DOI: https://doi.org/10.26642/sas-2024-6(6)-103-115
УДК 351

Соха Станіслав
кандидат юридичних наук, докторант,
Державний університет «Житомирська політехніка»
https://orcid.org/0009-0004-2606-1263

Савчук Сергій
здобувач
Державний університет «Житомирська політехніка»
https://orcid.org/0009-0007-7436-0702

Здибель Роман
аспірант
Державний університет «Житомирська політехніка»
https://orcid.org/0009-0009-7618-0961

Сучасний стан наукових досліджень з проблем державної кримінально-правової політики протидії кіберзлочинності

Анотація. Автори цієї статті комплексно вивчають сучасний стан наукових досліджень з проблем державної політики протидії кіберзлочинності. Бібліометричний аналіз як один із методів наукового дослідження дозволяє оцінити рівень вивчення цієї проблеми та є запорукою її подальших досліджень.

У цій статті проаналізовано наукові публікації бази даних *Scopus* за ключовими словами «*cyber security*», що означає кібербезпека. Зокрема, за допомогою цифрових інструментів *Scopus* та *Biblioshiny* було визначено: динаміку кількості статей у базі даних *Scopus* за пошуковим запитом «*cyber security*» за 1998–2024 рр. в часовому та географічному вимірах; 20 найбільш релевантних (5 і більше публікацій) країн, з якими афілійовані автори публікацій, та їх метрики; структуру публікаційної активності; джерела фінансування наукових досліджень; градацію наукових публікацій за приналежністю до організацій; загальну кількість цитувань журналів у сфері кібербезпеки; застосування закону Бредфорда до джерел, що спеціалізуються на тематиці кібербезпеки; тематичну мапу авторських ключових слів у сфері кібербезпеки; факторіальний аналіз авторських ключових слів у сфері кібербезпеки; 10 найбільш поширених ключових слів авторів та дерево цих слів у сфері кібербезпеки.

Відповідно до здійсненого аналізу зроблено такі висновки: захист критичної інфраструктури, боротьба з кіберзлочинністю та запобігання кібератакам є фундаментальними категоріями кібербезпеки, адже найбільша кількість публікацій присвячена їм; кіберзагрози є глобальними викликами сучасності, а тому спостерігається високий рівень публікацій у міжнародних журналах; аналіз наукової літератури засвідчує важливість подальших досліджень у галузі кібербезпеки задля вдосконалення державної політики, спрямованої на посилення захисту кіберпростору та забезпечення стійкості економіки в умовах сучасних викликів.

Ключові слова: «cyber security»; кібербезпека; Scopus; Biblioshiny; цифрові інструменти; база даних; кіберзлочинність; державна політика.

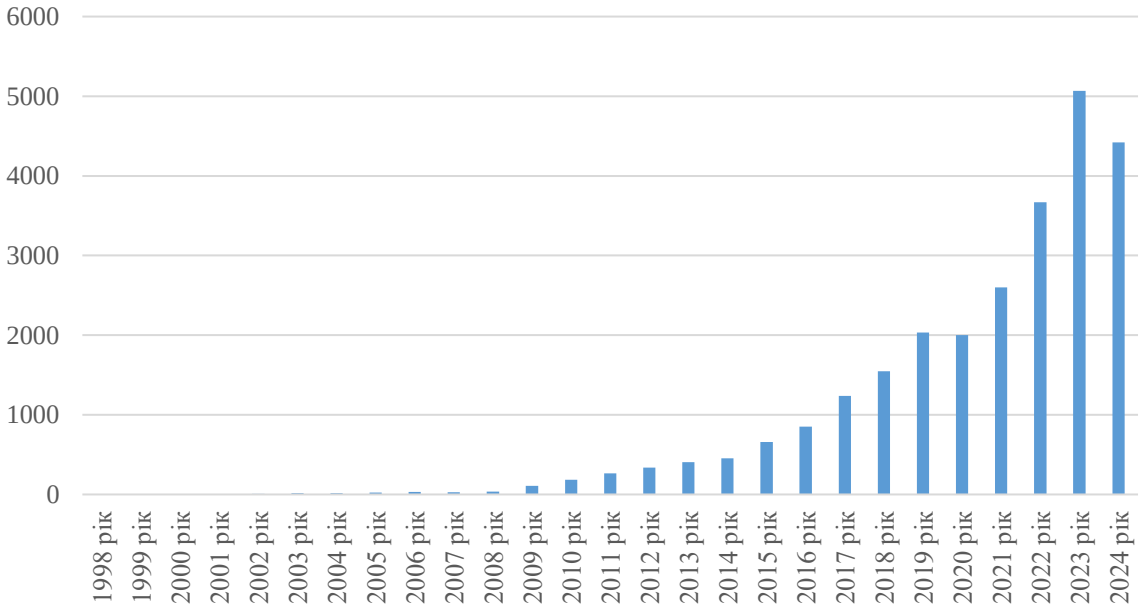
Актуальність теми. Бібліометричний аналіз є потужним інструментом оцінювання наукового впливу публікацій та авторитетності вчених. Проведення бібліометричного аналізу відкриває нові можливості для подальших наукових досліджень. Зокрема, глибоке вивчення цитування публікацій допоможе визначити найбільш впливові роботи та наукові школи, що формують сучасне розуміння ролі кібербезпеки у зміцненні економічної безпеки. Виявлення наукових спільнот дозволить з'ясувати, які школи найбільш активно досліджують цю проблематику та взаємозв'язки між ними.

Аналіз останніх досліджень і публікацій. Дослідженням сутності поняття «кіберзлочину» з урахуванням характеристики основних видів кіберзлочинів займалися як вітчизняні, так і зарубіжні науковці: В.Р. Атамась, О.М. Сокуренко [1], В.Бутузов [2], С.Буяджи [3], А.Ю. Ковальчук [4], І.Коцман [5], Т.Д. Лисько [6], В.В. Пивоваров, С.Ю. Лисенко [7], І.О. Харитоненко [8] та інші. Проте сучасний стан наукових досліджень з проблем державної політики протидії кіберзлочинності вимагає глибшого аналізу.

Мета статті полягає у вивченні сучасного стану наукових досліджень з проблем державної політики протидії кіберзлочинності.

Викладення основного матеріалу. Науково-теоретичною базою досліджень стали наукові публікації бази даних *Scopus* за ключовими словами «*cyber security*», що означає кібербезпека. Спочатку була зроблена вибірка з 33436 документів, пізніше її було вирішено обмежити за ключовими словами до 26164 документів. Дані, отримані з бази *Scopus,* дозволяють ідентифікувати ключові тенденції у дослідженні кібербезпеки, а також визначити основні напрями, що перебувають у фокусі наукової спільноти. Встановлено, що особлива увага приділяється дослідженням, пов'язаним із захистом критичної інфраструктури, боротьбою з кіберзлочинами, забезпеченням конфіденційності та захистом даних. Аналіз ключових публікацій допомагає з'ясувати, які інституції та автори є найбільш активними та впливовими у цій галузі, що сприяє формуванню загальної картини наукового розвитку досліджуваної проблематики.

