

УДК 32:004.056

DOI <https://doi.org/10.32782/2312-1815/2025-20-4>

Андрій Пролорензо

ORCID: 0009-0008-3704-2219

КІБЕРБЕЗПЕКА В УКРАЇНСЬКИХ ЛІТЕРАТУРНИХ ДЖЕРЕЛАХ: ПОЛІТИЧНИЙ ОГЛЯД

У статті проаналізовано стан наукової розробленості теми кібербезпеки в українських літературних джерелах з акцентом на її політичному контексті. Установлено, що питання кібербезпеки активно вивчається в Україні, і ця тема знайшла своє відображення в численних дослідженнях різного рівня, як-от підручники, навчальні посібники, монографії, дисертації, наукові статті, тези доповідей та аналітичні дослідження.

Значне підвищення інтересу до цієї теми спричинено гібридною війною РФ проти України, а також повномасштабним вторгненням Росії. Це стимулювало експоненціальне зростання кількості публікацій, що свідчить про надзвичайну актуальність кібербезпеки в сучасних політичних умовах. Водночас у дослідженнях зберігається невизначеність щодо змістового наповнення ключових термінів, що значно ускладнює як наукове, так і практичне осмислення проблем кіберзагроз та побудови ефективної системи кіберзахисту. У статті висвітлюється необхідність подальшого вдосконалення теоретичної бази та розвитку досліджень з політичних аспектів кібербезпеки для забезпечення стійкості держави в цифрову епоху.

Ключові слова: кібербезпека, кіберзахист, національна безпека, українські літературні джерела.

Постановка проблеми. Переміщення конфліктів із традиційного фізичного простору в кіберпростір, яке спостерігається вже тривалий час, породжує нові загрози та виклики в аспекті забезпечення кібербезпеки нашої держави, особливо в умовах протидії агресору – російській федерації. Технології інформаційної війни приваблюють саме через відносну дешевизну, доступність та ефективність, а отже, інтенсивність їх використання тільки наростатиме. Своєю чергою, для проведення дослідження будь-якого спрямування важливим у сучасному світі є аналіз розробки наукової проблематики.

Аналіз останніх досліджень і публікацій свідчить, що питання кібербезпеки та кіберзахисту неодноразово привертало увагу українських дослідників – представників різних суспільних наук, серед яких: Д. Дубов, Ю. Завгородня, К. Захаренко, Є. Котух та багато інших. Однак більшість наукових праць має фрагментарний характер.

Мета статті – проаналізувати стан наукової розробленості теми кібербезпеки в українських літературних джерелах.

Виклад основного матеріалу. Питання кібербезпеки є предметом значної кількості українських досліджень, проведених у різні роки. Окремі аспекти цієї теми дослідники розглядали на рівні підручників та навчальних посібників, монографій, дисертацій, наукових статей, тез доповідей, аналітичних досліджень. Інструментарій аналізу динаміки наукових досліджень дає змогу виявити ключові тенденції та закономірності відповідного дослідження, виявити теми, сфери, що занепадають, і потенційні прогалини в дослідженнях, а також оцінити вплив окремих досліджень та дослідників у галузі, визначити потенційних співавторів на основі спільних дослідницьких інтересів і сфер знань. Зокрема, аналіз частоти ключових слів, авторів та джерел видання слугує дослідникам підґрунтям для точного визначення найвидатніших тем у літературі.

Наукову цінність у комплексному дослідженні теми кібербезпеки продемонстрували Д. Дубов та Ю. Завгородня, які зробили вагомий внесок у вивчення різних аспектів цього явища.

Д. Дубов у статті «Підходи до формування тезаурусу у сфері кібербезпеки» [2], яка присвячена проблемі впорядкування кібербезпекової термінології (кіберпростір, кібербезпека, кібератака, кібертероризм) та огляду підходів, наявних у цій сфері в практиці вітчизняних і західних досліджень. У статті «Стратегічні аспекти кібербезпеки України» [3] розглядаються ключові аспекти формування національної політики у сфері кіберзахисту, визначаються основні загрози в інформаційному просторі та пропонуються напрями для розробки стратегічних підходів до забезпечення кібербезпеки. У доповіді «Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України: аналітична доповідь» [4] автор аналізує роль державно-приватного партнерства в забезпеченні кібербезпеки, розглядаючи міжнародний досвід країн ЄС, США, Ізраїлю та інших, а також пропонує шляхи адаптації цих практик в Україні.

