УДК 303+ 336.1
DOI: https://doi.org/10.32782/2786-8141/2025-10-7

Койбічук В. В.
кандидат економічних наук, доцент,
завідувач кафедри економічної кібернетики,
Сумський державний університет
ORCID: https://orcid.org/0000-0002-3540-7922
Vitalia Koybichuk
Sumy State University

Боженко В. В.
кандидат економічних наук, доцент,
доцент кафедри економічної кібернетики,
Сумський державний університет
ORCID: https://orcid.org/0000-0002-9435-0065
Victoria Bozhenko
Sumy State University

СТРУКТУРИЗАЦІЯ СВІТОВОГО НАУКОВОГО ДОРОБКУ ЩОДО РОЛІ ТА МІСЦЯ КІБЕРБЕЗПЕКИ У СИСТЕМІ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

STRUCTURING THE WORLD'S SCIENTIFIC RESEARCH FOR THE ROLE AND PLACE OF CYBERSECURITY IN THE SYSTEM OF ENSURING THE ECONOMIC SECURITY OF THE STATE

Анотація. *Дослідження спрямоване на структуризацію світового наукового доробку та системний огляд ролі та місця кібербезпеки у системі забезпечення економічної безпеки держави. Для цього застосовано комплексний бібліометричний та наукометричний аналіз на підґрунті масиву публікацій, отриманих за відповідним пошуковим запитом у базі даних Scopus загальним обсягом 1077, проіндексованих за період з 2004 року по вересень 2024 р. Поєднання сучасних інструментів бібліометричного аналізу (VOSviewer, SciVal), мови програмування R, програмного забезпечення R Studio, пакетів Shiny, Bibliometrix, igraph та їх відповідних бібліотек і функцій дозволило ретельно дослідили отриманий набір публікацій науковців світу, щоб виявити нові тенденції, ключові теми та прогалини в знаннях у означеній темі дослідження. Отже, на першому етапі згенеровано масив публікацій, що індексуються базою даних Scopus та експортовано в форматах csv та BibTex для подальшого аналізу. На другому етапі дослідження сформовано 8 тематичних кластерів у програмному забезпеченні VOSviewer та визначено хронологічну послідовність напрямків досліджень науковців світу щодо тематики ролі кібербезпеки в системі забезпечення економічної безпеки держави. Третім етапом визначено ключові наукові галузі щодо ролі кібербезпеки в системі забезпечення економічної безпеки держави, де вчені, дослідники, аналітики висвітлюють свої напрацювання. Такими галузями є інформатика, інженерія програмного забезпечення, комп'ютерні науки соціальні та повідкові науки. На четвертому етапі побудовано ряд бібліометричних метрик за допомогою програмного забезпечення R Studio, пакетів Shiny, Bibliometrix, igraph, а саме: деревоподібну карту, що відображає частоти використання ключових слів авторів; карту мережі співпраці дослідників за означеною темою; алювіальну діаграму, що відображає еволюцію досліджень ролі та місця кібербезпеки в системі забезпечення економічної безпеки держави; карту, що відображає ступінь розвитку теми та її значущість.*

Ключові слова: *кібербезпека, економічна безпека, системи інтелектуального аналізу даних, критична інфраструктура, бібліометричний аналіз.*

Abstract. *The study is aimed at structuring the world's scientific work and a systematic review of the role and place of cyber security in the system of ensuring the state's economic security. For this, a complex bibliometric and scientometric analysis was applied based on an array of publications obtained by a corresponding search query in the Scopus database with a total volume of 1077, indexed from 2004 to September 2024. A combination of modern bibliometric analysis tools (VOSviewer, SciVal), programming languages R, R Studio software, Shiny packages, Bibliometrix, igraph and their respective libraries and functions allowed to carefully examine the obtained set of publications of world scientists in order to identify new trends, key topics, and knowledge gaps in the specified research topic. Thus, at the first stage, an array of publications indexed by the Scopus database was generated and exported in CSV and BibTex formats for further analysis. In the second stage of the research, eight thematic clusters were formed in the VOSviewer software. The chronological sequence of research directions of world scientists on the topic of cyber security's role in ensuring the state's economic security was determined. The third stage defines key scientific fields regarding cyber security's role in ensuring economic security, in which scientists, researchers, and analysts highlight their developments. Such fields are computer science, software engineering, and social and behavioral science. In the fourth stage, several bibliometric metrics were constructed using the R Studio software, Shiny, Bibliometrix, and igraph packages, namely: a tree-shaped map showing the frequency of use of authors' keywords; a map of the cooperation network of researchers on the specified topic; an alluvial diagram reflecting the evolution of research on the role and place of cyber security in the system of ensuring the economic security of the state; a map reflecting the degree of development of the topic and its significance.*

Keywords: *cyber security, economic security, intelligent data analysis systems, critical infrastructure, bibliometric analysis.*

© Койбічук В. В., Боженко В. В., 2025

Постановка проблеми. Сучасний світ характеризується високим рівнем глобалізації та надзвичайно стрімким розвитком цифрових технологій. Ці процеси значно посилюють взаємозалежність економік різних країн та роблять їх більш вразливими до кібератак. Кібербезпека стає все більш гострою проблемою, яка турбує уряди, бізнес та громадян як в межах кожної країни, так і у всьому світі. Кіберзлочинність завдає суттєву шкоди економіці, спричиняючи як прямі фінансові втрати (від викупу даних або шахрайства), так і непрямі (втрата репутації, перебої в роботі). За результатами дослідження [1] прогноз у 2025 році вказує, що загальні збитки світової економіки від кіберзлочинності будуть сягати астрономічної суми в 10,5 трильйонів доларів США.

