ISSN 2415–881X Politology Bulletin, Issue 100 N1 (2026)

УДК 004:351.86(477)»2014/2025» DOI 10.17721/2415-881X.2026.100.1.314–323

Білецький Павло Васильович

Аспірант кафедри політології філософського факультету
Київський національний університет імені Тараса Шевченка (м. Київ, Україна)
https://orcid.org/0009-0000-9613-0771
e-mail: pavelbiletskyi87@gmail.com

ЕВОЛЮЦІЯ ПОНЯТТЯ «ІНФОРМАЦІЙНА БЕЗПЕКА» В УКРАЇНСЬКОМУ НАУКОВОМУ ДИСКУРСІ (2014 — 2025)

Резюме

Стаття присвячена дослідженню трансформації поняття «інформаційна безпека» в українському науковому дискурсі протягом 2014-2025 років — періоду, що охоплює початок гібридної агресії Російської Федерації, анексію Криму, збройний конфлікт на Донбасі та повномасштабне вторгнення 2022 року.

Здійснено періодизацію розвитку понятійного апарату інформаційної безпеки в Україні, виокремлено три ключові етапи: перший (2014-2017) — етап усвідомлення інформаційних загроз та початку концептуалізації; другий (2018-2021) — етап інституціоналізації та правового закріплення; третій (2022-2025) — етап воєнної трансформації та переосмислення. Для кожного етапу проаналізовано домінуючі теоретичні підходи, ключові наукові дискусії та нормативно-правові зміни.

Виявлено основні тенденції еволюції поняття: від вузького технократичного розуміння інформаційної безпеки як кіберзахисту до широкого міждисциплінарного трактування як системного чинника збереження державного суверенітету, суспільної єдності та демократичних цінностей. Обґрунтовано, що повномасштабна війна стала каталізатором якісного зрушення у понятійному апараті, спричинивши появу нових категорій — «інформаційна стійкість», «інформаційний суверенітет», «стратегічні комунікації воєнного часу».

Ключові слова: інформаційна безпека; науковий дискурс; понятійний апарат; гібридна війна; інформаційна стійкість; інформаційний суверенітет; Україна.

Вступ

Поняття «інформаційна безпека» є одним із центральних у сучасному безпековому дискурсі. Проте його зміст не є сталим — він еволюціонує під впливом зовнішніх загроз, технологічних змін, політичних процесів та наукових дискусій. В Україні цей процес еволюції набув особливої інтенсивності після 2014 року, коли інформаційна агресія Російської Федерації стала одним із ключових викликів національній безпеці.

До 2014 року поняття інформаційної безпеки в українській науці розглядалось переважно у технічному контексті — як захист інформаційних систем, баз даних та комунікаційних мереж від несанкціонованого доступу. Політичний, соціальний та гуманітарний виміри інформаційної безпеки залишалися на периферії наукової уваги. Анексія Криму та початок збройного конфлікту на Донбасі докорінно змінили цю ситуацію, продемонструвавши руйнівну силу інформаційних операцій як інструменту гібридної війни [1, с. 15].

Актуальність дослідження зумовлена кількома чинниками. По-перше, понятійний апарат є фундаментом будь-якої наукової дисципліни, і його стан безпосередньо впливає на якість наукових досліджень та ефективність практичних рекомендацій. По-друге, еволюція понять відображає зміну суспільних пріоритетів та наукових парадигм, що є важливим об›єктом наукознавчого аналізу. По-третє, розуміння логіки розвитку понятійного апарату дозволяє прогнозувати подальші тенденції та формулювати напрями досліджень.

Проблематика інформаційної безпеки досліджувалася у працях В. Ліпкана, О. Скирти, Г. Почепцова, В. Горбуліна, Є. Макаренко, І. Гуменюка, О. Зернецької та інших вітчизняних учених. Серед зарубіжних дослідників слід відзначити роботи Б. Бузана та О. Вевера з копенгагенської школи безпекових досліджень, які запропонували концепцію «сек›юритизації» як процесу перетворення певного явища на об›єкт безпекової політики.

Водночас комплексних досліджень, що простежують еволюцію саме понятійного апарату інформаційної безпеки в українському науковому дискурсі протягом визначеного періоду, на сьогодні бракує. Більшість робіт зосереджуються на конкретних аспектах інформаційної безпеки, не аналізуючи динаміку та трансформацію самих понять.