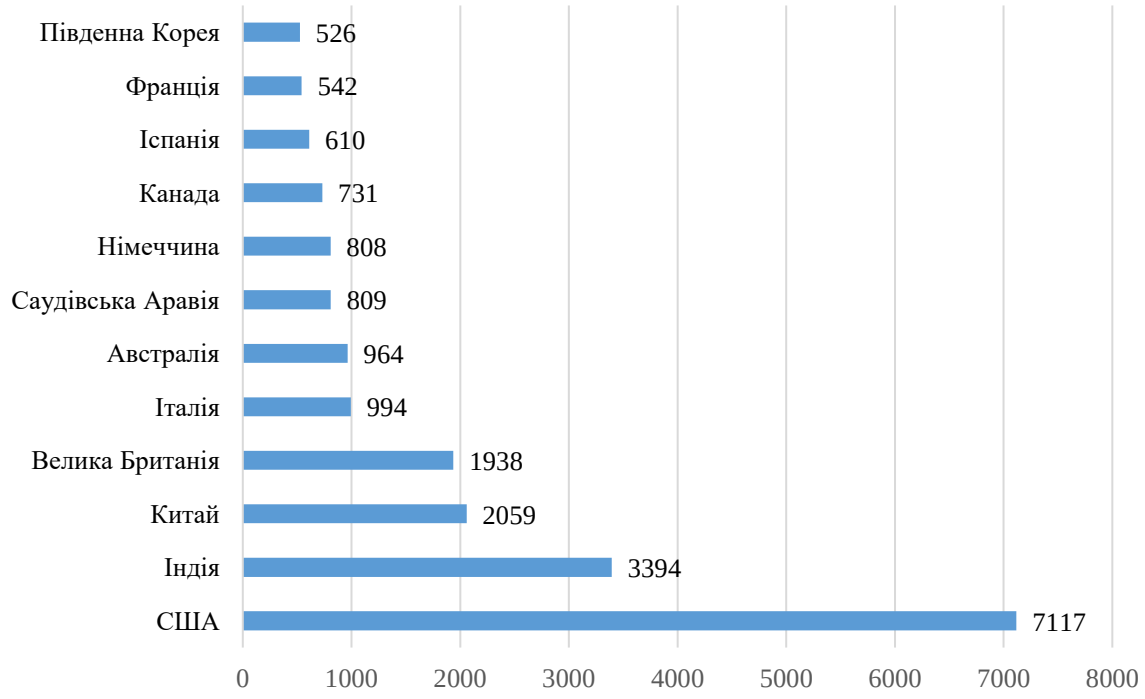
Крім того, проведення бібліометричного аналізу дозволяє відстежити еволюцію понять та концепцій у сфері кібербезпеки, зокрема в контексті їх взаємозв'язку з економічною безпекою. Сюди входить ідентифікація нових підходів, інноваційних рішень та перспективних технологій. Знаходження взаємозв'язків між науковими школами та їхнім внеском у формування політик кібербезпеки сприятиме розширенню міждисциплінарного підходу. Результати такого аналізу можуть використовуватися для вдосконалення державної політики, спрямованої на посилення захисту кіберпростору та забезпечення стійкості економіки в умовах сучасних викликів. Рисунок 1 показує динаміку публікацій у сфері кібербезпеки за 1998–2024 рр., що демонструє зростаючий інтерес наукової спільноти до проблеми кібербезпеки.



Джерело: сформовано автором на основі вбудованого інструментарію Scopus

Рис. 1. Динаміка кількості статей у базі даних Scopus за пошуковим запитом «cyber security» за 1998–2024 рр., часовий вимір

Розвиток кібербезпеки як окремої галузі досліджень бере свій початок наприкінці XX ст. Однією з перших наукових робіт, що визначила основи для формування цього напряму, стала робота A.Bequai, опублікована у 1998 р. Комісія президента Клінтона із захисту критичної інфраструктури відреагувала на основні положення дослідження і попередила, що США можуть бути вразливими до кіберпросторової версії атаки на Перл-Харбор. Вона надала рекомендації, аби уникнути цієї неминучої проблеми. Однак, наголошуючи на потребах модернізації високотехнологічних потреб Америки в безпеці, Комісія не звернула уваги на основні недоліки, які лежать в основі американської політики та плануванні у сфері високотехнологічної безпеки [10].



Джерело: сформовано автором на основі вбудованого інструментарію Scopus

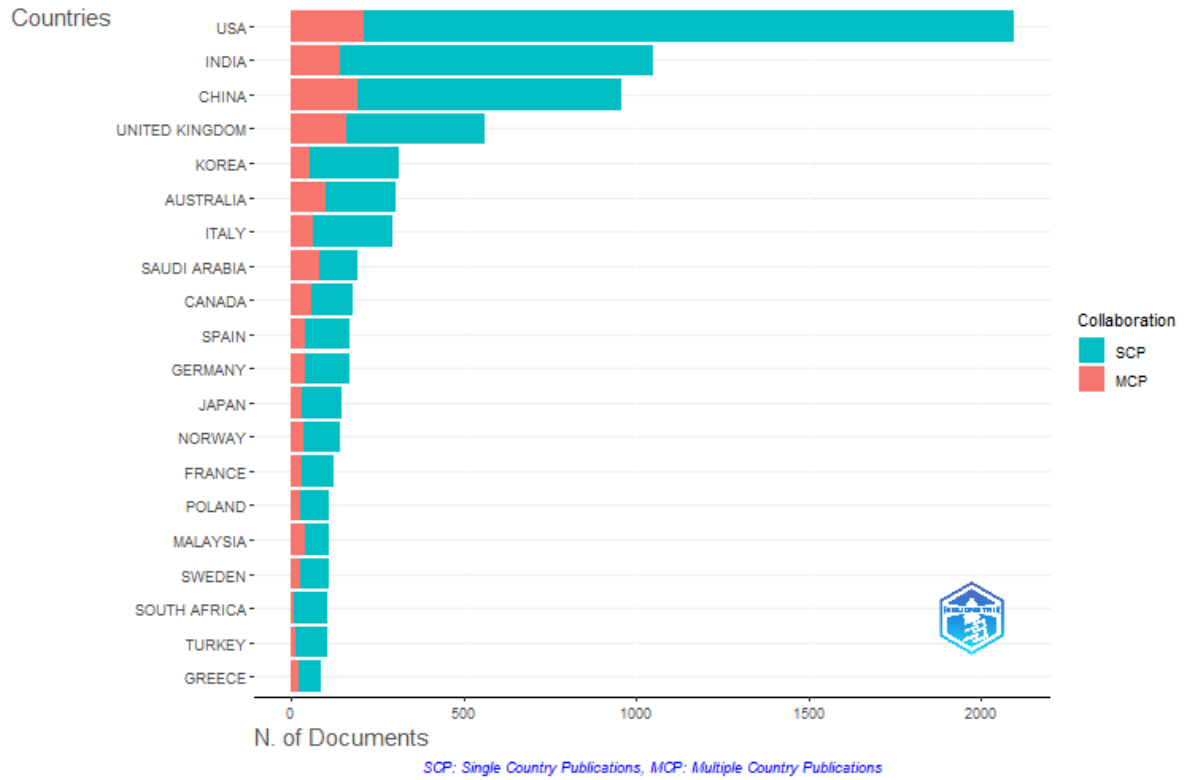
Рис. 2. Динаміка кількості статей у базі даних Scopus за пошуковим запитом «cyber security» за 1998–2024 рр., географічний вимір

Дані рисунку 2 свідчать, що найбільша кількість публікацій за пошуковим запитом «cyber security» належить науковцям зі Сполучених Штатів Америки, які репрезентували 7117 статей. На другому місці знаходиться Індія з 3394 публікаціями, яких майже вдвічі менше, ніж у США. Третє місце посідають китайські вчені, які опублікували 2059 робіт, а науковці Великої Британії надали 1938 публікацій. Італія та Австралія мають однаковий показник 964 статті, тоді як Саудівська Аравія та Німеччина майже зрівнялися у своєму внеску, опублікувавши 809 та 808 робіт відповідно. Канадські дослідники репрезентували 731 публікацію, іспанські – 610, французькі – 542, а південнокорейські – 526. Окремо слід відзначити внесок українських вчених, які опублікували 371 роботу з досліджуваної теми.

Серед вітчизняних напрацювань особливої уваги заслуговують дослідження А.Бойка, О.Бойка, В.Шендрика «Інформаційні системи для управління ланцюгами поставок: невизначеності, ризики та кібербезпека», які розкривають поточний стан та перспективи використання інформаційних систем для управління ланцюгами поставок компаній з багатокомпонентним виробництвом. У статті наведено якісний метод дослідження ланцюга поставок та визначення шляхів його інформаційного забезпечення. Автори зробили висновок, що для визначення найбільш ефективних стратегій інформаційної підтримки ланцюга поставок увага повинна бути зосереджена на ідентифікації та управлінні джерелами невизначеності, ризиків та кібербезпеки. Щоб успішно інтегрувати бізнес-процеси між постачальниками та клієнтами, виробники повинні вирішити складну проблему інформаційної безпеки. Основними практичними результатами є: новий підхід до ідентифікації та прогнозування ризику поставок в умовах невизначеності; комплексне рішення для захисту даних в інформаційних системах для управління ланцюгами поставок [11].

Використання бібліометрії поступово поширюється на всі наукові дисципліни, що робить її особливо ефективною для наукового картографування. Це актуально в умовах зростання обсягу, фрагментації та суперечливості дослідницьких потоків, викликаних акцентом на емпіричних внесках. Водночас процес наукового картографування є складним і багатоступеневим, оскільки передбачає використання різних програмних інструментів, які часто є платними або потребують специфічних знань для роботи.