Розширення фінансової доступності визнано одним з найважливіших шляхів до економічного зростання і соціального розвитку. Однак, реалізація цієї мети в багатьох країнах ускладнена низкою факторів. Цифрова трансформація фінансового сектору виступає перспективним інструментом для подолання цих перешкод, оскільки вона дозволяє надавати фінансові послуги більш ефективно та доступно, стимулюючи економічну активність та покращуючи добробут населення [2]. Проте фінансова доступність і кібербезпека є двома сторонами однієї медалі. Для того, щоб забезпечити фінансову інклюзію, необхідно створити безпечне цифрове середовище. І навпаки, розвиток цифрових фінансових послуг сприяє підвищенню рівня кібербезпеки, оскільки стимулює розробку нових технологій захисту інформації, що в свою чергу, сприяє підвищенню рівня економічної безпеки держави в цілому.

Таким чином, розуміння хронології розвитку досліджень, що спрямовані на посилення економічної безпеки країн, та дослідження еволюції змін напрямків цифрового десятиліття сприяють формуванню їхнього стійкого «імунітету» до внутрішніх та зовнішніх загроз, протистоянню різноманітним викликам кібератак, кібершахрайств. Отже, систематизація знань дозволить підвищити рівень обізнаності суспільства та політичних діячів, громад щодо ролі та місця кібербезпеки в системі економічної безпеки держави.

Аналіз останніх досліджень та публікацій. Забезпечення економічної безпеки – це комплексна задача, яка вимагає зусиль держави, бізнесу та громадянського суспільства та залежить від великої кількості макро- та мікрофакторів, що визначають її стійкість. Останнє тенденції цифрового простору охоплюють майже всі сфери діяльності населення. Особливо слід підкреслити значущість ефективності аграрного сектору для підвищення економічної безпеки, адже стабільне забезпечення населення продуктами харчування зменшує залежність від імпорту, а стійке виробництво продуктів харчування допомагає стабілізувати ціни на продовольчі товари, що є важливим фактором соціальної стабільності. Отже, велику зацікавленість викликає робота науковців [3], що присвячена удосконаленню бізнес-процесів в агросекторі з урахуванням економічної безпеки, цифровізації, ризиків та штучного інтелекту. Ґрунтуючись на досвіді всесвітньо відомих компаній (John Deere, Agricultural Bank of China, Fruition Sciences, TE-FOOD і FieldView), що підтвердили ефективність цифрових технологій та інновацій у підвищенні ефективності та сталого розвитку агросектору, автори [3] пропонують шляхи підвищення ефективності агробізнесу шляхом впровадження сучасних технологій та інноваційних підходів, що спрямовані на впровадження новітніх цифрових технологій (блокчейну, штучного інтелекту) та автоматизації процесів. З одного боку це потрібно для точного землеробства та оптимізації виробничих процесів, зниження витрат та підвищення якості продукції, а з іншого – посилення захисту агропідприємств України від кібершахрайств та кібератак.

Слід акцентувати увагу на дослідженні [4], де науковці сформували комплексний підхід до виявлення знань про кібербезпеку за допомогою тематичного моделювання BERT з використанням багатоаспектного аналізу академічних (15751публікація з бази даних Web of Science) і галузевих джерел (5831 стаття з журналу Security Magazine за період з 2011 по 2023 рік). У результаті тематичного моделювання було виявлено три ключових макрокластери на основі публікацій WoS, що визначальними факторами формування місця кібербезпеки для посилення економічної безпеки є технології, розумні міста та освіта. А на підґрунті BERT аналізу публікацій з журналу було сформовано чотири макрокластери – захист організацій, громадська безпека, управління та освіта.

Актуальним та високонауковим є комплексне дослідження науковців [5], що присвячене аналізу поточного стану кіберзлочинності та її впливу на національну безпеку. Основну увагу автори зосереджують на виявленні ключових загроз у цифровому просторі та розробці стратегій їх запобігання та протидії з метою забезпечення безпеки держави. Аналізуючи динаміку та еволюцію кіберзагроз, дослідження [5] пропонує практичні рекомендації для державних органів та приватних компаній щодо забезпечення кібербезпеки. Особлива увага приділяється необхідності уніфікації методів захисту інформаційних систем та міжнародному співробітництву у сфері кібербезпеки. Автори підкреслюють, що кібербезпека в державному управлінні досягається шляхом уніфікації методів обміну даними, використовуючи транспортні протоколи, такі як HTTP.

Метою статті є структуризація світового наукового доробку щодо ролі та місця кібербезпеки у системі забезпечення економічної безпеки держави за допомогою комплексу інструментів бібліометричного та наукометричного аналізу: програмного забезпечення VOSviewer, аналітичної системи SciVal, мови програмування R Studio та пакетів Shiny, Biblioshiny, igraph.

Виклад основного матеріалу. Вхідною інформаційною базою для структуризації світового наукового доробку щодо ролі та місця кібербезпеки в системі забезпечення економічної безпеки держави є масив публікацій, що були проіндексовані в базі даних Scopus за останнє двадцятиліття, з 2004 року по вересень 2024 року. За запитом «економічна безпека та кібербезпека» було знайдено 1077 документів. На рис. 1 відображено динаміку публікаційної активності науковців світу за означений період.

Подальший аналіз з використанням програмного забезпечення VOSviewer (популярний програмний інструмент для візуалізації та аналізу мережі публікацій) дозволив згрупувати світовий наукового доробку щодо ролі та місця кібербезпеки у системі забезпечення економічної безпеки держави у 8 кластерів. Граф на рисунку 2 містить 474 вузла, що пов'язані між собою, загальна кількість зв'язків складає 17831 одиницю.

