Борисова Л. В., Неклонський І. М., Собина В. О. Правові засади інформаційної безпеки України. Харків, 2018. С. 289.

2. Галіпчак В. Безпека інформаційного простору України в умовах російської агресії на сучасному етапі: основні завдання та виклики. *Науковий журнал «Регіональні студії».* 2023. № 34. С. 81–85.

3. Галіпчак В. Основні методологічні засади поняття національної безпеки: інформаційний вимір. *POLITIA. Вісник наукових робіт молодих вчених.* Івано-Франківськ : ЯРИНА, 2023. Вип. 5. С. 192–225.

4. Глобенко С. Інформаційний простір держави та проблеми забезпечення його захисту в Україні. *Науковий вісник: Державне управління.* 2023. № 1. С. 195–210.

5. Гурковський В. І. Інформаційна безпека в Україні як складова національної безпеки. *Наукові праці Української академії державного управління.* 2002. № 2. С. 9–18.

6. Дерев'янко С. М. Гібридна війна: інформаційно-безпековий вимір. *Вісник Прикарпатського університету. Серія: Політологія.* 2024. Вип. 18. С. 11–18.

7. Дніпренко Н. К. Зміна парадигми в державному управлінні інформаційною сферою. *Теорія та історія державного управління.* 2005. С. 20.

8. Довгань О. Д., Ткачук Т. Ю. Система інформаційної безпеки України: онтологічні виміри. *Інформація і право.* 2018. № 1 (24). С. 89–103.

9. Загирняк, М. Інформаційна війна Росії проти України: особливості, методи та наслідки. *«Гібридна війна»: виклики та загрози національній безпеці України.* Київ, 2015. С. 42.

10. Захаренко К. Чинники здійснення державної інформаційної політики України. *Регіональні студії.* 2019. № 17. С. 15–19.

References:

1. Bilenchuk, P.D., Borysova, L.V., Neklonskyi, I.M., & Sobyna, V.O. (2018). Pravovi zasady informatsiinoi bezpeky Ukrainy [Legal foundations of information security of Ukraine]. Kharkiv [in Ukrainian].

2. Halipchak, V. (2023). Bezpeka informatsiinoho prostoru Ukrainy v umovakh rosiiskoi ahresii na suchasnomu etapi: osnovni zavdannia ta vyklyky [Security of Ukraine's information space under Russian aggression at the present stage: main tasks and challenges]. *Rehionalni studii – Regional Studies*, 34, 81–85 [in Ukrainian].

3. Halipchak, V. (2023). Osnovni metodolohichni zasady poniattia natsionalnoi bezpeky: informatsiinyi vymir [Basic methodological principles of the concept of national security: information dimension]. *POLITIA. Visnyk naukovykh robit molodykh vchenykh – POLITIA. Bulletin of Scientific Works of Young Scientists*, 5, 192–225 [in Ukrainian].

4. Hlobenko, S. (2023). Informatsiinyi prostir derzhavy ta problemy zabezpechennia yoho zakhystu v Ukraini [State information space and problems of ensuring its protection in Ukraine]. *Naukovyi visnyk: Derzhavne upravlinnia – Scientific Bulletin: Public Administration*, 1, 195–210 [in Ukrainian].

5. Hurkovskyi, V.I. (2002). Informatsiina bezpeka v Ukraini yak skladova natsionalnoi bezpeky [Information security in Ukraine as a component of national security]. *Naukovi pratsi Ukrainskoi akademii derzhavnoho upravlinnia – Scientific Works of the Ukrainian Academy of Public Administration*, 2, 9–18 [in Ukrainian].

6. Derevianko, S.M. (2024). Hibrydna viina: informatsiino-bezpekovyi vymir [Hybrid war: information and security dimension]. *Visnyk Prykarpatskoho universytetu. Seriia: Politolohiia – Bulletin of the Precarpathian University. Series: Political Science*, 18, 11–18 [in Ukrainian].

7. Dniprenko, N.K. (2005). Zmina paradyhmy v derzhavnomu upravlinni informatsiinoiu sferoiu [Paradigm shift in public administration of the information sphere]. *Teoriia ta istoriia derzhavnoho upravlinnia – Theory and history of public administration*, 20 [in Ukrainian].

8. Dovhan, O.D., & Tkachuk, T.Yu. (2018). Systema informatsiinoi bezpeky Ukrainy: ontolohichni vymiry [Information security system of Ukraine: ontological dimensions]. *Informatsiia i pravo – Information and Law*, 1 (24), 89–103 [in Ukrainian].

9. Zahyrianiak, M. (2015). Informatsiina viina Rosii proty Ukrainy: osoblyvosti, metody ta naslidky [Russia's information war against Ukraine: features, methods and consequences]. In *"Hibrydna viina": vyklyky ta zahrozy natsionalnii bezpetsi Ukrainy* ["Hybrid war": challenges and threats to Ukraine's national security] (p. 42). Kyiv [in Ukrainian].

10. Zakharenko, K. (2019). Chynnyky zdiisnennia derzhavnoi informatsiinoi polityky Ukrainy [Factors of implementation of the state information policy of Ukraine]. *Rehionalni studii – Regional Studies*, 17, 15–19 [in Ukrainian].

Volodymyr Halipchak, Nataliia Rotar. Institutional Factors of Ukraine`s Information Security Policy under Martial Law: a research concept

The article reveals the research concept of institutional factors shaping Ukraine's information security policy under martial law. The relevance of the study is determined by the intensification of information threats during the period of martial law and the growing role of information security as one of the key components of ensuring Ukraine's national security in the context of the full-scale armed aggression of the russian federation against the state. The article analyzes theoretical and methodological approaches to understanding information security as a multidimensional phenomenon that integrates legal, political, organizational, and communicative components. Special attention is paid to the impact of martial law on the transformation of Ukraine's information security policy. It is substantiated that the war has become a catalyst for institutional changes aimed at strengthening the resilience of the information space, developing strategic communications, and enhancing counteraction to disinformation. At the same time, emphasis is placed on the necessity of maintaining a balance between security imperatives and democratic standards within the framework of Ukraine's European integration course.

The study concludes that institutional factors determine not only the state's capacity to respond to current information threats but also shape the strategic foundations of information security policy under martial law, ensuring its adaptability and long-term effectiveness.

Key words: *information security, information security policy, institutional factors, martial law, hybrid war, national security.*

Відомості про автора:
Галіпчак Володимир – доктор філософії,
Карпатський національний університет імені Василя Стефаника.
Ротар Наталія – доктор політичних наук,
професор кафедри політології та державного управління,
Чернівецький національний університет імені Юрія Федьковича.

Дата першого надходження статті до видання: 30.11.2025
Дата прийняття статті до друку після рецензування: 14.12.2025
Дата публікації (оприлюднення) статті: 28.01.2026