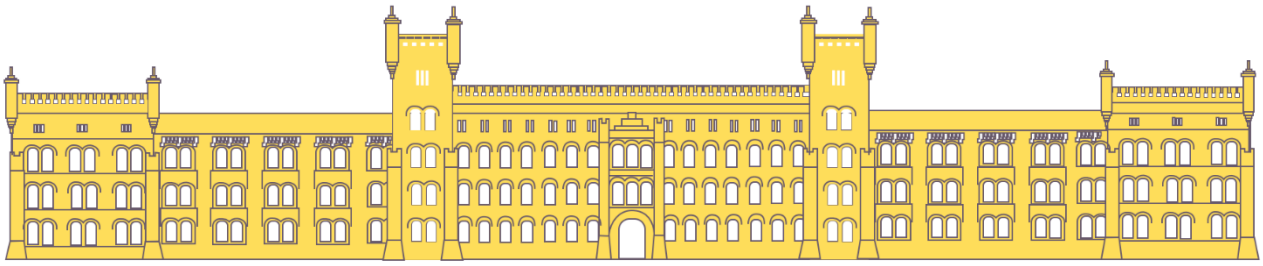
ДЕРЖАВНА СЛУЖБА УКРАЇНИ З НАДЗВИЧАЙНИХ СИТУАЦІЙ
ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ



ЦИВІЛЬНИЙ ЗАХИСТ В УМОВАХ ВІЙНИ

Збірник тез доповідей
ІІ Міжнародної науково-практичної конференції

15 квітня 2026 року

CIVIL PROTECTION IN TIMES OF WAR

The proceedings of the Second International Scientific and Practical Conference

15 April 2026

Ефективне здійснення публічної влади в умовах сучасних екзистенційних загроз нерозривно пов’язане із забезпеченням стійкості об’єктів критичної інфраструктури. Безпека таких об’єктів є не просто технічним завданням, а фундаментальною передумовою національного виживання та невід’ємною частиною забезпечення позитивних зобов’язань держави у сфері прав людини.

В умовах воєнної агресії публічна влада трансформує свою архітектуру, переходячи до централізованого стратегічного планування, де захист інфраструктури стає базисом для реалізації права на життя, безпеку та доступ до життєво необхідних ресурсів [3].

ЛІТЕРАТУРА

1. Долинська М. Запровадження електронної системи нотаріату в Україні. URL: https://repositsc.nuczu.edu.ua/bitstream/123456789/26712/1/Львів%203БІРНИК.pdf#page=330.
2. Ільєва Н. В. Створення електронного нотаріату в Україні. Прав. засади орг. та здійснення публ. влади, 2025. 148 с. URL: https://univer.km.ua/sites/default/files/Наукова%20діяльність/Збірник%20Публічна%20влада%2016.05.2025_0.pdf#page=148.
3. Письменний О. О. Цифровізація нотаріату та державних реєстрів в Україні: незахищеність системи та необхідність перегляду адміністративно-правової політики. *New ukrainian law*. 2025. № 1. С. 223–230. URL: https://doi.org/10.51989/nul.2025.1.28
4. Стетсюк З. Як працює е-нотаріат і що відбувалося під час тестування: інтерв'ю з Зоряною Стетсюк. URL: https://thedigital.gov.ua/news/technologies/yak-pratsyue-e-notariat-i-shcho-vidbuvalosya-pid-chas-testuvannya-intervyu-zoryani-stetsyuk
5. Труфанова Є. І. Електронний нотаріат в Україні: сучасний стан та перспективи розвитку. *Збірник тез доповідей студентів, аспірантів та здобувачів – учасників 81-ї звітної конференції Одеського національного університету імені І. І. Мечникова, присвячений 160-й річниці університету. Секція економічних і правових наук* / ред.: О. В. Побережець та ін. Одеса, 2025. С. 125–127. URL: https://dspace.onu.edu.ua/handle/123456789/42908.
6. Fursa S. Y. Introduction of e-notarial services in Ukraine: current problems of notarial activities and the role of the science of notarial process (on the example of certification of contracts arising from land legal relations). *Uzhhorod national university herald. series: law*. 2025. Vol. 1, no. 91. P. 455–462. URL: https://doi.org/10.24144/2307-3322.2025.91.1.67
7. Notarialna palata povidomyla pro porushennya notarialnoyi tayemnytsi pid chas testuvannya elektronnoyi systemy. URL: https://ips.ligazakon.net/lawnews/doc/NZ254362-notarialna-palata-povidomyla-pro-porushennya-notarialnoyi-tayemnytsi-pid-chas-testuvannya-elektronnoyi-systemy