У цій роботі ми застосуємо інструмент з відкритим кодом bibliometrix, який дозволяє виконувати комплексний бібліометричний аналіз. Цей інструмент забезпечує широкий спектр функцій для наукового картографування, що містить аналіз цитування, визначення ключових тем і авторів, а також візуалізацію взаємозв'язків між ними [9]. Використання bibliometrix забезпечує доступність і прозорість аналізу, що сприятиме створенню обґрунтованих наукових висновків (рис. 3).



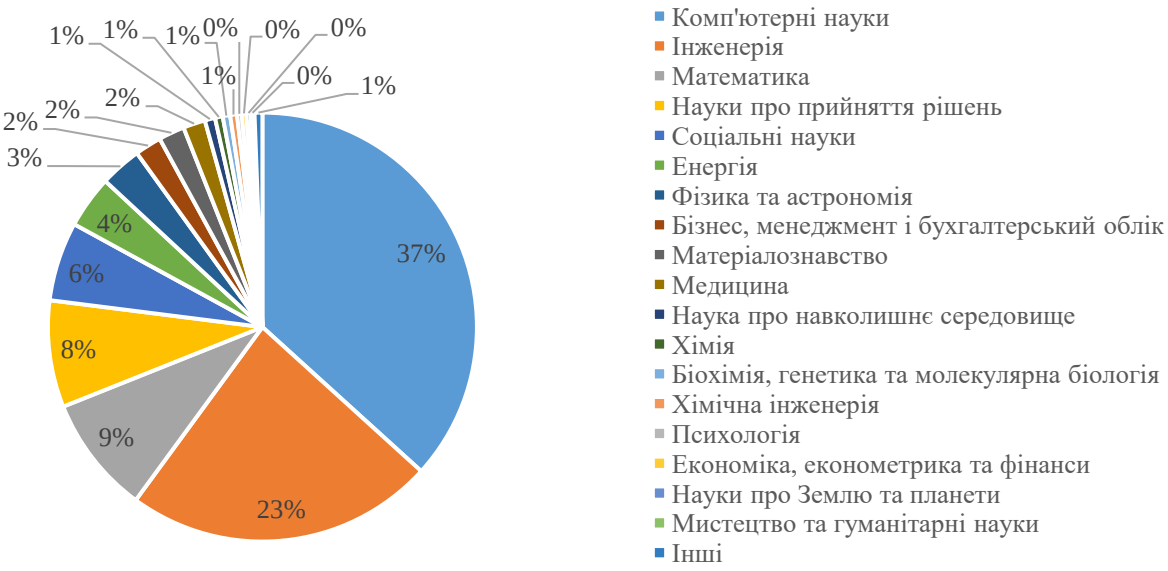
Джерело: сформовано автором за допомогою Biblioshiny та Scopus

Рис. 3. 20 найбільш релевантних (5 і більше публікацій) країн, з якими афілійовані автори публікацій, та їх метрики

Дані рисунку 3 демонструють кількість наукових публікацій, підготовлених авторами з різних країн, поділених на дві категорії: SCP (публікації в межах однієї країни) та MCP (публікації за участю авторів із кількох країн). Основними лідерами за кількістю публікацій є США, Індія та Китай, що підкреслює їхню важливу роль у глобальній науковій діяльності. США значно випереджають інші країни за загальною кількістю публікацій, причому більшість із них належать до категорії SCP. Це свідчить про потужний внутрішній науковий потенціал і велику кількість дослідницьких ресурсів у межах країни. Індія та Китай також демонструють сильні національні дослідницькі традиції.

Країни, як-от: Саудівська Аравія, Австралія, Канада та Китай, вирізняються значним відсотком MCP, що вказує на активну міжнародну співпрацю. Особливо це характерно для європейських країн, таких як Норвегія та Франція, де міжнародна співпраця відіграє також важливу роль у наукових дослідженнях. Це підкреслює важливість колективної роботи у вирішенні складних глобальних питань. Країни з меншим загальним обсягом публікацій, як-от Туреччина та Греція, мають значно нижчий рівень наукової активності, порівняно з лідерами. Проте навіть у цих країнах помітна частка MCP свідчить про зусилля в інтеграції до міжнародної наукової спільноти. Отримані дані відображають як регіональні, так і глобальні тенденції в наукових дослідженнях. Лідери, такі як США, активно розвивають внутрішню науку, тоді як країни із вищим відсотком MCP формують міцні міжнародні наукові зв'язки, що сприяє вирішенню глобальних проблем.

На рисунку 4 зображена структура публікаційної активності з кібербезпеки, поділена за галузями наукових знань. Згідно з наведеними даними найбільшу кількість робіт, що стосуються досліджуваної тематики, опубліковано в галузі комп'ютерних наук, яка становить 37 % від загальної кількості, тобто 20 726 публікацій. Така значна частина публікацій в цій галузі свідчить про домінуючий інтерес до теми кібербезпеки серед комп'ютерних наук, що підкреслює безпосередній взаємозв'язок між розвитком інформаційних технологій та необхідністю забезпечення кіберзахисту. Понад 23 % публікацій зроблені у сфері інженерії, 9 % – у сфері математики та 8 % – у сфері наук про прийняття рішень.



Джерело: сформовано автором на основі вбудованого інструментарію Scopus

Рис. 4. Структура публікаційної активності за пошуковим запитом «cyber security», що були опубліковані в наукометричній базі Scopus у розрізі галузей наукових знань

Інші галузі також демонструють зацікавленість у вивченні проблем кібербезпеки, хоча їхня частка є значно меншою. Наприклад, нейронаука має 93 публікації, сільськогосподарські та біологічні науки – 79 публікацій, багатопрофільні наукові дослідження – 79 публікацій, медичні професії – 65 публікацій. Крім того, менша кількість публікацій репрезентована у таких сферах, як сестринська справа (10 публікацій), фармакологія, токсикологія та фармацевтика (4 публікації), імунологія та мікробіологія (2 публікації), стоматологія (1 публікація). Дані на рисунку 4 підтверджують, що кібербезпека активно досліджується в галузі комп'ютерних наук, проте її важливість все більше визнається і в інших сферах, таких як нейронаука, сільське господарство та медицина. Зростаюча кількість публікацій в інших наукових галузях свідчить про інтеграцію питань кібербезпеки в різноманітні сфери науки, що є важливим аспектом для розвитку міждисциплінарних досліджень та практичних застосувань в цих областях.