Ю. Завгородня у своїй статті «Кібербезпека як інноваційний захист у політичному просторі України» [5] акцентує увагу на цінності в сучасному інформаційному суспільстві ролі кібербезпеки. Зазначаючи, що система захисту, яка є в суспільстві, спрямована на врегулювання суперечностей, які виникають на рівні фактичного протистояння та суттєвого впливу на політичні процеси із чітко визначеними суб'єктами політичної активності, автор указує, що в політичному процесі невід'ємним елементом взаємодії є інформаційний простір, оскільки сучасна платформа для публічних взаємовідносин між суб'єктами політики переформатована під новітні способи, а тому й механізми впливу на громадян набувають інноваційного характеру та демонструють невизначену реакцію від суспільства й можливі шляхи розвитку політичних подій. З огляду на це виникає потреба сформуванню низки механізмів для захисту всіх користувачів кіберпростору, які беруть участь у публічному спілкуванні щодо важливих політичних питань. У статті Ю. Завгородньої «Історія становлення кібервійни як складової політичного процесу» [6] розглянуто розвиток кібервійни як важливого елементу сучасних політичних відносин. Автор аналізує історичний контекст зародження цього явища, починаючи від перших випадків використання кіберзасобів у військових і політичних цілях, і до їх перетворення на потужний інструмент впливу в глобальній політиці. Особливу увагу приділено механізмам реалізації кібервійни, які виходять за межі традиційного розуміння збройних конфліктів, перетворюючи кіберпростір на арену боротьби за політичний, економічний та інформаційний контроль. У дослідженні розкривається роль державних і недержавних акторів, зокрема приватних корпорацій, хакерських груп та міжнародних організацій, у процесах планування та здійснення кібератак. Стаття також торкається міжнародного виміру кібервійни, аналізуючи її вплив на геополітичну стабільність і національну безпеку різних країн. Особливий акцент зроблено на кібератаках як інструменті гібридної війни, що набули поширення в умовах сучасних конфліктів. Так, дослідження підкреслює важливість інтеграції кібервійни в наукове та практичне розуміння політичних процесів, а також необхідність формування ефективних стратегій кіберзахисту в умовах дедалі більших глобальних загроз. У статті Ю. Завгородньої «Можливості політики кіберзахисту в зовнішніх та внутрішніх процесах» [7] розглядається роль кіберзахисту як ключового елементу сучасної державної політики, спрямованого на забезпечення безпеки в умовах дедалі більших викликів у цифровому середовищі. Автор аналізує, як політика кіберзахисту інтегрується в зовнішньополітичну діяльність держави, сприяючи зміцненню її позицій на міжнародній арені, та у внутрішньополітичні процеси, забезпечуючи захист критичної інфраструктури, персональних даних громадян і державних ресурсів. Дослідження фокусується на важливості створення комплексної системи кіберзахисту, яка поєднує технічні, правові та організаційні заходи, спрямовані на протидію кібератакам і мінімізацію їх наслідків. Особливу увагу приділено аналізу викликів, пов'язаних зі стрімким розвитком технологій, зростанням кількості кібератак та активізацією гібридних загроз.

Дисертаційна праця Є. Котух «Теоретико-методологічні засади забезпечення кібербезпеки в публічному секторі» [9] обґрунтовує концептуальні засади забезпечення кібербезпеки в органах публічної влади, які поділяються на дві групи: виміри кібербезпеки (людський, організаційний, інфраструктурний, технологічний, нормативний) та дії, необхідні для забезпечення кібербезпеки (побудова онлайн-довіри, розвиток координації, співпраця та кооперація, профілювання кіберстану, сприяння впровадженню систем кібербезпеки).

Значний внесок у розвиток практичних аспектів кібербезпеки зробив В. Машталір та співавтори [10], які у своїх дослідженнях детально проаналізували питання кіберборотьби в умовах збройного протистояння. Автори розглядають кіберборотьбу як сукупність взаємоузгоджених за метою, завданнями, місцем та часом заходів визначених військ (сил), спрямованих на здобуття інформації про кіберінфраструктуру противника, її знищення всіма видами зброї або захоплення, заподіяння їй шкоди шляхом здійснення кібердій, проведення кібероперацій та радіоелектронного подавлення, захист своєї кіберінфраструктури від кіберрозвідки й кібердій противника.

У 2024 році опубліковано дослідження А. Худоля [11], присвячене аналізу сучасних викликів кібербезпеки перед Україною. Автор зазначає, що, за даними дослідження «Лабораторії Касперського», Україна посідає досить низькі позиції в рейтингу кібербезпеки серед 60 країн світу, що вимагає термінового вдосконалення систем кіберзахисту. Особлива увага приділяється аналізу кібератак на критичну інфраструктуру, зокрема банки, аеропорти, державну залізничну компанію, телекомпанії, мережеві супермаркети, енергетичні компанії, державні фіскальні служби, органи державної влади та місцевого самоврядування.

