УДК 327:351.746.1 DOI 10.17721/2415-88IX.2025.96.263–271

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

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ЕЛЕМЕНТ НАЦІОНАЛЬНОЇ СТРАТЕГІЇ У КОНТЕКСТІ ПРОТИДІЇ ЗОВНІШНІМ ЗАГРОЗАМ

Резюме

Сучасні виклики які стоять перед інформаційною безпекою, зумовлені глобалізацією, розвитком цифрових технологій та зростанням гібридних загроз, вимагають від держав нового погляду на структуру та пріоритети національної безпеки.

Визначено, що інформаційна безпека — це сукупність заходів та методів, спрямованих на захист цілісності інформаційних систем від несанкціонованого доступу, зміни, викрадення або знищення інформації, порушення її доступності та конфіденційності.

Здійснено аналіз нормативно-правових документів, що визначають та регулюють сферу інформаційної безпеки України, зокрема Закону України «Про національну безпеку», Національної стратегії кібербезпеки та інших офіційних документів. Розглянуто міжнародний досвід (США, ЄС, Ізраїлю), виявлено його потенціал для адаптації в українських реаліях гібридної інформаційної війни. Окрему увагу приділено загрозам інформаційному простору України, які проявляються у кібератаках, пропаганді, фейках, психологічному впливі через соціальні мережі та загалом мережу Інтернет (мережі вебсайтів, месенджери та ін.).

Запропоновано практичні кроки щодо зміцнення системи інформаційної безпеки, а саме: розробку окремої стратегії інформаційної безпеки України, розвиток національної освіти у сфері інформаційної безпеки, інституціалізацію стратегічних комунікацій на рівні державної політики.

Ключові слова: інформаційна безпека, національна безпека, кібербезпека, кіберзахист, інформаційний суверенітет.

Вступ

У наш час питання інформаційної безпеки набуває пріоритетного значення у системі національної безпеки будь-якої держави. Інформаційна сфера давно вже перетворилася на самостійний простір протистояння, де здійснюються цілеспрямований вплив на політичні процеси, громадську думку, економічні зв'язки та навіть оборонні спроможності держав. Інформаційний простір постійно ускладнюються та технічно вдосконалюється, що автоматично призводить до ускладнення та вдосконалення інформаційних атак, їх методів та засобів. Враховуючи це, інформаційна безпека будь-якої держави повинна також вдосконалюватись і ускладнюватися, тобто не бути статичною системою норм і документів, правил та технічних засобів їх застосування. Наприклад, порушення цілісності елементу інформаційної системи будь-якого стратегічного об'єкта чи галузевого міністерства буде мати наслідки, які вийдуть далеко за межі інформаційного (кібернетичного) впливу на сам об'єкт і перейдуть в величезні іміджеві, соціальні та матеріальні наслідки. Особливо актуальним це питання стало для України, яка з 2014 року фактично стала об'єктом масштабної інформаційної агресії, а з 2022 року об'єктом повномасштабного вторгнення з боку російської федерації. У зв'язку з цим формування ефективної системи інформаційної безпеки розглядається як невід'ємний елемент загальної стратегії забезпечення національної безпеки держави та посилення її обороноздатності.

Так, відповідно до Закону України «Про національну безпеку України», інформаційна безпека визначається як «захищеність життєво важливих інтересів людини і громадянина, суспільства і держави в інформаційній сфері»[1, с. 12]. На практиці ж це означає необхідність не лише технічного захисту інформаційних систем, але й забезпечення інформаційної стійкості суспільства до зовнішніх впливів, захисту «інформаційного суверенітету» держави та запобігання поширенню дезінформації. Але впровадження цих принципів відбувається занадто повільно у відношенні до зростання кількості та складності викликів, які з часом постають перед інформаційною безпекою нашої держави.

Зазначена проблематика вже давно розглядається в контексті національної стратегії багатьох країн. Наприклад, у Сполучених Штатах Америки інформаційна безпека входить до компетенції Департаменту внутрішньої безпеки, який розробляє та ефективно впроваджує спеціальні стратегії щодо захисту критичної інформаційної інфраструктури [2, с. 19].

У Європейському Союзі ухвалено Стратегію кібербезпеки ЄС для цифрового десятиліття (2020-2030 роки), яка включає положення щодо зміцнення інформаційної безпеки, боротьби з дезінформацією та протидії інформаційним загрозам з боку третіх країн [3, с. 7 — 9].

З огляду на посилення гібридної інформаційної та повномасштабної військової агресії проти України, що включає інформаційні атаки, дезінформаційні кампанії, кібератаки на критичну інфраструктуру, питання ефективної протидії інформаційним загрозам стає надзвичайно важливим. Національна стратегія кібербезпеки України, затверджена у 2021 році, визнає інформаційну безпеку одним із головних пріоритетів державної політики у сфері безпеки [4, с. 2 — 4]. Однак цього не достатньо так як наявні загрози вимагають постійного оновлення стратегічних підходів, практичного інструментарію, адаптації міжнародного досвіду та впровадження сучасних технологій у сфері інформаційного захисту.