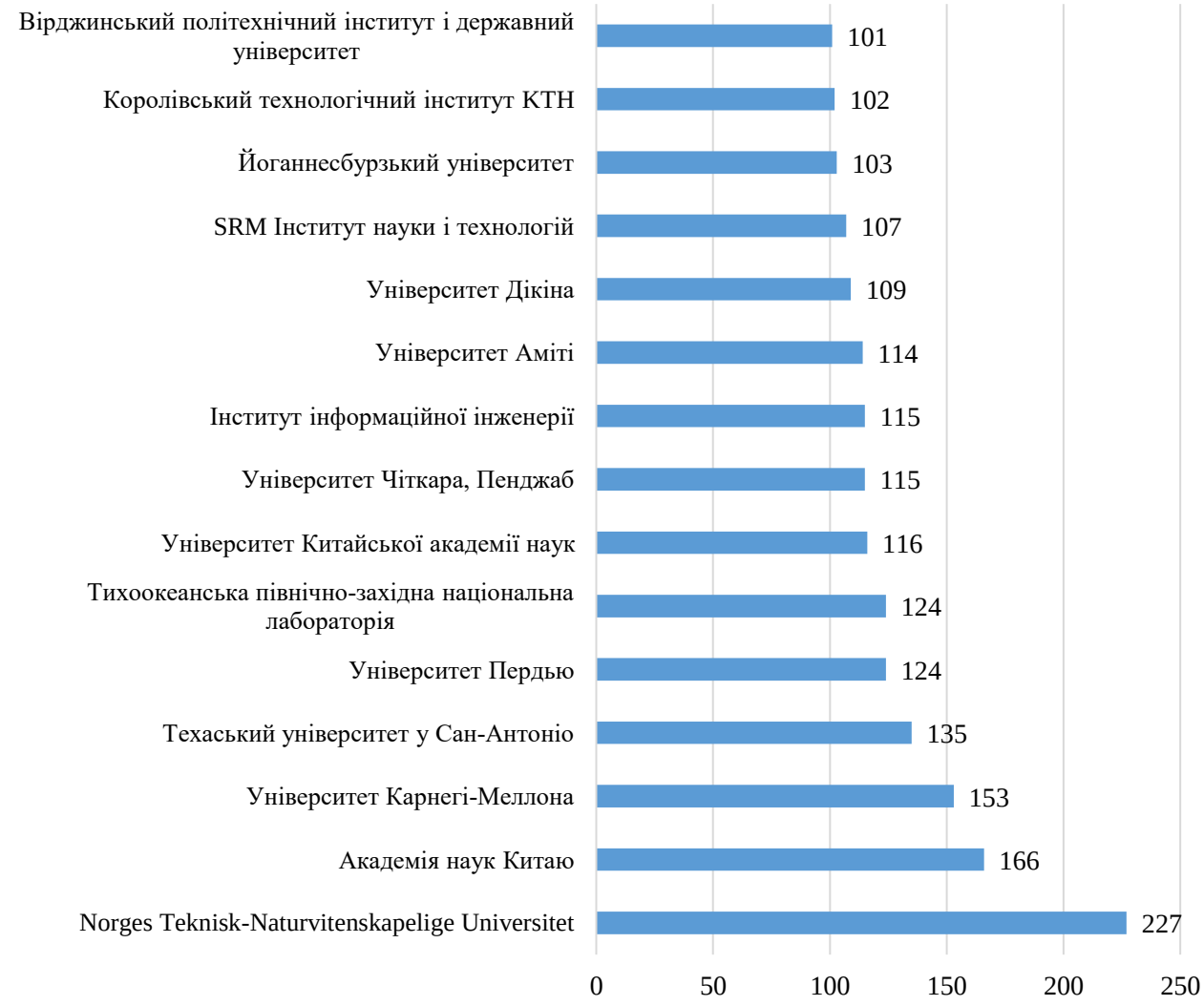
Джерело: сформовано автором на основі вбудованого інструментарію Scopus

Рис. 5. Джерела фінансування наукових досліджень за пошуковим запитом «cyber security», що були опубліковані в наукометричній базі даних Scopus

Найбільші внески у фінансування досліджень з кібербезпеки роблять урядові та міжнародні організації, зокрема Національний науковий фонд США та Європейська комісія, що свідчить про глобальну важливість і пріоритетність цієї проблематики для науки та безпеки на міжнародному рівні. Згідно з даними рисунка 5 можна стверджувати, що основними джерелами фінансування наукових публікацій з досліджуваної проблематики є:

- Національний науковий фонд – 1078 статей;
- Європейська комісія – 807 статей;
- Рамкова програма «Горизонт 2020» – 614 статей;
- Національний фонд природничих наук Китаю – 590 статей;
- Міністерство енергетики США – 312 статей;
- Міністерство оборони США – 241 стаття;
- Міністерство науки і технологій КНР – 229 статей;
- Європейський фонд регіонального розвитку – 207 статей;
- Дослідницька рада інженерно-фізичних наук – 206 статей;
- Національна ключова програма досліджень і розвитку Китаю – 206 статей.

Аналіз найбільших наукових установ, що активно досліджують проблеми кібербезпеки, вказує на значну роль таких університетів, як *Norges Teknisk-Naturvitenskapelige Universitet*, Академія наук Китаю та Університет Карнегі-Меллона, які займають провідні позиції щодо кількості публікацій з питань кібербезпеки (рис. 6).



Джерело: сформовано автором на основі вбудованого інструментарію Scopus

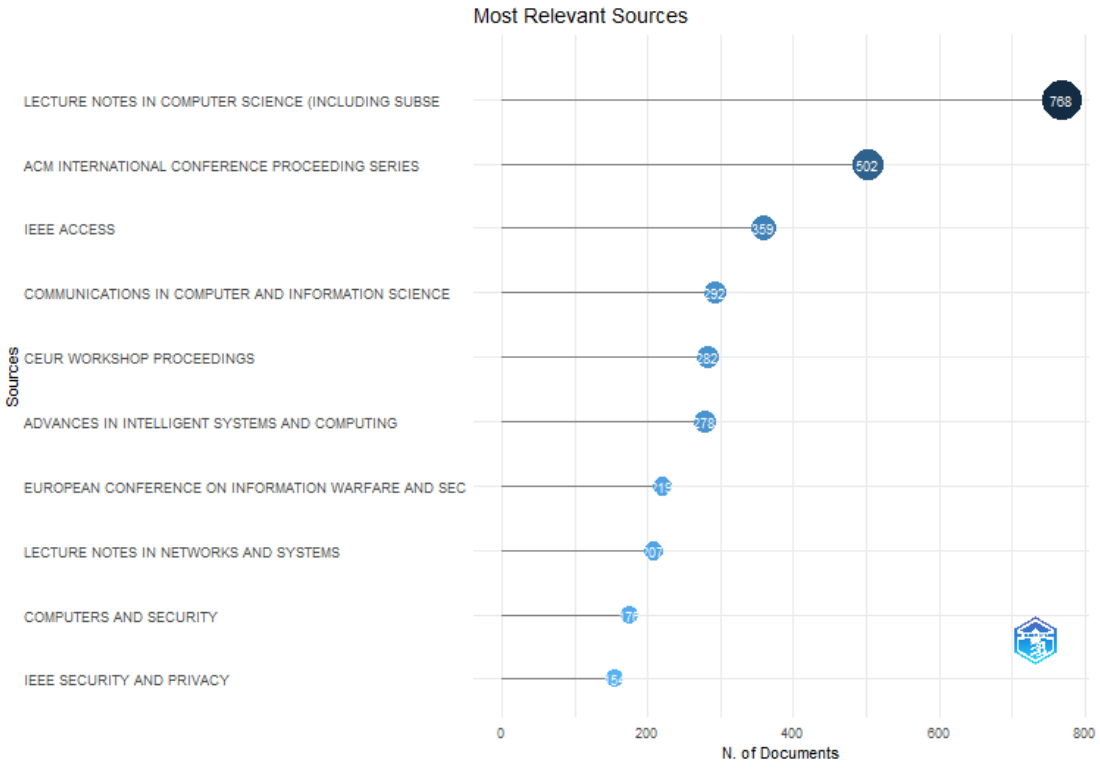
Рис. 6. Градація наукових публікацій за пошуковим запитом «cyber security», що були опубліковані в наукометричній базі Scopus за приналежністю до організацій

Згідно з даними рисунка 6 найбільшу кількість наукових робіт у галузі кібербезпеки було опубліковано вченими з таких установ:

- Norges Teknisk-Naturvitenskapelige Universitet – 227 статей;
- Академія наук Китаю – 166 статей;
- Університет Карнегі-Меллона – 153 статті;
- Техаський університет у Сан-Антоніо – 135 статей;
- Університет Пердью – 124 статті;
- Тихоокеанська північно-західна національна лабораторія – 124 статті;
- Університет Китайської академії наук – 116 статей;
- Університет Чіткара, Пенджаб – 115 статей;
- Інститут інформаційної інженерії – 115 статей;
- Університет Аміті – 114 статей;
- Університет Дікіна – 109 статей;
- SRM Інститут науки і технологій – 107 статей;
- Йоганнесбурзький університет – 103 статті;
- Королівський технологічний інститут KTH – 102 статті;
- Вірджинський політехнічний інститут і державний університет – 101 стаття.

Найбільш цитованою є публікація «Огляд методів інтелектуального аналізу даних і машинного навчання для виявлення вторгнень у кібербезпеку». У цьому оглядовому дослідженні автори провели систематичний аналіз літератури, присвячений методам машинного навчання (ML) та аналізу даних (DM), які застосовуються у кібераналітиці для підтримки виявлення вторгнень. У документі наведено короткі навчальні описи кожного методу ML/DM, а також визначено, прочитано та підсумовано ключові роботи, що стосуються цих методів, на основі кількості цитувань або релевантності нових підходів. Особливу увагу науковці приділили даним, що є важливими для застосування ML/DM, зокрема описано відомі набори кіберданих, які використовуються в цих методах. Також автори розглянули складність алгоритмів ML/DM, з'ясували основні проблеми, пов'язані з їх використанням у кібербезпеці, та надали рекомендації щодо вибору конкретного методу залежно від завдання [12].