Великого значення для розвитку теоретичних засад кібербезпеки має дослідження Г. Гончаренко [1], яке пропонує комплексний підхід до визначення та розмежування базових дефініцій у сфері кібербезпеки. На основі аналізу широкого кола джерел, включно з дослідженнями Гарвардського університету та провідних міжнародних експертів, авторка пропонує чітке розмежування понять «інформаційна безпека» та «кібербезпека». За її визначенням, інформаційна безпека – це стан захищеності інформаційного середовища, що забезпечує конфіденційність, цілісність та доступність інформації незалежно від її форми. Водночас кібербезпека розглядається як підсистема інформаційної безпеки, зосереджена на захисті комп'ютерних систем, мереж і програмного забезпечення від цифрових загроз.

Особливу цінність у дослідженні Г. Гончаренко становить розроблена класифікація кібервразливостей, яка містить: вразливості політики, процесів і процедур; технічні вразливості; вразливості кінцевих пристроїв; вразливості, пов'язані з людським фактором; фізичні та екологічні вразливості. Авторка наголошує на важливості комплексного підходу до забезпечення кібербезпеки, який урахує всі ці аспекти та передбачає впровадження відповідних захисних механізмів.

Висновки. Підсумовуючи, варто зазначити, що аналіз літератури дає змогу виявити ключові тенденції та закономірності відповідного дослідження, потенційні прогалини в дослідженнях, а також оцінити вплив окремих досліджень і дослідників у галузі, визначити потенційних співавторів на основі спільних дослідницьких інтересів і сфер знань.

Зокрема, з'ясовано, що дослідження кібербезпеки та кіберзахисту, як загалом, так і окремих їх компонентів, було актуальним у різні роки. Однак ведення гібридної війни рф проти України, а також повномасштабне вторгнення росії на території нашої держави неабияк активізувало проведення досліджень з обраної теми. Експоненціальне зростання кількості публікацій свідчить про високу актуальність дослідження ролі кібербезпеки.

Водночас, незважаючи на те, що такі поняття, як «кібербезпека», «кіберзахист», «кіберпростір», «кібервійна», «кібератака» та «кібертероризм», широко використовують у науковій літературі, все ще є значна невизначеність щодо змістового наповнення цих термінів, що значно ускладнює наукове й практичне осмислення проблеми загроз у кіберпросторі. До того

ж варто констатувати, що більшість вітчизняних науковців досліджує питання кібербезпеки без урахування останніх законодавчих змін.

Література:

1. Гончаренко Г. А. До проблеми визначення та розмежування дефініцій «інформаційна безпека» і «кібербезпека». *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2024. С. 466–471.
2. Дубов Д. Підходи до формування тезаурусу у сфері кібербезпеки. *Політичний менеджмент*. 2010. № 5. С. 19–30.
3. Дубов Д. Стратегічні аспекти кібербезпеки України. Стратегічні пріоритети 4, 2013. С. 119–127.
4. Дубов Д., Бойко В., Гнатюк С., Ісакова Т., Ожеван М., Покровська А. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України: аналітична доповідь. Київ : НІСД, 2018. С. 81.
5. Завгородня Ю. В. Кібербезпека як інноваційний захист у політичному просторі України. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право*. 2021. Випуск 4(52). С. 33–38.
6. Завгородня Ю. В. Історія становлення кібервійни як складової політичного процесу // *Актуальні проблеми політики*. 2023. С. 42.
7. Завгородня Ю. В. Можливості політики кіберзахисту в зовнішніх та внутрішніх процесах. *Актуальні проблеми філософії та соціології*. 2024. С. 187.
8. Захаренко К. В. Інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири: дисертація на здобуття наукового ступеня доктора політичних наук : 23.00.02 / Національний педагогічний університет імені М.П. Драгоманова, Львівський національний університет імені Івана Франка, Львів, 2021. 421 с.
9. Котух Є. В. Теоретико-методологічні засади забезпечення кібербезпеки в публічному секторі: дисертація на здобуття наукового ступеня доктора наук з державного управління: 25.00.02 / Національний університет цивільного захисту України, Харків, 2022. 479 с.
10. Машталір В. В., Гук О. М., Мурашов Р. К., Фараон С. І., Лоза В. В. Кіберборотьба в умовах збройного протистояння: аналіз, стратегії та виклики. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2024. № 1(49). С. 93–104.
11. Худолій А. Кібербезпека: сучасні виклики перед Україною. *Acta de Historia & Politica: Saeculum XXI*. 2024. С. 138–146.