Метою статті є аналіз еволюції поняття «інформаційна безпека» в українському науковому дискурсі протягом 2014-2025 років, виявлення основних тенденцій та етапів цієї еволюції, а також визначення чинників, що зумовили трансформацію понятійного апарату.

Методи дослідження

Методологічна основа дослідження базується на поєднанні кількох взаємодоповнюваних методів, що дозволили забезпечити комплексний аналіз еволюції понятійного апарату інформаційної безпеки. Так, історико-генетичний метод використано для простеження хронологічної послідовності змін у розумінні інформаційної безпеки та виявлення причинно-наслідкових зв›язків між суспільно-політичними подіями та трансформацією понятійного апарату. Цей метод дозволив виокремити три ключові етапи еволюції поняття. Метод контент-аналізу застосовано для систематичного дослідження наукових публікацій, нормативно-правових актів та стратегічних документів, що містять визначення та інтерпретації інформаційної безпеки. Проаналізовано масив наукових статей, монографій та дисертацій за період 2014 — 2025 років. Компаративний метод забезпечив порівняння різних визначень інформаційної безпеки на кожному з виділених етапів, а також зіставлення українського наукового дискурсу із зарубіжними підходами, зокрема концепцією сек›юритизації копенгагенської школи. Дискурс-аналіз дозволив дослідити не лише зміст понять, а й контекст їх формування, виявити домінуючі наративи, конкуруючі інтерпретації та владні відносини, що впливають на формування понятійного апарату.

Результати дослідження

1. Перший етап (2014 — 2017): усвідомлення інформаційних загроз та початок концептуалізації

Події 2014 року — анексія Криму та початок збройного конфлікту на сході України — стали потужним каталізатором переосмислення інформаційної безпеки в українському науковому та політичному дискурсі. До цього моменту поняття інформаційної безпеки було переважно технічним терміном, що асоціювалося із захистом інформаційних систем та кіберзахистом [2, с. 112].

Масштабна інформаційна кампанія Російської Федерації, що супроводжувала анексію Криму, — з використанням фейкових новин, пропагандистських наративів про «захист російськомовного населення», «фашистську хунту в Києві» та ін. — наочно продемонструвала, що інформаційна безпека має значно ширший зміст, ніж технічний захист даних [3, с. 22].

На цьому етапі в українській науці формується розуміння інформаційної безпеки як комплексного явища, що включає не лише технічний, а й політичний, соціальний, психологічний та гуманітарний виміри. Починає активно використовуватися поняття «інформаційна війна», яке до 2014 року сприймалося переважно як теоретична абстракція [4, с. 45].

Ключовим нормативним документом цього етапу стала Доктрина інформаційної безпеки України, затверджена Указом Президента у 2017

році. Цей документ вперше на державному рівні визначив інформаційну безпеку як стан захищеності життєво важливих інтересів людини, суспільства і держави в інформаційній сфері та окреслив основні загрози, серед яких інформаційна агресія РФ була визнана пріоритетною [5].

У наукових дискусіях цього періоду домінували два підходи. Перший — «оборонний» — розглядав інформаційну безпеку як захист від зовнішніх загроз і передбачав обмеження доступу до ворожого контенту, блокування російських медіа та соціальних мереж. Другий — «розвитковий» — акцентував увагу на необхідності формування власного якісного медіапростору, розвитку медіаграмотності та критичного мислення населення [6, с. 70].

2. Другий етап (2018 — 2021): інституціоналізація та правове закріплення

Другий етап характеризується поступовою інституціоналізацією інформаційної безпеки як самостійного напряму державної політики та її правовим закріпленням у ключових нормативних документах.

Закон України «Про національну безпеку України» 2018 року інтегрував інформаційну безпеку до загальної системи національної безпеки, визначивши її як один із ключових секторів безпекової політики [7, с. 12]. Це означало визнання на законодавчому рівні того, що інформаційна безпека є не технічним, а стратегічним питанням.

Національна стратегія кібербезпеки України 2021 року розглянула інформаційну безпеку у тісному зв›язку з кібербезпекою, фактично запропонувавши інтегроване розуміння кіберінформаційної безпеки [8, с. 5]. У науковому дискурсі цього періоду з›являється поняття «кіберінформаційна безпека», що відображає конвергенцію технічного та соціально-гуманітарного вимірів.