Для зручності аналізу сформовані кластери (рис. 2) марковані різними кольорами. Так, найбільший за

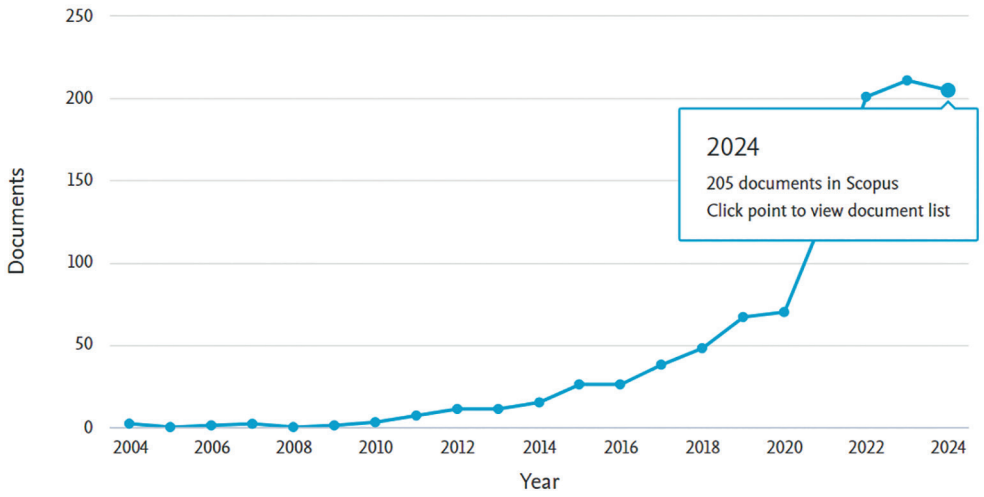

Рисунок 1 – Динаміка публікацій, що присвячені дослідженням ролі кібербезпеки у системі забезпечення економічної безпеки країни

Джерело: побудовано авторами засобами аналітичної системи БД Scopus

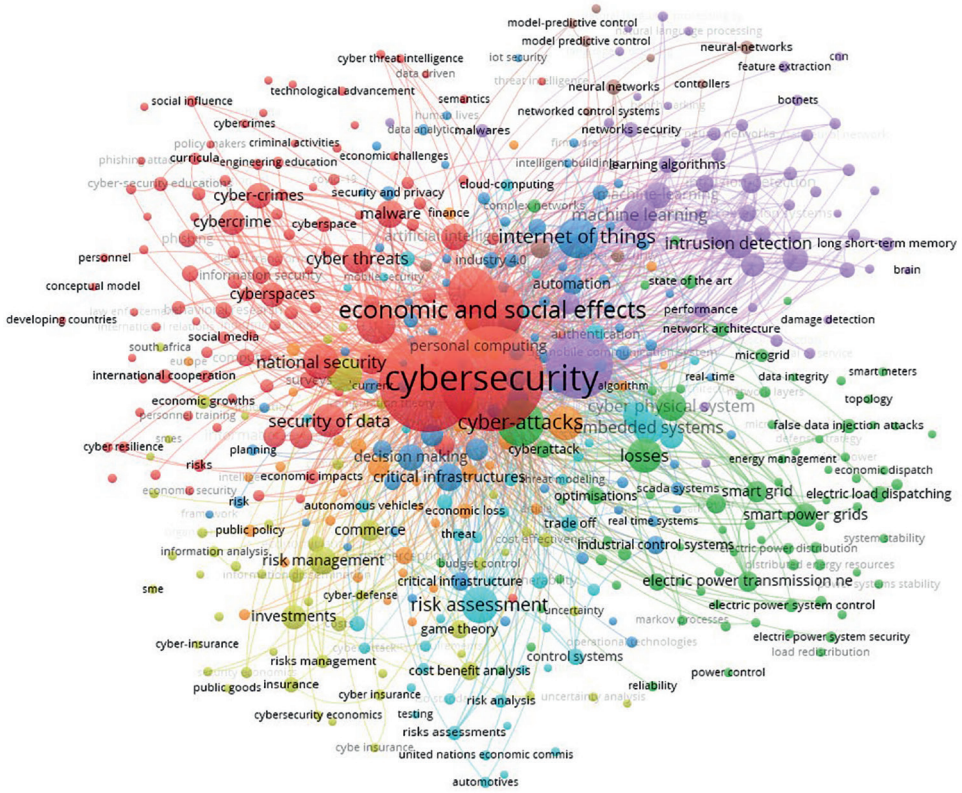

Рисунок 2 – Граф, що відображає взаємозв'язки між кібербезпекою та економічною безпекою держави за ключовими словами авторів

Джерело: побудовано авторами з використанням інструментів VOSviewer 1.6.15.

розміром по кількості ключових слів, це кластер червоного кольору (містить 108 елементів). Його основу складають дослідження, що пов'язані з кіберпростором, кіберстійкістю, кібербезпекою, кіберзагрозами, кіберкриміналом, цифровою криміналістикою, а також з великими даними, цифровими пристроями, цифровою економікою, питаннями безпеки, вимірами безпеки, безпеки систем та даних. Безумовно, збір, аналіз та захист великих даних є критично важливим для забезпечення економічної безпеки.

Група ключових слів, що позначена зеленим кольорам, містить 82 пункти. Поєднання ключових слів в цю групу пов'язане з питаннями потужності електричної мережі, електричним навантаженням та розподілом, електронною потужністю передачі а також з питаннями щодо безпеки енергетичних систем. Отже кластер зеленого кольору

охоплює публікації, що стосуються питань захисту критичної інфраструктури – енергетичних систем. Їх функціональність безпосередньо залежить від цифрових технологій, адже Автоматизація процесів, SCADA-системи (Supervisory Control And Data Acquisition, програмний пакет, призначений для збору, обробки, відображення та архівування інформації про технологічний процес в реальному часі, тобто це технологія, що дозволяє операторам моніторити та керувати різноманітними промисловими процесами, від виробництва енергії до управління трубопроводами), розумні мережі – все це робить енергетику вразливою до кіберзагроз та, як наслідок, послаблює національну безпеку держави. Отже кібербезпека енергетики є одним з найважливіших аспектів забезпечення економічної безпеки держави.

Синій колір характеризує кластер, що містить 79 ключових слів. Його основу складають дослідження, що пов'язані з технологіями блокчейну, розподіленими мережами, стандартами мобільного зв'язку 5-го покоління (5G), новітніми технологіями, інтелектуальними системами, інтернетом речей, екосистемами, розумними містами, прийняттям рішень, аналізом даних, теорією рішень, стратегіями безпеки, оцінюванням безпеки. Нові технології створюють як нові можливості, так і нові загрози. Для забезпечення економічної безпеки необхідно постійно розвивати нові методи захисту і адаптувати існуючі системи до нових умов.