У науковій літературі існує певний дефіцит комплексних досліджень, які б розглядали інформаційну безпеку саме як системоутворюючий елемент національної стратегії, а не лише як технічний чи правовий аспект. Здебільшого брак наукового осмислення проблематики інформаційної безпеки полягає у практичній відірваності авторів від практики побудови систем захисту цілісності інформації та інформаційних систем.

Метою статті є аналіз інформаційної безпеки як одного з ключових елементів національної стратегії України, визначення основних загроз в інформаційній сфері та вироблення пропозицій щодо удосконалення стратегічних підходів до забезпечення інформаційної безпеки в умовах зовнішньої агресії.

Методологія дослідження

Методологічна основа дослідження базується на системному використанні комплексу загальнонаукових і спеціальних методів, зокрема — компаративний, системний та критико-діалектичний — що забезпечили багатовимірність та глибину аналізу. Так, компаративний метод дав змогу здійснити порівняльне вивчення досвіду провідних країн (США, ЄС, Ізраїль) у сфері інформаційної безпеки, виокремити ефективні механізми протидії інформаційним загрозам і оцінити можливості їх адаптації в українських умовах. Саме через призму цього методу вдалося виявити сильні та слабкі сторони національного підходу до інформаційної безпеки, окреслити можливості для реформ. Системний метод дозволив розглядати інформаційну безпеку не як ізольований феномен, а як багаторівневу систему, що включає правові, організаційні, технічні, політичні та гуманітарні елементи. Такий підхід надав можливість охопити складність предмета дослідження і проаналізувати взаємозв'язки між складовими безпекової

політики, виявивши, зокрема, прогалини в координації та реалізації національних рішень. Критико-діалектичний метод забезпечив глибоке осмислення внутрішніх суперечностей в існуючих моделях інформаційної безпеки, зокрема між оборонною функцією та дотриманням прав людини, між технократичним підходом і потребою в стратегічній комунікації. Завдяки цьому методу вдалося не лише описати поточний стан, а й запропонувати теоретично виважені напрями вдосконалення політики у сфері інформаційної безпеки.

Поєднання цих методів дозволило здійснити цілісний і критичний аналіз інформаційної безпеки як пріоритетного елементу сучасної національної стратегії держави.

Результати дослідження

Аналіз законодавчої бази України свідчить, що інформаційна безпека як незалежний вимір практичної безпекової діяльності вперше отримала чітке законодавче закріплення як складова національної безпеки у Законі України «Про національну безпеку України» 2018 року [1, с. 13].

У Законі підкреслюється, що захист інформаційного простору держави є однією з важливих умов забезпечення державного суверенітету, територіальної цілісності та демократичного розвитку.

Національна стратегія кібербезпеки України, яка була створена в 2021 році розглядає інформаційну безпеку як невід'ємну частину кібербезпеки та національної безпеки загалом [2, с. 5]. По суті це перше інституціональне виокремлення інформаційної безпеки з інформаційної політики як складова національної безпеки на законодавчому рівні. Вона визначає пріоритети державної політики, серед яких особливе місце займають захист критичної інформаційної інфраструктури, протидія інформаційним операціям з боку іноземних держав та формування стійкості українського суспільства до інформаційних загроз. Водночас, окрім законодавчого затвердження, чіткого визначення суті інформаційної безпеки в нормативно-правовій базі України наразі не існує.

Таким чином, сучасна концепція національної безпеки України виходить із необхідності комплексного підходу до інформаційної безпеки, що включає правові, організаційні, технічні та соціальні аспекти. *Результати дослідження* нормативно-правової бази свідчать, що основними загрозами інформаційній безпеці України є:

- інформаційна агресія з боку російської федерації, яка включає масові кампанії дезінформації, фальсифікації історичних фактів, пропагандистські наративи про «неспроможність української державності» [3, с. 37 — 39];

- кібератаки на критичну інфраструктуру, зокрема енергетичний сектор, банківську систему, державні інформаційні ресурси (атаки BlackEnergy, Industroyer) [4, с. 8–12];

- маніпуляція громадською думкою через соціальні мережі, створення бот-мереж для поширення фейків та формування панічних настроїв серед населення [5, с. 44–45];

- недостатній рівень інформаційної культури населення, що полегшує поширення фейкових новин та сприяє соціальній нестабільності [6, с. 50].