References:

1. Honcharenko, H. A. (2024). Do problemy vyznachennia ta rozmezhuvannia defynitsii “informatsiina bezpeka” i “kiberbezpeka” [On the problem of defining and distinguishing the definitions of “information security” and “cyber security”]. *Elektronne naukovye vydannia “Analitychno-porivnialne pravoznavstvo”*, 466–471.
2. Dubov, D. (2010). Pidkhody do formuvannia tezaurusu u sferi kiberbezpeky [Approaches to forming a thesaurus in the field of cyber security]. *Politychnyi menedzhment*, (5), 19–30.
3. Dubov, D. (2013). Stratehichni aspekty kiberbezpeky Ukrainy [Strategic aspects of Ukraine’s cyber security]. *Stratehichni priorytety*, (4), 119–127.
4. Dubov, D. V., Boiko, V., Hnatiuk, S., Isakova, T., Ozhevan, M., & Pokrovska, A. (2018). Derzhavno-privatne partnerstvo u sferi kiberbezpeky: mizhnarodnyi dosvid ta mozhlyvosti dlia Ukrainy: analitychna dopovid [Public-private partnership in the field of cybersecurity: International experience and opportunities for Ukraine: Analytical report]. Kyiv: NISD. (81 p.)
5. Zavhorodnia, Yu. V. (2021). Kiberbezpeka yak innovatsiinyi zakhyst u politychnomu prostori Ukrainy [Cyber security as an innovative protection in the political space of Ukraine]. *Visnyk NTUU “KPI”. Politolohiia. Sotsiolohiia. Pravo* [Bulletin of NTUU “KPI”. Political Science. Sociology. Law], 4(52), 33–38.
6. Zavhorodnia, Yu. V. (2023). Istoriia stanovlennia kiberviiyny yak skladovoi politychnoho protsesu [The history of the formation of cyberwar as a component of the political process]. *Aktualni problemy polityky* [Actual Problems of Politics], p. 42.

7. Zavorodnia, Yu. V. (2024). *Mozhlyvosti polityky kiberzakhystu v zovnishnikh ta vnutrishnikh protsesakh* [Opportunities for cyber defense policy in external and internal processes]. *Aktualni problemy filosofii ta sotsiologhii* [Current Problems of Philosophy and Sociology], p. 187.
8. Zakharenko, K. V. (2021). *Instytutsiinyi vymir informatsiinoi bezpeky Ukrainy: transformatsiini vyklyky, hlobalni konteksty, stratehichni oriientyry* [Institutional dimension of Ukraine's information security: Transformational challenges, global contexts, strategic guidelines] (Doctoral dissertation). National Pedagogical Dragomanov University & Ivan Franko National University of Lviv, Lviv, Ukraine. (421 p.)
9. Kotukh, Ye. V. (2022). *Teoretyko-metodolohichni zasady zabezpechennia kiberbezpeky v publichnomu sektori* [Theoretical and methodological foundations of ensuring cybersecurity in the public sector] (Doctoral dissertation). National University of Civil Protection of Ukraine, Kharkiv, Ukraine. (479 p.)
10. Mashtalir, V. V., Huk, O. M., Murasov, R. K., Faraon, S. I., & Loza, V. V. (2024). *Kiberborotba v umovakh zbroinoho protistoiannia: analiz, stratehii ta vyklyky* [Cyber struggle in the conditions of armed confrontation: Analysis, strategies, and challenges]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony* [Modern Information Technologies in the Sphere of Security and Defense], 1(49), 93–104.
11. Khudolii, A. (2024). *Kiberbezpeka: suchasni vyklyky pered Ukrainoiu* [Cybersecurity: Current challenges facing Ukraine]. *Acta de Historia & Politica: Saeculum XXI*, 138–146.

Prolorenzo Andrii. Cyber security in Ukrainian literary sources: a political review

The article analyzes the state of research on cyber security in Ukrainian literary sources, with a focus on its political context. It has been established that cyber security is actively studied in Ukraine, and this topic is reflected in numerous studies of various levels, including textbooks, educational manuals, monographs, dissertations, scientific articles, conference proceedings, and analytical reports.

The significant increase in interest in this topic was driven by Russia's hybrid war against Ukraine and the full-scale invasion of Russian forces. This has led to an exponential growth in the number of publications, highlighting the exceptional relevance of cyber security in modern political conditions.

At the same time, a lack of clarity remains in the conceptual definitions of key terms, which significantly complicates both the scientific and practical understanding of cyber threats and the development of an effective cyber defense system. The article emphasizes the need for further refinement of the theoretical framework and the advancement of research on the political aspects of cyber security to ensure the resilience of the state in the digital age.

Key words: cybersecurity, cyber defense, national security, ukrainian literary sources.

Відомості про автора:

Пролорензо Андрій – аспірант кафедри політичних наук,
Прикарпатський національний університет імені Василя Стефаника.