Кластер жовтого кольору містить 53 ключових слова та об'єднує дослідження щодо економіки кібербезпеки, інвестицій в кібербезпеку, контролем бюджету, вартості, безпеки інвестицій, економічного аналізу, обчислювальної теорії, ризик-менеджменту. Узагальнюючи цей блок публікацій, відзначимо, що дослідження щодо необхідності інвестицій в галузь кібербезпеки визначають їх оптимальний рівень, враховуючи ризики, вартість захисту та потенційні збитки від кібератак. Дослідження щодо контролю бюджету спрямовані на розробку ефективних механізмів контролю за використанням бюджетних коштів, спрямованих на кібербезпеку, забезпечуючи прозорість і відповідальність. Економічний аналіз проведений науковцями для оцінювання впливу кібератак на різні сектори економіки та розроблення ефективних стратегії відновлення постраждалих галузей (секторів). Дослідження з обчислювальною теорією спрямовані на розробку нових методів захисту інформації та виявлення вразливостей в мережі та інформаційних системах. Дослідження в галузі ризик-менеджменту проводились для визначення ймовірності та наслідків кібератак, а також розроблення ефективних стратегій управління ризиками.

Основу досліджень, що увійшли до кластеру фіолетового кольору, формують теми, що пов'язані з використанням методів інтелектуального аналізу даних, дерев рішень, глибокого навчання, систем навчання, нейронних мереж для виявлення аномальних випадків кібератак, проблем збереження даних та розроблення прогнозів збитків від кібершахрайств. В цьому кластері знаходиться 52 ключових слова. Тож дана проблематика пов'язана з використанням штучного інтелекту для захисту від кібератак. Системи захисту, що використовують штучний інтелект, дозволяють перейти від реактивного до проактивного підходу до кібербезпеки, виявляючи загрози на стадії зародження. Ця тема не досліджена науковцями всебічно, є досить складною та важливою посилення економічної безпеки держави.

Кластер блакитного кольору має 48 ключових слів та присвячений дослідженням, що стосуються заходам від кібератак, що ґрунтуються на обізнаності населення, цільових груп щодо різних видів вірусів та типів кібератак, обізнаності щодо ISO стандартів, необхідності подвійної автентифікації, можливостям та особливостям хмарних технологій при збереженні та обміну даними, особливостям відкритих систем.

Помаранчевим кольором марковано кластер, що охоплює 40 ключових слів, та містить загальну тенденцію досліджень, що стосуються заходів держави для посилення захисту даних, безпеки даних, економічного впливу, формування у населення довіри до цифрового простору, а також публікації щодо оцінювання економічного прибутку та економічних втрат від кібервійн.

Восьмий кластер, помічений коричневим кольором, найменший за розміром. Тут всього 12 ключових слів, а публікаційна активність науковців спрямована на опис криптографічних алгоритмів для захисту від кібератак та забезпечення кібербезпеки, розроблення економічних моделей з використанням методів нейронного моделювання, захисту систем управління мережею для посилення економічної безпеки держави.

Візуалізація накладання додаткових шарів інформації поверх базової карти в VOSviewer дозволила отримати популяризацію тем та їх хронологію розвитку з роками (рис. 3).

Фіолетово-синій колір характеризує масив публікацій, що були проіндексовані у 2019–2020 роках та присвячений безпеці даних, національній безпеці, ризикам, публічній політиці, плануванню.

Синьо-блакитний колір відображає дослідження, що стосуються кіберпростору, економіки кібербезпеки, аналізу ризиків, контролю потужності мережі, контролю бюджету, прийнятті рішень та були опубліковані у 2020–2021 роках.

Наступний етап досліджень, що позначені блакитно-зеленим кольором еволюціонував у аналіз проблем щодо інвестицій в кібербезпеку, ролі соціальних мереж, індустрії 4.0, ризик-менеджменту, економічному впливу, міжнародному співробітництва для посилення кібербезпеки та стійкості національної безпеки (2021–2022 роки).

Далі більшість науковців досліджували (зелено-салатовий колір, 2022–2023 рр.) питання та проблеми кібератак, вірусів, втрати, інтернет речей, електричну потужність систем, публічні сервіси, кіберстійкість, розвідування кіберзагроз.

Салатово-жовтий колір (з 2023 року – по теперішній час) відповідає напрямкам щодо безпеки мережі, технологічному прогресу, нейромоделюванню, машинному навчанню, оптимізації процесів, менеджменту енергетичного сектору, цілісності даних, кіберкриміналу.

Наступним етапом дослідження є аналіз галузей, що є найбільш поширеними для публікації напрацювань науковців світу за останні п'ять років (з 2019 по 2023 рік) щодо ролі кібербезпеки в системі економічної безпеки. Такий аналіз проведено за результатами, отриманими в системі SciVal. За відповідним запитом ("cybersecurity in economic security") було знайдено 26 публікацій. Аналітичні інструменти SciVal дозволили сформувати розподіл публікацій за предметними галузями (рис. 4) та хмару ключових слів (рис. 5).

Трійку галузей з найбільшим обсягом публікацій обіймають галузь інженерії програмного забезпечення