Зазначене дає змогу стверджувати, що інформаційні загрози є системними і комплексними за своїм характером, що потребує відповідної системної відповіді на державному рівні. Найголовніше не тільки створити класифікацію загроз та методи атак, а підготувати кваліфікований персонал для ефективного відпрацювання цих атак, побудови захищеного інформаційного простору з урахуванням досвіду інформаційної безпеки за стандартами НАТО, National Cyber Strategy (США), що передбачає проактивні заходи протидії кібератакам та дезінформаційним кампаніям [7, с. 23 — 24].

Порівняння підходів різних країн до організації інформаційної безпеки дозволило виявити кілька ефективних практик. Європейський Союз діє через Європейське агентство з кібербезпеки (ENISA) та імплементує стратегію NIS2 (Network and Information Security Directive 2), яка встановлює мінімальні стандарти захисту інформаційних систем для усіх держав-членів [8, с. 10]. В Ізраїлі створено спеціалізовану структуру — Israel National Cyber Directorate, що координує як державні, так і приватні ініціативи у сфері кіберзахисту. Країна робить акцент на превентивних заходах та постійній підготовці кадрів у сфері інформаційної безпеки [9, с. 6 — 7].

Таким чином, міжнародний досвід свідчить про необхідність комплексного підходу до захисту інформаційного простору, де технічні засоби безпеки доповнюються інформаційною політикою, просвітницькими програмами та міжнародною співпрацею. Дослідники цієї проблематика виділяють такі основні перепони, що перешкоджають ефективній реалізації політики інформаційної безпеки в Україні:

- нерівномірна імплементація стандартів безпеки у різних секторах економіки [10, с. 88];

- брак єдиного координаційного органу з питань інформаційної безпеки на рівні держави;

- недостатня інтеграція приватного сектору у систему забезпечення інформаційної безпеки;

- низький рівень підготовки спеціалістів та відсутність системної освіти у сфері інформаційної безпеки;

- обмеженість фінансування державних програм кібер- та інформаційного захисту.

Ці завдання вимагають невідкладного вирішення, оскільки подальше ігнорування загроз буде мати унаслідки для державного суверенітету, інформаційного суверенітету України. На мій погляд, для їх реалізації необхідно наступне:

1) розробити окрему Національну стратегію інформаційної безпеки, інтегровану у загальну систему національної безпеки;

2) законодавчо закріпити обов'язковість впровадження стандартів інформаційної безпеки (ISO/IEC 27001) у критичних секторах економіки.

3) розробити програми підготовки кадрів та масової просвіти з питань інформаційної безпеки;

4) інтенсифікувати міжнародне співробітництво у сфері боротьби з кібер- та інформаційними загрозами задля реалізації спільних програм та обміну досвідом.

Це дозволить посилити інформаційну стійкість України та ефективно протидіяти зовнішнім інформаційним загрозам.

Висновки

По-перше, встановлено, що інформаційна безпека є однією з ключових складових національної безпеки держави, без якої неможливе забезпечення політичної стабільності, соціальної єдності та державного суверенітету. Інформаційна сфера сьогодні є полем боротьби за вплив, формування громадської думки та маніпулювання соціальними процесами, настроями що зумовлює необхідність активної протидії інформаційним загрозам на державному рівні.

По-друге, в умовах гібридної агресії з боку російської федерації, що триває з 2014 року, Україна постійно стикається з інформаційними атаками, спрямованими на підрив довіри до державних інституцій, формування фальшивих наративів щодо політичного та економічного розвитку країни, деморалізацію населення та міжнародну ізоляцію України.

По-третє, проаналізувавши міжнародний досвід (США, Європейський Союз, Ізраїль), можна дійти висновку, що ефективна система інформаційної безпеки повинна базуватися на інтеграції технічних, правових, організаційних, дипломатичних і освітніх заходів. Особливо важливими є: інтеграція зусиль державного і приватного секторів у вдосконаленні механізмів інформаційної безпеки, активна просвітницька

діяльність та участь у міжнародних об'єднаннях із протидії інформаційним загрозам.

По-четверте, в Україні залишається низка нерозв'язаних проблем у сфері інформаційної безпеки, серед яких можна виокремити: нерівномірне впровадження міжнародних стандартів безпеки, відсутність єдиної національної стратегії інформаційної безпеки, недостатню координацію між органами влади та низький рівень інформаційної культури громадян.

В умовах гібридної війни інформаційна безпека стає не просто функціональною сферою діяльності держави, а стратегічним напрямом, що має безпосередній вплив на збереження її незалежності, демократії та європейського вибору. Посилення державної політики у сфері інформаційної безпеки є необхідною передумовою для успішної протидії сучасним загрозам та побудови стійкої демократичної держави.