У сфері наукових досліджень найбільш релевантним джерелом є видання *«Lecture Notes in Computer Science (including subseries)»*, що налічує 788 документів. Це свідчить про те, що цей журнал є одним із ключових платформ для публікації робіт, присвячених кібербезпеці, комп'ютерним наукам та суміжним темам. Висока кількість публікацій демонструє важливість цього джерела для академічної спільноти та його вплив на розвиток сучасних технологій (рис. 7).



Джерело: сформовано автором за допомогою Biblioshiny та Scopus

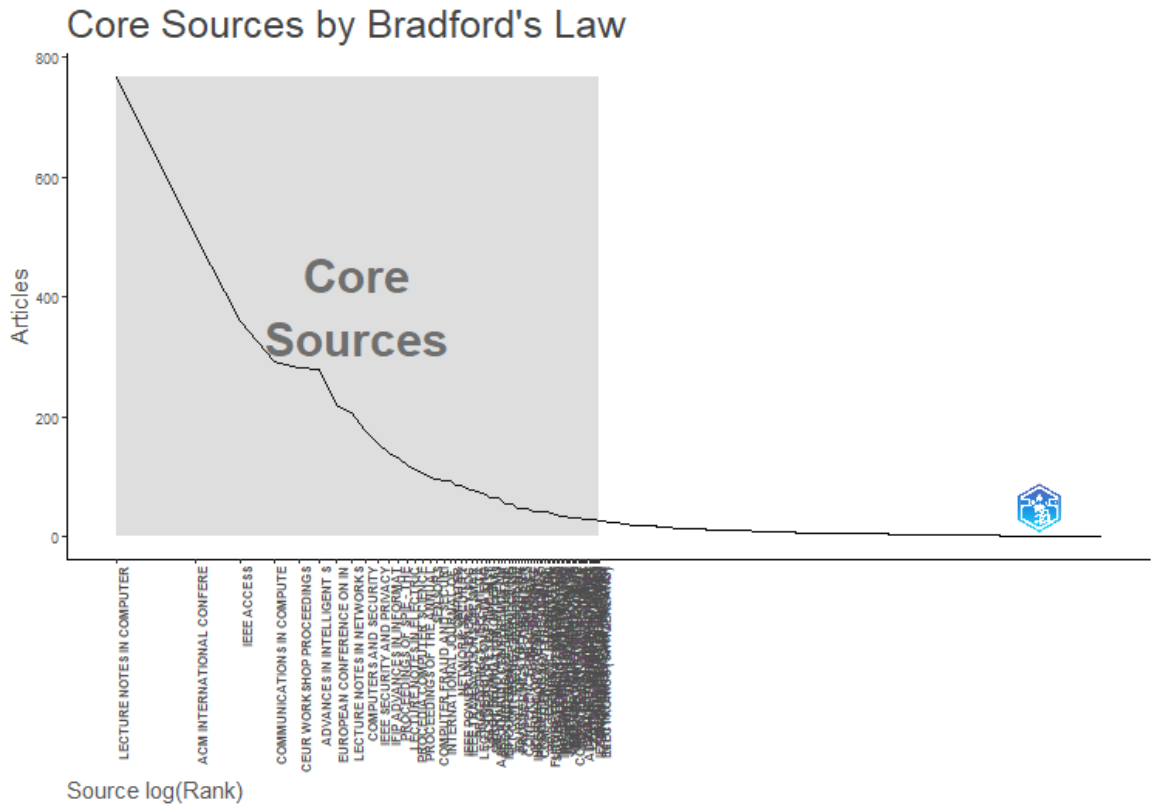
Рис. 7. Загальна кількість цитувань журналів у сфері кібербезпеки

На другому місці за кількістю документів знаходиться *«ACM International Conference Proceedings Series»* (502 документи). Це видання відіграє важливу роль у сприянні міжнародній співпраці, обміну ідеями та результатами досліджень між науковцями різних країн. Такий рівень публікацій підкреслює значення глобального підходу до вирішення проблем, пов'язаних із кібербезпекою. Серед інших джерел, що мають значний внесок, варто виокремити *«IEEE Access»* (359 документів) та *«Communications in Computer and Information Science»* (292 документи). Ці журнали охоплюють широкий спектр тем, враховуючи обробку інформації, інтелектуальні системи та новітні розробки у галузі обчислювальних технологій. Їхня популярність підтверджує важливість інновацій у боротьбі з кіберзагрозами та впровадженні захисних технологій.

Видання *«Advances in Intelligent Systems and Computing»* (278 документів) та *«Future Generation Computer Systems»* (219 документів) акцентують увагу на спеціалізованих напрямах, таких як інтелектуальні обчислювальні системи та безпека майбутніх поколінь комп'ютерних мереж. Це демонструє необхідність дослідження не лише сучасних викликів, але й прогнозування майбутніх загроз у цифровому середовищі. Таким чином, бібліометричний аналіз показує, що основні наукові джерела охоплюють широкий спектр досліджень у сфері кібербезпеки. Лідируючі видання зосереджені як на базових, так і на спеціалізованих аспектах, підкреслюючи важливість міждисциплінарного підходу до вирішення проблем цифрової безпеки. Це підтверджує необхідність продовження наукових досліджень для забезпечення ефективного захисту в умовах стрімкої цифровізації.

Закон Бредфорда використовується для ідентифікації «ядрових» джерел, що публікують найбільшу кількість матеріалів на певну тематику. Рисунок 8 ілюструє застосування закону Бредфорда до джерел, що спеціалізуються на тематиці кібербезпеки. У затемненій зоні (*Core Sources*) показані «ядрові» джерела, які публікують найбільшу кількість статей із цієї тематики. Ці джерела мають найбільший вплив на наукову дискусію в галузі кібербезпеки. Вони формують ядро наукової інформації, забезпечуючи значний внесок у розвиток досліджень. До ядра входять видання, такі як «*Lecture Notes in Computer Science*» та «*IEEE Access*», що публікують найбільше статей.

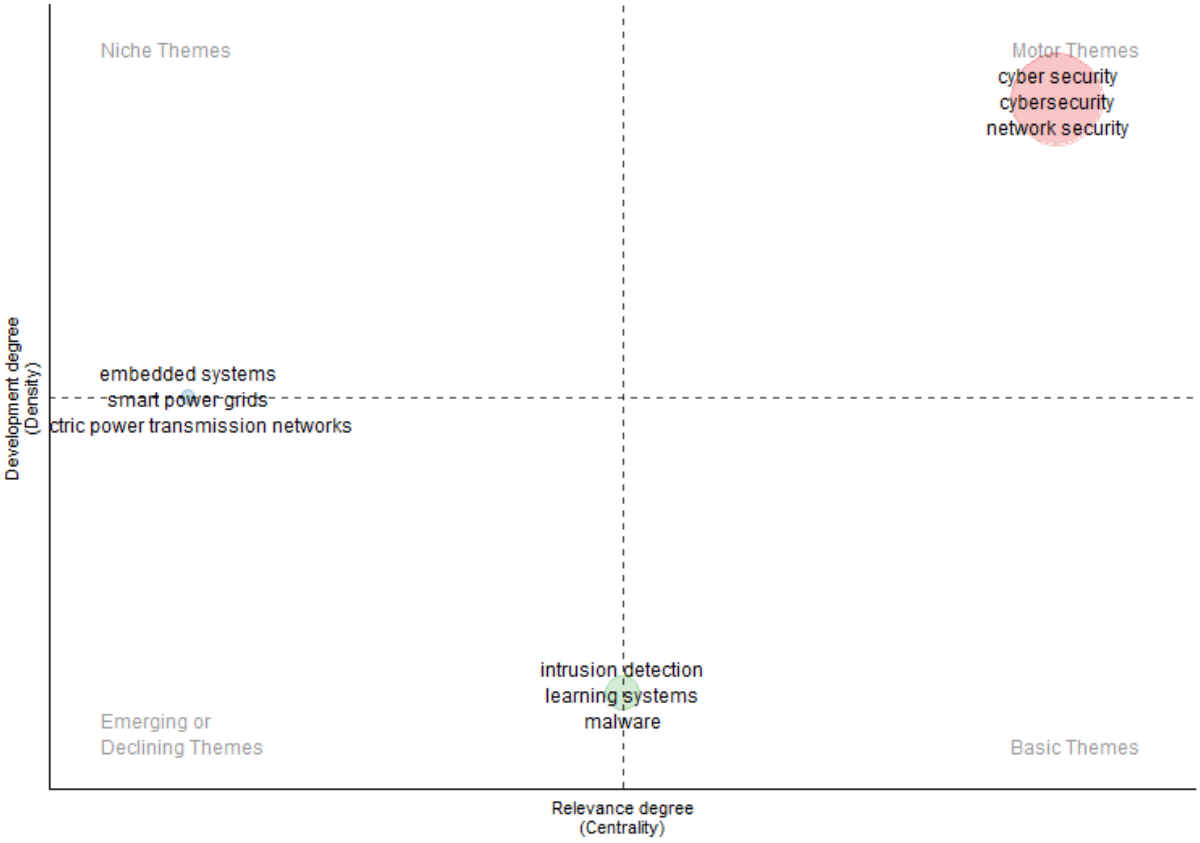
Закон Бредфорда також демонструє структуру «*довгий хвіст» («long tail»)* для джерел, які публікують значно меншу кількість статей із цієї тематики. Хоча ці джерела можуть не мати такого значного впливу, вони розширюють спектр досліджень і розширюють коло наукового обговорення. Це свідчить про те, що поряд із впливовими джерелами існує значна кількість менш активних видань, які, хоча й публікують лише кілька статей, але також є важливими учасниками наукового поля.