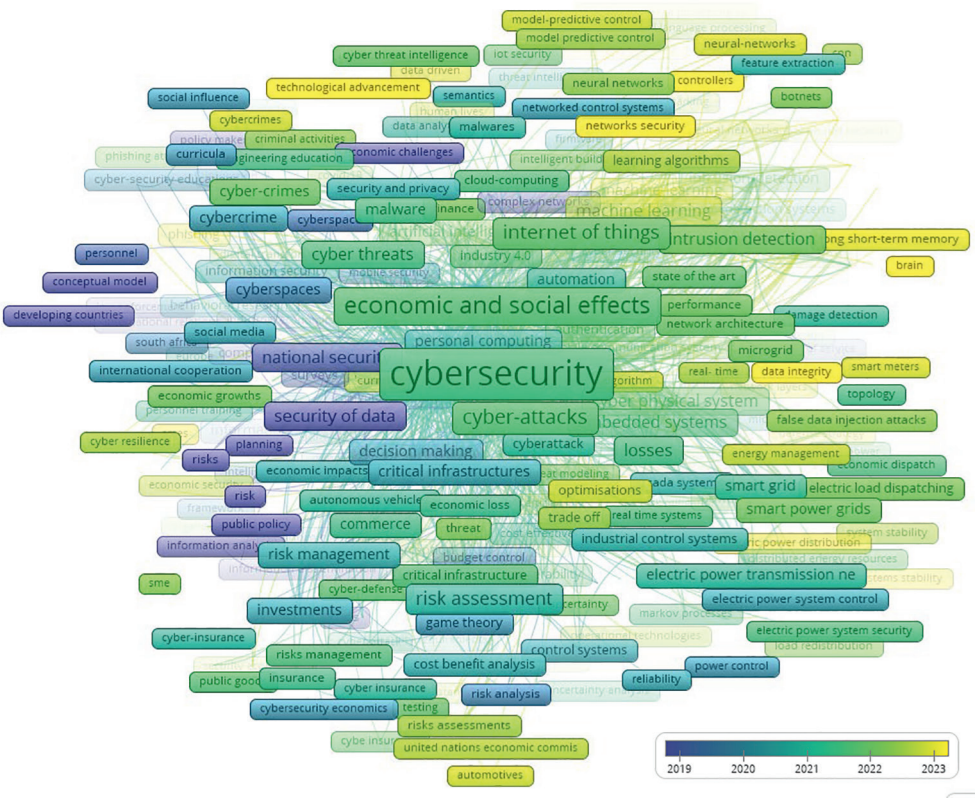

Рисунок 3 – Хронологічна послідовність напрямків досліджень науковців світу щодо тематики ролі кібербезпеки в системі забезпечення економічної безпеки держави.

Джерело: побудовано авторами з використанням інструментів VOSviewer 1.6.15.

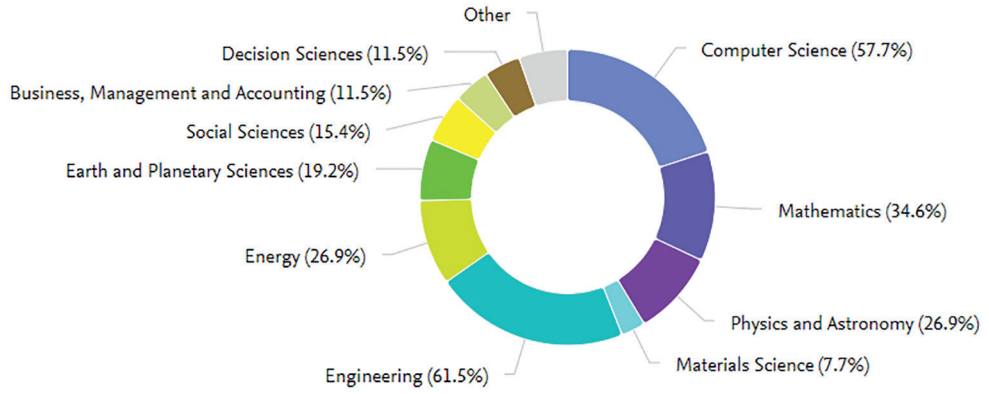

Рисунок 4 – Розподіл публікацій за предметними галузями

Джерело: побудовано авторами засобами SciVal 10.

(61,5%), комп'ютерних наук (57,7%) та математика (34,6%) зі знайденого масиву публікацій. Це цілком логічно, адже питання кібербезпеки безпосередньо пов'язане з використанням комп'ютерної техніки, програмного забезпеченні, інформаційних технологій та мереж передачі даних, мереж комунікацій (мобільного зв'язку чи супутникового), алгоритмів оброблення, передачі, збереження даних. Енергетичний сектор, фізика та астрономія охоплюють 26,9% публікацій. Такі результати збігаються з результатами бібліометричного аналізу засобами VOSviewer (публікації, що увійшли до кластеру зеленого кольору), тобто місце та роль кібербезпеки спрямована на захист енергетичної галузі, як об'єкта критичної інфраструктури, та сприяє посиленню економічної безпеки. Соціальні науки охоплюють 19,2% публікацій, а галузі бізнесу, менеджменту та обліку та наука про прийняття рішень охоплюють 11,5%, що теж корелює з результатами попереднього бібліометричного аналізу.

Хмару ключових слів за вибіркою 26 публікацій наведено на рисунку 5.

На рисунку 5 розмір шрифту ключового слова вказує на його значущість (чим більший розмір, тим більш значуще ключове слово або фраза, тобто використовується в більшості публікацій), а колір шрифту вказує на занепадання теми (блакитний), стабільність (дослідження постійно проводяться в аналізованому періоді – чорний колір шрифту) та зростання зацікавленості науковців

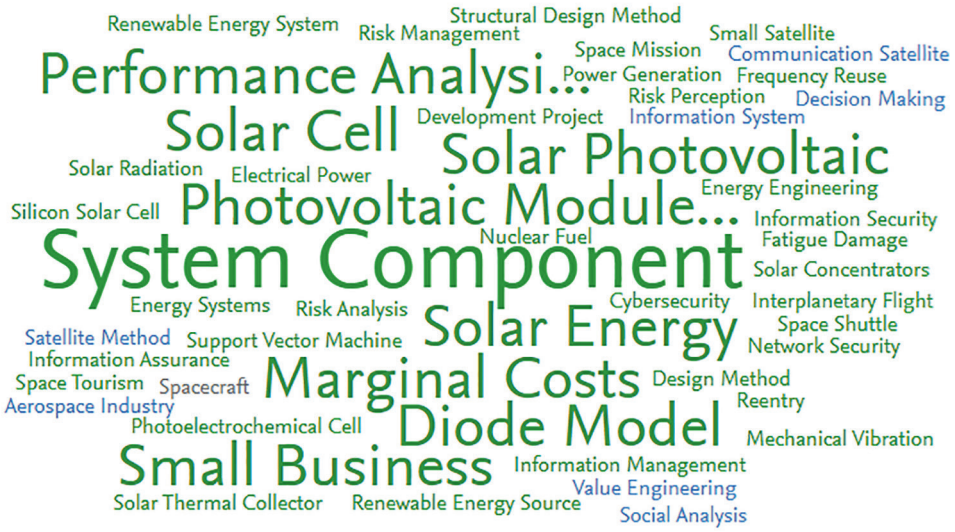

Рисунок 5 – Хмара ключових слів щодо ролі кібербезпеки в системі забезпечення економічної безпеки держави

Джерело: побудовано авторами засобами SciVal 10.