Список посилань

1. Закон України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII. Офіційний вісник України. 2018. № 55. С. 12-30.
2. Національна стратегія кібербезпеки України, затверджена Указом Президента України № 447/2021 від 26 серпня 2021 року. Офіційний вісник Президента України. 2021. № 68. С. 2 — 14.
3. Інститут масової інформації. Російські дезінформаційні кампанії проти України: аналітичний звіт. Київ: IMI, 2022. 32 с. (Режимдоступу:https://imi.org.ua/news/rosiyski-dezinformatsijni-kampaniyi-proty-ukrayiny-i43218, дата звернення: 30.04.2025).
4. ICS-CERT. BlackEnergy and Ukraine power outage: Incident Report. Washington, D.C.: ICS-CERT, 2016. 18 p. (Режим доступу: https://us-cert.cisa.gov/ics/advisories/ICS-ALERT-16-074-01, дата звернення: 30.04.2025).
5. Інформаційна війна у соцмережах: практики Росії проти України. — Київ: StopFake, 2021. 44 с. (Режим доступу: https://www.stopfake.org, дата звернення: 30.04.2025).
6. Скирта О. В. Інформаційна безпека в умовах глобалізації: сучасні виклики та загрози. Інформаційне право України. 2021. № 3. С. 70 — 79.
7. Department of Homeland Security. DHS Cybersecurity Strategy 2018 — 2023. Washington, D.C.: DHS, 2018. 38 p. (Режим доступу: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf, дата звернення: 30.04.2025).

8. European Commission. The EU's Cybersecurity Strategy for the Digital Decade. Brussels: European Union, 2020. — 32 p. (Режим доступу: https://ec.europa.eu/digital-strategy/cybersecurity_en, дата звернення: 30.04.2025).
9. Israel National Cyber Directorate. Cybersecurity Annual Report 2022. Jerusalem: INCD, 2022. 28 p. (Режим доступу: https://www.gov.il/en/departments/cyber, дата звернення: 30.04.2025).
10. Гуменюк І. Б. Розвиток законодавства України у сфері інформаційної безпеки: ретроспективний аналіз. Юридичний вісник України. 2021. № 6. С. 101-108.

References

1. Law of Ukraine "On National Security of Ukraine" of June 21, 2018, No. 2469-VIII. Official Bulletin of Ukraine, 2018, No. 55, 12 — 30 p.
2. 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 p.
3. Institute of Mass Information (2022). Russian Disinformation Campaigns Against Ukraine: Analytical Report, Kyiv: IMI, 32 p.
4. ICS-CERT (2016). BlackEnergy and Ukraine Power Outage: Incident Report. Washington, D.C.: ICS-CERT, 2016, 18 p.
5. Information War on Social Media: Russian Practices Against Ukraine. Kyiv: StopFake, 2021, 44 p. (Access mode: https://www.stopfake.org, accessed: 30.04.2025).
6. Skyrta, O. V. (2021). Information Security in the Context of Globalization: Current Challenges and Threats. Information Law of Ukraine, No. 3, 70-79 p.
7. Department of Homeland Security (2018). DHS Cybersecurity Strategy Washington, D.C.: DHS, 38 p.
8. European Commission (2020). The EU's Cybersecurity Strategy for the Digital Decade. Brussels: European Union, 32 p.
9. Israel National Cyber Directorate. (2022). Cybersecurity Annual Report. Jerusalem: INCD, 28 p.
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 p.

УДК 327:351.746.1 DOI 10.17721/2415-88IX.2025.96.263–271

Pavlo Biletskyi

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

INFORMATION SECURITY AS AN ELEMENT OF THE NATIONAL STRATEGY IN THE CONTEXT OF COUNTERING EXTERNAL THREATS

Abstract

The modern challenges facing information security, driven by globalization, the development of digital technologies, and the rise of hybrid threats, require states to adopt a new perspective on the structure and priorities of national security.

It has been established that information security is a set of measures and methods aimed at protecting the integrity of information systems from unauthorized access, alteration, theft, or destruction of information, as well as from breaches of its availability and confidentiality. An analysis was carried out of legal and regulatory documents that define and govern the field of information security in Ukraine, in particular the Law of Ukraine «On National Security,» the National Cybersecurity Strategy, and other official documents. International experience (USA, EU, Israel) was also examined, and its potential for adaptation to the Ukrainian context of hybrid information warfare was identified. Special attention was given to the threats to Ukraine's information space, manifested in cyberattacks, propaganda, fake news, and psychological influence through social networks and the Internet in general (websites, messengers, etc.).

Practical steps have been proposed to strengthen the system of information security, namely: the development of a separate Information Security Strategy of Ukraine, the promotion of national education in the field of information security, and the institutionalization of strategic communications at the level of state policy.

Keywords: information security, national security, cybersecurity, cyber defense, information sovereignty.

Стаття надійшла до редакції 03.06.25