Джерело: сформовано автором за допомогою Biblioshiny та Scopus

Рис. 8. Закон Бредфорда для журналів з вибірки у сфері кібербезпеки

Тематична карта ключових слів авторів на рисунку 9 ілюструє, як різні теми, пов'язані з кібербезпекою, розподіляються за двома основними критеріями: ступенем розвитку (щільність) і ступенем важливості (центральність). Ці параметри дозволяють класифікувати теми, залежно від їхньої зрілості та значення для наукової спільноти. Моторні теми (Motor Themes) характеризуються високими показниками як щільності, так і центральності, що свідчить про їх важливість та активний розвиток. У цьому випадку ключовими моторними темами є «*cyber security», «cybersecurity» та «network security»*, які відіграють провідну роль у дослідженнях кібербезпеки.

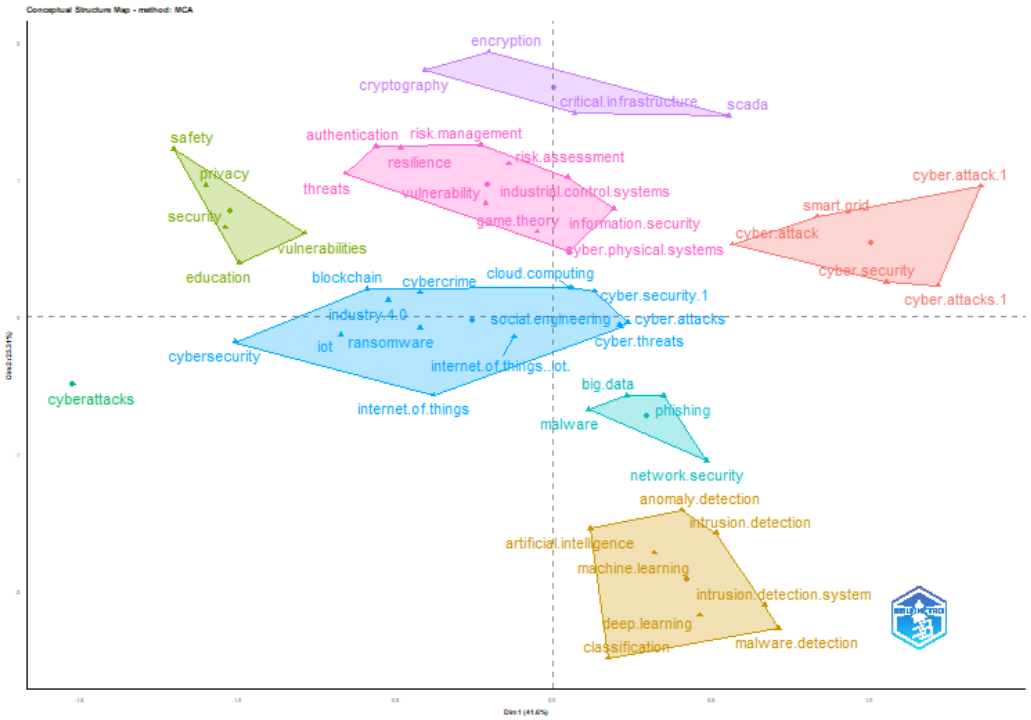


Джерело: сформовано автором за допомогою Biblioshiny та Scopus

Рис. 9. Тематична мапа авторських ключових слів у сфері кібербезпеки

Базові теми (*Basic Themes*) відрізняються високою центральністю, проте їх розвиток менш інтенсивний. До таких тем належать «*intrusion detection», «learning systems» і «malware»*, що є основою досліджень, але вимагають подальшого розвитку. Нішеві теми (*Niche Themes*) мають високий рівень розробленості, проте їхня релевантність для ширшого наукового контексту обмежена. У цьому випадку такі теми, як «*embedded systems», «smart power grids» та «electric power transmission networks»*, розглядаються як спеціалізовані та вузьконаправлені. Тематики, що виникають або занепадають (*Emerging or Declining Themes)*, характеризуються низькими показниками і центральності, і щільності. Вони перебувають на ранній стадії розвитку або поступово втрачають актуальність.

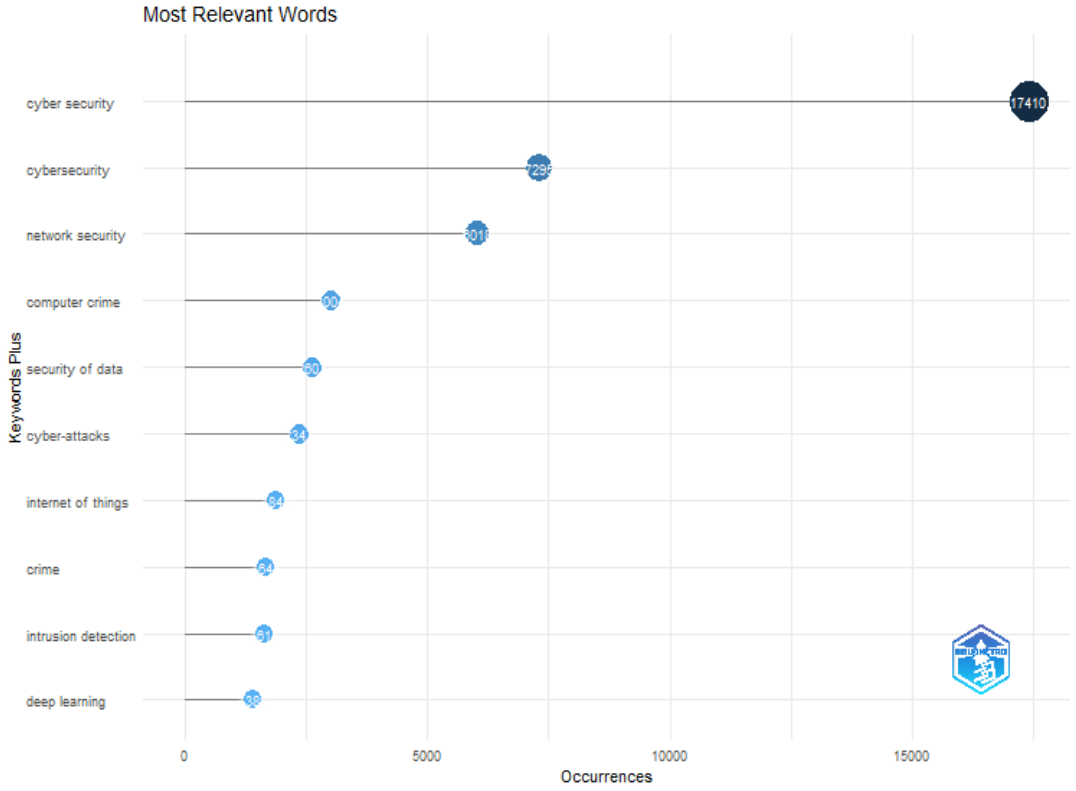
Карта тем відображає баланс між інтенсивно розвиненими та фундаментальними напрямами досліджень у сфері кібербезпеки, а також вказує на спеціалізовані області та нові напрями, що потребують уваги (рис. 10).