до означеної проблематики (зелений колір). Отже, більшість тем є актуальними для сучасної науки та підкреслюють зв'язок між кібербезпекою (напрямки, пов'язані з інформаційним менеджментом, аналізом ризиків, інформаційною безпекою, кібербезпекою) та економічною безпекою (малий бізнес аналіз продуктивності, функціональність та захист енергетичних систем).

Далі з метою структуризації світового наукового доробку щодо ролі та місця кібербезпеки у системі забезпечення економічної безпеки держави використано програмне забезпечення R Studio, пакети Shiny та Bibliometrix з їх відповідними бібліотеками та функціями. В результаті такого аналізу є можливість отримання різних типів мап (деревоподібної, алювіальної) та графів для комплексного аналізу означеної проблематики [6]. Вхідну вибірку масиву публікацій отримано за запитом «економічна безпека та кібербезпека» за 2004 року по вересень 2024 року, що проіндексовані наукометричною базою даних Scopus, яку попередньо було застосована для побудови мережевого графа засобами VOSviewer. Кожне з цих програмних забезпечень, як VOSviewer, так і пакет Bibliometrix має свої унікальні особливості, а їх поєднання дозволяє провести комплексний, всебічний, ґрунтовний аналіз щодо тематики дослідження.

Загальну інформацію для подальшого бібліометричного аналізу засобами R Studio та пакету Bibliometrix відображено на рисунку 6.

Рисунок 7 відображає деревоподібну карту, що згенерована на підгрунті частот найбільш вживаних ключових слів – Keyword Plus, тобто ключових слів, отриманих з назв посилань, цитованих у конкретній статті. В параметрах Bibliometrix за власною ініціативою авторів було встановлено 70 Keyword Plus.

Аналіз ключових тенденцій та напрямів досліджень (рис. 7) свідчить про лідерство та номінанту позицію публікацій, що присвячені кібербезпеці в цілому (14%), безпеці мережі (7%), економічним та соціальним ефектам (5), комп'ютерному криміналу (3%), кібератакам (3%), оцінюванню ризиків (2%), національній безпеці (2%), економіці (2%), безпеки даних (2%) та безпеки в цілому (2%). Зазначимо, що вказані відсотки відносяться лише до топ 70 ключових слів плюс, що були обрані авторами в якості тестового масиву. А інша частина публікацій присвячена методам та технологіям, що сприяють підвищенню рівня кібербезпеки держави.

Інформативним та змістовним є аналіз вхідного масиву публікацій за розподілом на категорії та напрямки досліджень, що відображаються в Інтернет просторі (рис. 8). Такий аналіз дозволяє здійснити пакет igraph мови R Studio. В результаті його застосування розраховуються мережеві показники: обчислюйте різні мережеві показники (ступінь розподілу публікацій, коефіцієнт кластеризації, показники центральності), а також визначаються найкоротші шляхи для розуміння інформаційних потоків або впливу досліджень у мережі.

Рисунок 6 – Узагальнена статистика щодо аналізованого масиву публікацій щодо ролі кібербезпеки в системі забезпечення економічної безпеки держави

Джерело: побудовано авторами з використанням програмного забезпечення R Studio, пакету Bibliometrix.

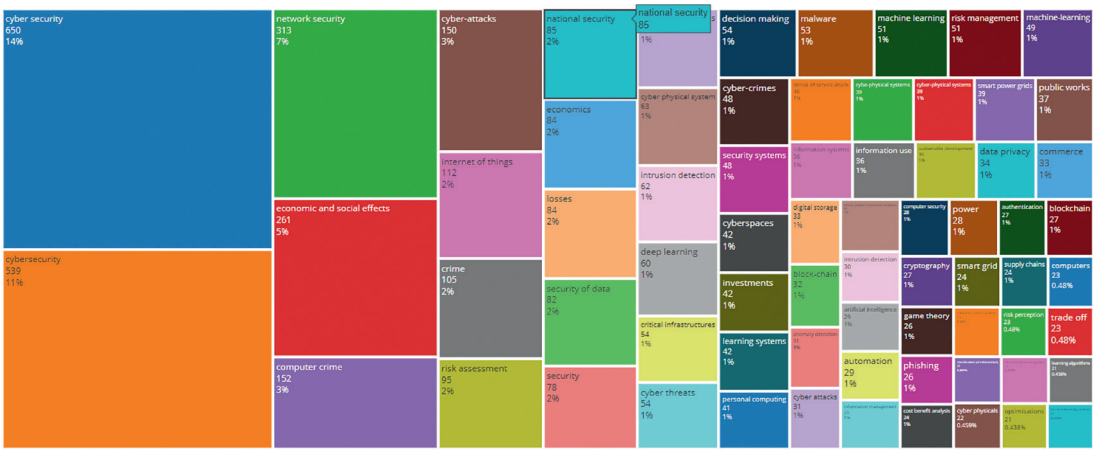

Рисунок 7 – Деревоподібна карта ключових слів щодо ролі та місця кібербезпеки в системі забезпечення економічної безпеки держави.