Створення у 2021 році Центру протидії дезінформації при Раді національної безпеки і оборони стало знаковою інституційною подією, що символізувала визнання дезінформації як стратегічної загрози, а протидію їй — як систематичну державну функцію [9].

У науковому дискурсі цього етапу відбувається розширення понятійного поля інформаційної безпеки. Поряд із традиційними категоріями (кіберзахист, захист інформації, інформаційна війна) з›являються нові: «інформаційна гігієна», «цифрова стійкість», «медіаграмотність як чинник безпеки», «алгоритмічна маніпуляція». Це свідчить про міждисциплінарне розширення предметного поля інформаційної безпеки — від суто технічного та правового до психологічного, педагогічного та культурологічного вимірів [10, с. 88].

3. Третій етап (2022 — 2025): воєнна трансформація та переосмислення

Повномасштабне вторгнення Російської Федерації 24 лютого 2022 року спричинило якісне зрушення у розумінні інформаційної безпеки. Масштаб та інтенсивність інформаційних атак, що супроводжували воєнну агресію, перевершили всі попередні прогнози та вимагали принципово нових підходів.

На цьому етапі в науковому дискурсі формується розуміння інформаційної безпеки як екзистенційного чинника збереження державності. Інформаційна безпека перестає бути лише однією зі складових національної безпеки і набуває значення наскрізного, системоутворюючого елементу, від якого залежить ефективність усіх інших секторів безпеки — воєнного, економічного, екологічного [11, с. 34].

Ключовою новацією понятійного апарату цього етапу стало поняття «інформаційна стійкість» (information resilience). На відміну від «інформаційної безпеки», що акцентує увагу на захисті від загроз, «інформаційна стійкість» передбачає здатність суспільства не лише протидіяти інформаційним атакам, а й швидко відновлюватися після них, зберігаючи єдність та функціональність [12, с. 56]. Це поняття відображає зміну парадигми — від оборонної до адаптивної моделі інформаційної безпеки.

Іншою важливою категорією стало поняття «інформаційний суверенітет», що трактується як здатність держави самостійно визначати свою інформаційну політику, контролювати критичну інформаційну інфраструктуру та забезпечувати захист національного інформаційного простору від зовнішнього втручання. Досвід блокування російських соціальних мереж та медіа, запровадження єдиного телемарафону «Єдині новини» актуалізував дискусію про межі та зміст інформаційного суверенітету в демократичному суспільстві.

Значного поширення набуло поняття «стратегічні комунікації воєнного часу», що описує координовану діяльність державних та недержавних акторів у формуванні інформаційного простору, спрямовану на досягнення стратегічних цілей — підтримку морального духу населення, мобілізацію міжнародної підтримки, дискредитацію ворожих наративів. Це поняття стало ключовим для опису нової моделі комунікації між державою, суспільством та міжнародною спільнотою в умовах війни.

Характерною особливістю наукового дискурсу цього етапу є зростання ролі практиків — військових аналітиків, журналістів, фактчекерів, OSINT-дослідників — у формуванні понятійного апарату. Поняття, що народжувалися у практичній площині (наприклад, «бот-ферма», «наративна

зброя», «інформаційний ПСІОП»), поступово входили до наукового обігу та отримували теоретичне осмислення.

Узагальнюючи проведений аналіз, можна виокремити кілька ключових тенденцій еволюції поняття «інформаційна безпека» в українському науковому дискурсі 2014 — 2025 років.

Від технократичного до міждисциплінарного розуміння. Якщо на початку досліджуваного періоду інформаційна безпека розумілася переважно як технічний кіберзахист, то до 2025 року це поняття набуло комплексного характеру, що інтегрує технічний, правовий, політичний, психологічний, педагогічний та культурологічний виміри.

Від оборонної до адаптивної парадигми. Класичне розуміння інформаційної безпеки як захисту від загроз поступово доповнюється концепцією інформаційної стійкості — здатності суспільства адаптуватися до інформаційних викликів та відновлюватися після інформаційних атак.