Джерело: сформовано автором за допомогою Biblioshiny та Scopus

Рис. 10. Факторіальний аналіз авторських ключових слів у сфері кібербезпеки

Факторний аналіз авторських ключових слів у галузі кібербезпеки дозволяє визначити основні слова та взаємозв'язки між ними (рис. 11). Результати аналізу свідчать, що певні ключові слова формують окремі факторні кластери, які відображають основні теми досліджень. Деякі концепти зустрічаються в різних кластерах або перетинаються, що вказує на міждисциплінарний характер досліджень у цій сфері.

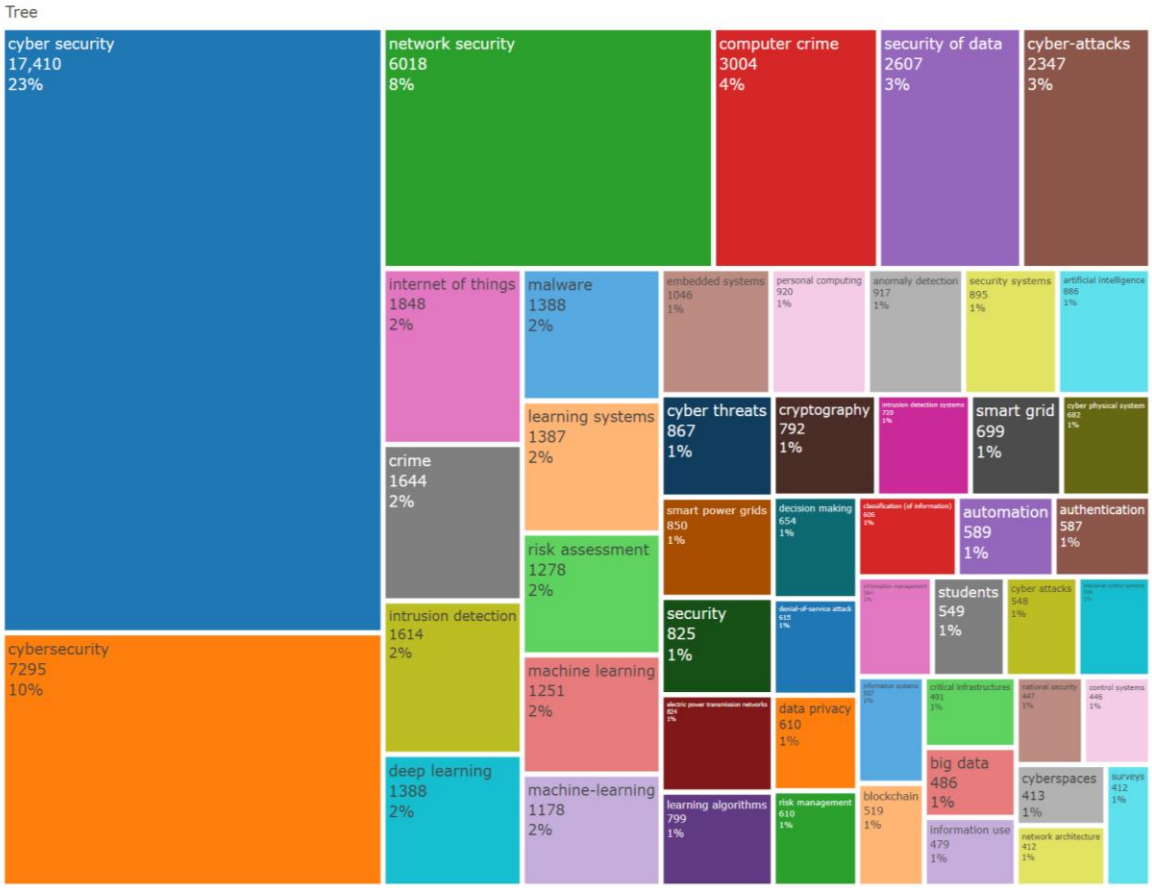


Джерело: сформовано автором за допомогою Biblioshiny та Scopus

Рис. 11. 10 найбільш поширених ключових слів авторів у сфері кібербезпеки

Дані рисунка 11 свідчать, що аналіз ключових слів, які використовуються в наукових роботах, дозволяє краще зрозуміти роль кібербезпеки. 10 найбільш поширених ключових слів демонструють те, що основними напрямами дослідження є захист критичної інфраструктури (транспорт, енергетика, фінанси), охорона персональних даних та інтелектуальної власності. Від рівня розвитку цифрових технологій залежить здатність соціально-економічних об'єктів, таких як підприємства, банки, компанії, фінансові установи, ефективно протистояти кіберзагрозам та забезпечувати стабільність кіберпростору.

Для більш детального аналізу розглянемо дерево ключових слів (рис. 12).



Джерело: сформовано автором за допомогою Biblioshiny та Scopus

Рис. 12. Дерево ключових слів авторів у сфері кібербезпеки

Рисунок 12 відображає структуру досліджень у сфері кібербезпеки, демонструючи основні тенденції та напрями, що цікавлять науковців. Найбільш поширеним ключовим словом є «*cyber security*» (23 %), що підкреслює фундаментальну важливість цієї теми для захисту цифрового середовища. Крім того, «*cybersecurity*» (10 %) також займає значну частку досліджень, що вказує на популярність цієї сфери незалежно від варіантів написання терміна. Серед провідних напрямів досліджень виокремлюються «*network security*» (8 %), «*computer crime*» (4 %), «*security of data*» (3 %) і «*cyber-attacks*» (3 %), що фокусуються на захисті мереж, запобіганні кіберзлочинності та забезпеченні конфіденційності даних. Ці аспекти є ключовими для створення надійних механізмів протидії кіберзагрозам, особливо в умовах зростання масштабів цифровізації суспільства.

Окрему увагу приділено сучасним технологіям, таким як «*internet of things*» (2 %), «*machine learning*» (2 %) та «*deep learning*» (2 %), які є важливими інструментами для виявлення та прогнозування кіберзагроз. Також теми «*malware*» (2 %), «*intrusion detection*» (2 %) та «*cyber threats*» (1 %) висвітлюють конкретні форми загроз і методи їх аналізу, що підсилює акцент на практичних аспектах кібербезпеки. Крім того, дослідження охоплюють галузеві аспекти, наприклад, «*smart grid*» (1 %), «*data privacy*» (1 %) і «*blockchain*» (1 %), що демонструє міждисциплінарний підхід у вирішенні проблем безпеки. Зокрема, питання конфіденційності даних та захисту розумних енергосистем стають дедалі актуальнішими на тлі зростання цифрових інновацій.

Таким чином, бібліометричний аналіз підтверджує, що кібербезпека є багатогранною сферою, яка охоплює широкий спектр досліджень: від базових концептів до специфічних технологій, що свідчить про необхідність подальшого розвитку інтегрованих підходів до захисту цифрового простору, враховуючи

постійне зростання кількості та складності кіберзагроз. Бібліографічний аналіз досліджень у сфері кібербезпеки демонструє її високу актуальність і багатогранність, що відображає глобальний характер проблем, пов'язаних із захистом цифрового простору. Ключові наукові джерела охоплюють широкий спектр питань, зокрема захист мереж, конфіденційність даних, виявлення загроз, інтеграцію інтелектуальних систем і використання новітніх технологій, таких як штучний інтелект, машинне навчання та блокчейн.

Висновки. Встановлено, що найбільшу кількість досліджень зосереджено на базових концептах кібербезпеки, таких як: захист критичної інфраструктури, запобігання кібератакам та боротьба з кіберзлочинністю. При цьому помітний міждисциплінарний підхід, що містить аспекти інформаційної безпеки, інтелектуальних систем і соціально-економічного контексту. Високий рівень публікацій у міжнародних журналах свідчить про активну глобальну співпрацю, спрямовану на створення ефективних рішень для боротьби з кіберзагрозами. Водночас аналіз демонструє зростання інтересу до інноваційних підходів, таких як використання штучного інтелекту та автоматизованих систем для моніторингу й аналізу загроз. Розвиток цих напрямів сприяє підвищенню стійкості кіберпростору, що є критично важливим на тлі швидкої цифровізації різних сфер життя. Отже, бібліографічний аналіз підтверджує необхідність продовження наукових досліджень у сфері кібербезпеки, враховуючи стрімке зростання складності та масштабів кіберзагроз.