Джерело: побудовано авторами з використанням програмного забезпечення R Studio, пакету Bibliometrix

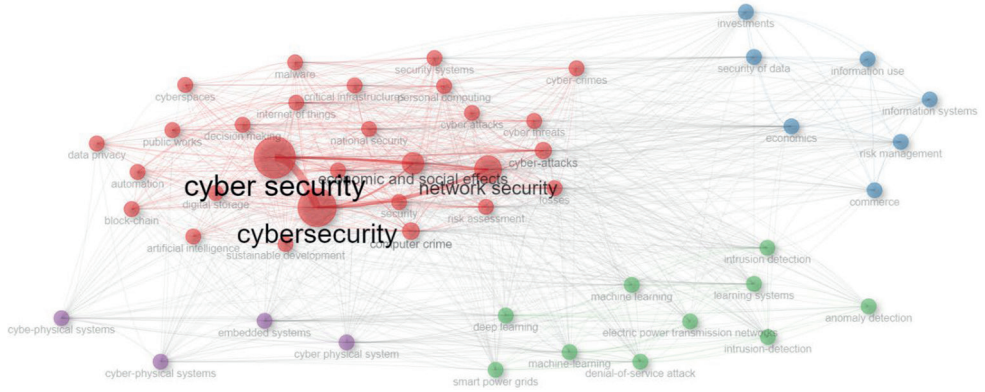

Рисунок 8 – Колаборційна активність науковців за напрямами досліджень щодо ролі та місця кібербезпеки у системі забезпечення економічної безпеки держави

Джерело: побудовано авторами з використанням програмного забезпечення R Studio пакету Bibliometrix

Результати (рис. 8) свідчать про угрупування наукових інтересів дослідників та міжкатегоріальний характер їхніх досліджень, що стосуються ролі та місця кібербезпеки в системі забезпеченні економічної безпеки держави.

Перша категорія (дослідження, що марковані червоним кольором) орієнтована на питання посилення національної безпеки та протидії кібератакам, вірусам, шахрайським схемам. Друга (зелений колір) – інноваційним технологіям що дозволяють виявляти аномальні поведінки шахраїв з використанням відповідного програмного забезпечення (штучний інтелект, глибоке навчання). Третя категорія стосується питань інвестицій в кібебербезпеку та оцінювання ризиків, електронної комерції (блакитний колір тематик дослідження). Четверта – це категорія, що пов'язана з організацією кіберфізичних систем (фіолетовий колір).

Для візуалізації змін в категоріальних даних з плином часу побудовано алювіальну діаграму (рис. 9), та дозволила проаналізувати як ключові слова змінювались з часом та «протікали» між категоріями з часом.

Отже, тематика еволюцій 2004–2020 рр. у 2021–2024 рр., що відображена на алювіальній діаграмі (рис. 9), така:

– оцінювання та конфіденційність, ризики перетікають в безпеку;

– критична інфраструктура, кіберзагрози, кіберстрахування – в кібербезпеку;

– ризики та кіберризики – в критичну інфраструктуру;

– великі дані – в кібербезпеку, соціальні мережі, економічний вплив;

– кібербезпека так і залишилась в тематиці кібербезпеки, також еволюціонувала в інформаційні технології, розвідувальний аналіз кіберзагроз, критичну інфраструктуру та безпеку мережі;

– кіберфізичні системи – в кібератаки та критичну інфраструктуру;

– національна безпека – в циркулярну економіку, кібербезпеку, економічну безпеку;

– кібербезпекова освіта – так і залишилась, освітою в галузі кібербезпеки.

При цьому бачимо також, що певні теми, наприклад, такі, як ризики (в безпеку, критичну інфраструктуру), штучний інтелект (кібербезпека, розвідування кібербезпеки) еволюціонували в декілька напрямів. Щільність потоку, що характеризує ступінь еволюції, визначається шириною смуги, що з'єднує відповідні категорії ключових слів.

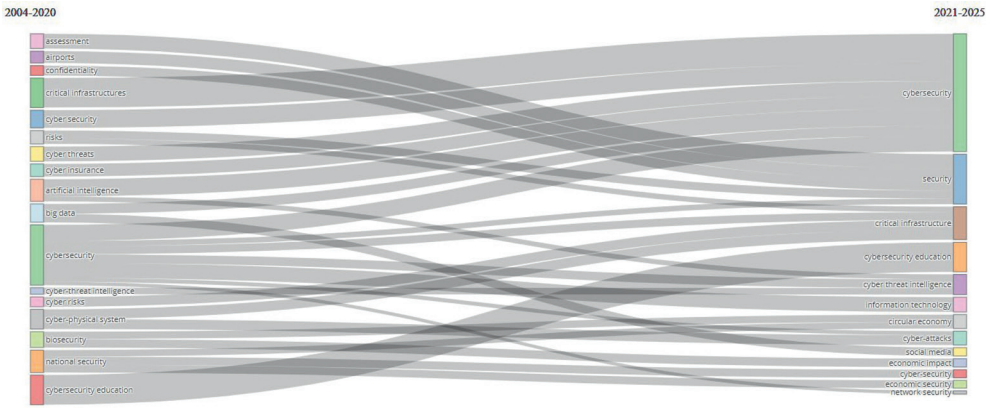

Рисунок 9. Еволюція досліджень ролі та місця кібербезпеки в системі забезпечення економічної безпеки держави

Джерело: побудовано авторами з використанням програмного забезпечення R Studio, пакету Bibliometrix

Цікавим також та високорелевантим є аналіз ключових слів за розподілом їх на теми, що є базовими, темами, що занепадають або розвиваються, теми які містять багато не розкритих питань (нішеві теми), та теми, що інтенсивно розвиваються, є двигунами сучасного наукового світу. Такий розподіл наведено на рисунку 10.

Горизонтальна вісь (рис. 10) відображає ступінь значущості тем, а горизонтальна – ступінь розвитку (щільність). Координати тем відображають міру належності до певної зони.

На рис. 10 відсутні напрямки досліджень в розрізі ролі та місця кібербезпеки в системі забезпечення економічної безпеки, до яких науковці втратили інтерес, лівий нижній кут порожній. Проте бачимо «перетікання» до базових, тобто таких, що постійно досліджуються, та зростання зацікавленості щодо ролі кіберфізичних систем, інформаційних технологій, освіти в сфері кібербезпеки, розвідувальної аналітики в сфері кіберзагроз, економічної безпеки та економічного впливу.