Від державоцентричного до мережевого підходу. На першому етапі основним суб›єктом інформаційної безпеки розглядалася держава. На третьому етапі визнається множинність акторів — від державних органів до волонтерських OSINT-спільнот, від традиційних медіа до блогерів та інфлюенсерів.

Сек›юритизація інформаційної сфери. Відповідно до концепції Б. Бузана та О. Вевера, протягом досліджуваного періоду відбулася послідовна сек›юритизація інформаційної сфери — перетворення інформаційних питань на об›єкт безпекової політики, що легітимізує застосування надзвичайних заходів [13, с. 177].

Прагматизація наукового дискурсу. Під тиском реальних загроз український науковий дискурс про інформаційну безпеку став значно більш практико-орієнтованим. Зростає частка прикладних досліджень, збільшується участь практиків у наукових дискусіях, а нові поняття формуються не лише «зверху» (від теоретиків), а й «знизу» (від практиків інформаційної боротьби).

Висновки

Проведене дослідження дозволяє зробити низку висновків щодо еволюції поняття «інформаційна безпека» в українському науковому дискурсі протягом 2014-2025 років.

Встановлено, що поняття «інформаційна безпека» зазнало суттєвої трансформації під впливом безпекових викликів, пов›язаних із гібридною та повномасштабною агресією Російської Федерації. Виокремлено три етапи цієї еволюції: етап усвідомлення загроз (2014-2017), етап інституціоналізації (2018-2021) та етап воєнної трансформації (2022-2025).

Виявлено, що ключовими тенденціями еволюції є перехід від технократичного до міждисциплінарного розуміння, від оборонної до адаптивної парадигми, від державоцентричного до мережевого підходу, а також прагматизація наукового дискурсу та його наближення до практичних потреб.

Визначено, що повномасштабна війна стала потужним каталізатором понятійних інновацій, спричинивши появу нових категорій, як «інформаційна стійкість», «інформаційний суверенітет», «стратегічні комунікації воєнного часу», які відображають якісно нове розуміння ролі інформаційної сфери у забезпеченні національної безпеки.

Перспективними напрямами подальших досліджень є порівняльний аналіз еволюції понятійного апарату інформаційної безпеки в інших країнах, що зазнали інформаційної агресії, а також дослідження впливу технологій штучного інтелекту та deepfake на трансформацію поняття інформаційної безпеки у найближчій перспективі.

Список посилань

1. Горбулін В. П. Світова гібридна війна: український фронт. Київ: НІСД, 2017. 496 с.
2. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції: навч. посібник. Київ: КНТ, 2016. 280 с.
3. Інститут масової інформації. Російські дезінформаційні кампанії проти України: аналітичний звіт. Київ: ІМІ, 2022. 32 с. (Режим доступу: https://imi.org.ua).
4. Почепцов Г. Г. Інформаційні війни: теорія і практика. Київ: Видавничий дім «Києво-Могилянська академія», 2015. 368 с.
5. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» від 25 лютого 2017 року № 47/2017.
6. Скирта О. В. Інформаційна безпека в умовах глобалізації: сучасні виклики та загрози. Інформаційне право України. 2021. № 3. С. 70-79.
7. Закон України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII. Офіційний вісник України. 2018. № 55. С. 12 — 30.
8. Національна стратегія кібербезпеки України, затверджена Указом Президента України № 447/2021 від 26 серпня 2021 року. Офіційний вісник Президента України. 2021. № 68. С. 2 — 14.

9. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації» від 19 березня 2021 року № 106/2021.
10. Гуменюк І. Б. Розвиток законодавства України у сфері інформаційної безпеки: ретроспективний аналіз. Юридичний вісник України. 2021. № 6. С. 101-108.
11. Макаренко Є. А. Міжнародна інформаційна політика: підручник. Київ: Наша культура і наука, 2019. 452 с.
12. Зернецька О. В. Інформаційна стійкість суспільства в умовах гібридної війни: теоретичні засади. Стратегічні пріоритети. 2023. № 1. С. 48-62.
13. Buzan B., Waever O., de Wilde J. Security: A New Framework for Analysis. Boulder: Lynne Rienner Publishers, 1998. 239 p.