Список використаної літератури:

1. *Атамась В.Р.* Щодо проблеми визначення поняття «кіберзлочини» та «кіберзлочинність» / *В.Р. Атамась, О.М. Сокуренко* // Актуальні проблеми формування громадянського суспільства та становлення правової держави : збірник матеріалів IV Всеукраїнської науково-практичної інтернет-конференції, 21 травня. – Черкаси, 2021. – С. 106–110.
2. *Бутузов В.М.* Протидія комп'ютерній злочинності в Україні / *В.М. Бутузов.* – Київ : КИТ, 2010. – 148 с.
3. *Буяджи С.А.* Правове регулювання боротьби з кіберзлочинністю : теоретико-правовий аспект : дис. ... канд. юрид. наук : спеціальність 12.00.01 / *С.А. Буяджи.* – Київ, 2018. – 203 с.
4. *Ковальчук А.Ю.* Кіберзлочини як загроза державній безпеці : кримінологічні та організаційні особливості обліку / *А.Ю. Ковальчук* // Інформація і право. – 2023. – № 4. – С. 187–196 [Електронний ресурс]. – Режим доступу : http://nbuv.gov.ua/UJRN/Infpr_2023_4_20.
5. *Коцман І.* Державне регулювання протидії кіберзлочинності в Україні : поняття та основні напрямки / *І.Коцман* // Публічне управління та адміністрування в Україні. – 2024. – № 40. – С. 245–252.
6. *Лисько Т.Д.* Протидія кіберзлочинності : сучасний стан вітчизняного законодавства та досвід зарубіжних країн / *Т.Д. Лисько* // Актуальні проблеми держави і права. – 2022. – № 96. – С. 44–49 [Електронний ресурс]. – Режим доступу : http://nbuv.gov.ua/UJRN/apdp_2022_96_6.
7. *Пивоваров В.В.* Кіберзлочинність : кримінологічний погляд на генезис явища та шляхи запобігання / *В.В. Пивоваров, С.Ю. Лисенко* // Право і суспільство. – 2016. – № 3 (2). – С. 177–182 [Електронний ресурс]. – Режим доступу : http://nbuv.gov.ua/UJRN/Pis_2016_3%282%29__32.
8. *Харитоненко І.О.* Причини та умови вчинення кіберзлочинів / *І.О. Харитоненко* // Економіка. Фінанси. Право. – 2023. – № 7. – С. 67–72.
9. *Aria M.* Bibliometrix : An R-tool for comprehensive science mapping analysis / *M.Aria, C.Cuccurullo* // Journal of Informetrics. – 2017. – Vol. 11 (4). – P. 959–975.
10. *Bequai A.* High-tech security and the failings of president clinton's commission on critical infrastructure protection / *A.Bequai* // Computers & Security. – 1998. – Vol. 17, No. 1. – P. 19–21. DOI: 10.1016/s0167-4048(97)80244-1.
11. *Boiko A.* Information systems for supply chain management : uncertainties, risks and cyber security / *A.Boiko, V.Shendryk, O.Boiko* // Procedia Computer Science. – 2019. – Vol. 149. – P. 65–70. DOI: 10.1016/j.procs.2019.01.108.
12. *Buczak A.L.* A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection / *A.L. Buczak, E.Guven* // IEEE Communications Surveys & Tutorials. – 2016. – Vol. 18, No. 2. – P. 1153–1176. DOI: 10.1109/comst.2015.2494502.

References:

1. Atamas, V.R. and Sokurenko, O.M. (2021), «Shchodo problemy vyznachennia poniattia «kiberzlochyny» ta «kiberzlochynnist»», *Aktualni problemy formuvannia hromadianskoho suspilstva ta stanovlennia pravovoi derzhavy*, zbirnyk materialiv IV Vseukrainskoi naukovo-praktychnoi internet-konferentsii, 21 travnia, Cherkasy, pp. 106–110.
2. Butuzov, V.M. (2010), *Protydiia kompiuternii zlochynnosti v Ukraini*, KYT, Kyiv, 148 p.
3. Buiadzhy, S.A. (2018), «Pravove rehuliuvannia borotby z kiberzlochynnistiu: teoretyko-pravovyi aspekt», Ph.D. Thesis of dissertation, 12.00.01, Kyiv, 203 p.
4. Kovalchuk, A.Yu. (2023), «Kiberzlochyny yak zahroza derzhavnii bezpetsi: kryminolohichni ta orhanizatsiini osoblyvosti obliku», *Informatsiia i pravo*, No. 4, pp. 187–196, [Online], available at: http://nbuv.gov.ua/UJRN/Infpr_2023_4_20

5. Kotsman, I. (2024), «Derzhavne rehuliuvannia protydii kiberzlochynnosti v Ukraini: poniattia ta osnovni napriamky», *Publichne upravlinnia ta administruvannia v Ukraini*, No. 40, pp.245–252.
6. Lysko, T.D. (2022), «Protydiia kiberzlochynnosti: suchasnyi stan vitchyznianoho zakonodavstva ta dosvid zarubizhnykh krain», *Aktualni problemy derzhavy i prava*, No. 96, pp. 44–49, [Online], available at: http://nbuv.gov.ua/UJRN/apdp_2022_96_6
7. Pyvovarov, V.V. and Lysenko, S.Yu. (2016), «Kiberzlochynnist: kryminolohichnyi pohliad na henezys yavyshcha ta shliakhy zapobihannia», *Pravo i suspilstvo*, No. 3 (2), pp. 177–182, [Online], available at: http://nbuv.gov.ua/UJRN/Pis_2016_3%282%29__32
8. Kharytonenko, I.O. (2023), «Prychyny ta umovy vchynennia kiberzlochyniv», *Ekonomika. Finansy. Pravo*, No. 7, pp. 67–72.
9. Aria, M. and Cuccurullo, C. (2017), «Bibliometrix: An R-tool for comprehensive science mapping analysis», *Journal of Informetrics*, Vol. 11 (4), pp. 959–975.
10. Bequai, A. (1998), «High-tech security and the failings of president clinton's commission on critical infrastructure protection», *Computers & Security*, Vol. 17, No. 1, pp. 19–21, doi: 10.1016/s0167-4048(97)80244-1.
11. Boiko, A., Shendryk, V. and Boiko, O. (2019), «Information systems for supply chain management: uncertainties, risks and cyber security», *Procedia Computer Science*, Vol. 149, pp. 65–70, doi: 10.1016/j.procs.2019.01.108.
12. Buczak, A.L. and Guven, E. (2016), «A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection», *IEEE Communications Surveys & Tutorials*, Vol. 18, No. 2, pp. 1153–1176, doi: 10.1109/comst.2015.2494502.

Sokha S., Savchuk S., Zdybel R.

The current state of scientific research on the problems of state policy to combat cybercrime

Abstract. The authors of this article comprehensively study the current state of scientific research on the problems of state policy to combat cybercrime, because bibliometric analysis as one of the methods of scientific research allows us to give a general assessment of the researchability of the problem and is the key to its further study.

The presented article analyzed scientific publications in the Scopus database using the keywords "cyber security", which means cybersecurity. In particular, using the digital tools Scopus and Biblioshiny, the following were determined: the dynamics of the number of articles in the Scopus database for the search query "cyber security" for 1998–2024 in time and geographical dimensions; the top 20 most relevant (5 or more publications) countries with which the authors of the publications are affiliated, and their metrics; the structure of publication activity; sources of funding for scientific research; gradation of scientific publications by affiliation to organizations; total number of citations of journals in the field of cybersecurity; application of Bradford's law to sources specializing in cybersecurity; thematic map of author keywords in the field of cybersecurity; factorial analysis of author keywords in the field of cybersecurity; top 10 keywords of authors and a tree of keywords of authors in the field of cybersecurity.

According to the analysis, the following conclusions were made: protection of critical infrastructure, combating cybercrime and preventing cyberattacks are fundamental categories of cybersecurity, since the largest number of publications is devoted to them; cyber threats are global challenges of our time, and therefore there is a high level of publications in international journals; The analysis of scientific literature demonstrates the importance of further research in the field of cybersecurity in order to improve public policy aimed at strengthening the protection of cyberspace and ensuring the sustainability of the economy in the face of modern challenges.

Keywords: «cyber security»; cybersecurity; Scopus; Biblioshiny; digital tools; database; cybercrime; public policy.

Стаття надійшла до редакції 01.11.2024.