До нішевих тем (рис. 10) увійшли теми, що стосуються циркулярної економіки, захисту та безпеки даних, адже останні п'ять років супроводжувались аномальною кількістю та різновидами шахрайських схем та політичною нестабільністю, економічними кризами для певною групи країн та їх роллю на міжнародній арені. А з розвитком епохи 5 G, data mining, штучного інтелекту питання захисту даних, економічної безпеки, національної безпеки, кіберзахисту потребують безперервного моніторингу та контролю.

Домінантними темами дослідження є критична інфраструктура, приватність даних, оцінювання ризиків (правий верхній кут рис. 10).

Висновки. Комплексний бібліометрико-наукометричний аналіз світового наукового доробку щодо ролі та місця кібербезпеки у системі забезпечення економічної безпеки держави показав, що, по-перше, кібербезпека є стратегічним імперативом та має міждисциплінарний характер, що такі галузі, як інформатика, інженерія програмного забезпечення, комп'ютерні науки, соціальні та поведенкові науки. Міждисциплінарний підхід має важливе значення для вирішення багатогранних викликів, що породжують кіберзагрози.

По-друге, проведене дослідження однозначно визначає кібербезпеку як наріжний камінь економічної безпеки. Зростаюча залежність від цифрових технологій та їх динамічного розвитку зробила економіки країн вразливими до кібератак, що підкреслює потребу в надійних заходах кібербезпеки. Особливої уваги для захисту від кібершахрайств та посилення стійкості та захисту національної безпеки країн потребують галузі критичної інфраструктури, зокрема енергетичні мережі, а також фінансові системи.

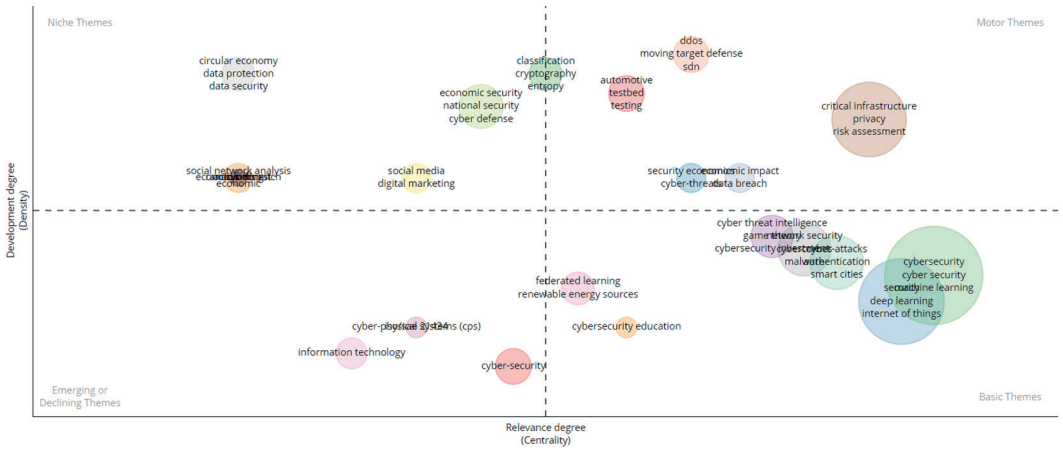

Рисунок 10 – Ступінь розвитку та значущість тем щодо ролі та місця кібербезпеки у системі забезпечення економічної безпеки держави

Джерело: побудовано авторами з використанням програмного забезпечення R Studio, пакету Bibliometrix

По-третє, слід підкреслити роль новітніх технологій, що використовують інтелектуальний аналіз даних, блокчейн-технології, штучний інтелект, методи машинного навчання в системі забезпечення економічної безпеки держави. Ці технології пропонують нові автоматизовані інструменти та підходи для виявлення нових загроз в стадії їх зародження, дозволяють оперативно керувати процесами в режимі реального часу, упереджуючи потенційні загрози. А глобальний характер кіберзагроз, по-четверте, вимагає міжнародного співробітництва для розробки ефективних стратегій кібербезпеки та вирішення спільних проблем.

По-п'яте, дослідження підкреслює необхідність постійних інвестицій у сферу кібербезпеки та освіту в галузі кібербезпеки для протистояння сучасним викликам кіберпростору та розробка надійних структур управління кібербезпекою.

Бібліографічний список:

1. Dalei, N., Kandpal, V. (2024). Understanding the Global Landscape of Cybersecurity Risks, Economic Impacts, and Challenges: Lesson for India. *Cybersecurity, Law, and Economics: The Case of India.* Book Chapter, P. 17–37. DOI: http://doi.org/10.4324/9781003517290-4

2. Maatallah, M. (2024). The Role of Digital Transformation in Enhancing Financial Inclusion: Unveiling the Economic and Social Challenges from Residents' Perspective. *SocioEconomic Challenges,* 8(3), 93–107. DOI: https://doi.org/10.61093/sec.8(3).93-107.2024

3. Zelisko, N., Raiter, N., Markovych, N., Matskiv, H., Vasylyna, O. (2024). Improving business processes in the agricultural sector considering economic security, digitalization, risks, and artificial intelligence. *Ekonomika APK,* 31 (3). P. 10–21. DOI: http://doi.org/10.32317/2221-1055.2024030.10

4. Alqurashi, F., Ahmad, I. (2024). A data-driven multi-perspective approach to cybersecurity knowledge discovery through topic modelling. *Alexandria Engineering Journal,* 107. P. 374–389. DOI: http://doi.org/10.1016/j.aej.2024.07.044

5. Ievdokymov, V, Frikel, A., Polishchuk, V., Savchuk, S., Klimova, I. (2024). Cybercrime and Information Protection in the Field of State Security: Current Threats and Measures for their Prevention. *Economic Affairs (New Delhi).* 69. P. 61–69. DOI: http://doi.org/10.1016/j.aej.2024.07.044

6. Aria, M. and Cuccurullo, C. (2017). Bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Informetrics,* Vol. 11(4), P. 959–975.

Стаття надійшла до редакції 01.02.2025