References

1. Horbulin, V.P. (2017). The World Hybrid War: Ukrainian Front. Kyiv: NISS, 496 p. [in Ukrainian].
2. Lipkan, V.A. (2016). Information Security of Ukraine in the Context of European Integration: Textbook. Kyiv: KNT, 280 p. [in Ukrainian].
3. Institute of Mass Information. Russian Disinformation Campaigns Against Ukraine: Analytical Report. Kyiv: IMI, 2022. 32 p. [in Ukrainian].
4. Pocheptsov, H.H. (2015). Information Wars: Theory and Practice. — Kyiv: Kyiv-Mohyla Academy Publishing, 368 p. [in Ukrainian].
5. Decree of the President of Ukraine «On the Decision of the National Security and Defense Council of Ukraine of December 29, 2016, 'On the Doctrine of Information Security of Ukraine'» of February 25, 2017, No. 47/2017.
6. Skyrta, O.V. (2021). Information Security in the Context of Globalization: Current Challenges and Threats. Information Law of Ukraine, No. 3, 70-79. [in Ukrainian].
7. Law of Ukraine «On National Security of Ukraine» of June 21, 2018, No. 2469-VIII. Official Bulletin of Ukraine. (2018), No. 55, 12-30.
8. National Cybersecurity Strategy of Ukraine, approved by Presidential Decree No. 447/2021 of August 26, 2021. Official Bulletin of the President of Ukraine, 2021, No. 68, 2-14.
9. Decree of the President of Ukraine «On the Decision of the National Security and Defense Council of Ukraine of March 11, 2021, 'On the

Establishment of the Center for Countering Disinformation'» of March 19, 2021, No. 106/2021.

10. Humeniuk, I.B. (2021). Development of Ukrainian Legislation in the Field of Information Security: A Retrospective Analysis. Legal Bulletin of Ukraine, No. 6, 101-108. [in Ukrainian].
11. Makarenko, Ye.A. (2019). International Information Policy: Textbook. Kyiv: Nasha Kultura i Nauka, 452 p. [in Ukrainian].
12. Zernetska, O.V. (2023). Information Resilience of Society in the Context of Hybrid War: Theoretical Foundations. Strategic Priorities, No. 1, 48-62. [in Ukrainian].
13. Buzan, B., Waever, O., de Wilde, J. Security: A New Framework for Analysis. Boulder: Lynne Rienner Publishers, 1998. 239 p.

УДК 004:351.86(477)»2014/2025» DOI 10.17721/2415-881X.2026.100.1.314–323

Pavlo Biletskyi
Postgraduate Student, Department of Political Science, Faculty of Philosophy
Taras Shevchenko National University of Kyiv (Kyiv, Ukraine)
https://orcid.org/0009-0000-9613-0771
e-mail: pavelbiletskyi87@gmail.com

EVOLUTION OF THE CONCEPT OF «INFORMATION SECURITY» IN UKRAINIAN SCIENTIFIC DISCOURSE (2014 — 2025)

Abstract

The article examines the transformation of the concept of "information security" in Ukrainian academic discourse over the period 2014 — 2025 — a timeframe encompassing the onset of the Russian Federation's hybrid aggression, the annexation of Crimea, the armed conflict in the Donbas, and the full-scale invasion of 2022.

A periodization of the development of the conceptual apparatus of information security in Ukraine is proposed, identifying three key stages: the first (2014 — 2017) as the stage of recognizing information threats and the initial conceptualization; the second (2018 — 2021) as the stage of institutionalization and legal consolidation; and the third (2022 — 2025) as the stage of wartime transformation and conceptual rethinking. For each stage, the dominant theoretical approaches, key academic debates, and regulatory changes are analyzed.

The main trends in the evolution of the concept are identified: a shift from a narrow technocratic understanding of information security as cyber protection to a broad interdisciplinary interpretation as a systemic factor in safeguarding state sovereignty, social cohesion, and democratic values. It is substantiated that the full-scale war has acted as a catalyst for a qualitative shift in the conceptual framework, leading to the emergence of new categories such as "information resilience," "information sovereignty," and "wartime strategic communications."

Keywords: information security; academic discourse; conceptual framework; hybrid war; information resilience; information sovereignty; Ukraine.

Надійшла до редакції/ Received: 03.02.2026

Прорецензовано/ Revised: 18.02.2026

Прийнято до друку/ Accepted: 27.02.2026