УДК 614.8.084

БІБЛІОМЕТРИЧНИЙ АНАЛІЗ ДОСЛІДЖЕНЬ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Андрій КАСТРАНЕЦЬ, Олена ШКУРКА
Львівський державний університет безпеки життєдіяльності

Безпека та безперебійне функціонування об'єктів критичної інфраструктури є базовою умовою стабільності будь-якої сучасної держави. Проте, незважаючи на стрімкий розвиток інформаційних технологій та систем предиктивного аналізу, методики захисту таких об'єктів часто залишаються обмеженими.

Традиційні підходи до цивільного захисту, які фокусуються на ізольованому підході до забезпеченні безпеки та реагуванні на наслідки надзвичайних подій, сьогодні виявляють свою

нездатність протистояти комплексним загрозам — від кліматичних змін до цілеспрямованих атак.

Сучасні дослідження демонструють небезпечний розрив: класичні алгоритми цивільного захисту та пожежної безпеки повільно інтегруються з новітніми інструментами комп'ютерного зору, машинного навчання та динамічного моделювання. Сьогодні руйнування енергетичного вузла або кібератака на систему SCADA більше не є локальною подією — це тригер, здатний викликати каскадний параліч секторів критичної інфраструктури. Саме тому переосмислення методів захисту критичної інфраструктури є не просто технічним завданням, а питанням національного виживання.

Метою даного дослідження є комплексний аналіз глобальних наукових трендів у сфері захисту критичної інфраструктури для ідентифікації ключових методологічних прогалин та визначення найбільш актуальних напрямів інноваційних розвідок в умовах гібридних загроз.

Дослідження базується на аналізі масиву з 5289 наукових публікацій за 2015-2026 роки, проіндексованих у базі Scopus. Інструментарієм для кластеризації та просторової візуалізації зв’язків між ключовими поняттями виступило програмне забезпечення VOSviewer [1]. Даний програмний продукт дав можливість відстежити зв’язки між ключовими поняттями на основі масиву даних із Scopus.

В результаті аналізу візуалізації отриманої у [1] можна виділити чітку кластеризацію наукових досліджень [2] (представлено різними кольорами). Таких кластерів сформовано 8 із 149 елементів, які між собою пов'язані. Загальна кількість зв’язків складає 2313 одиниць.

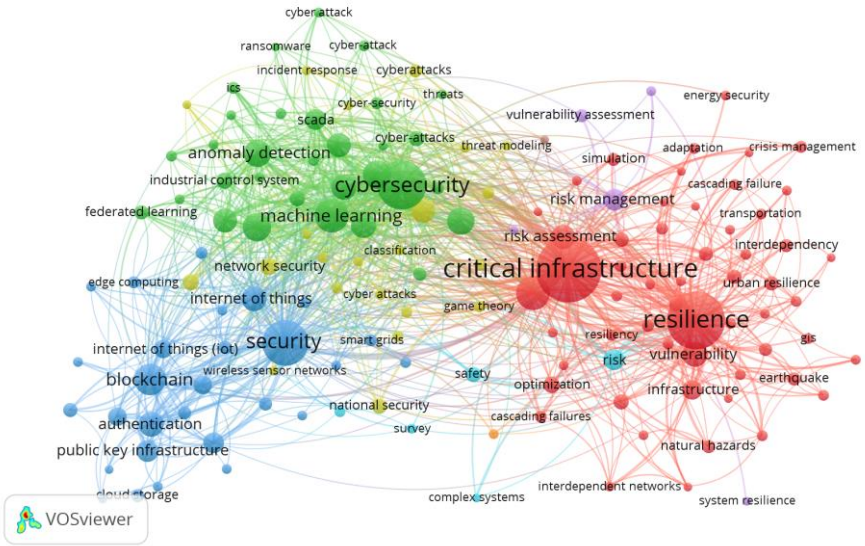


Рисунок 1 – Карта бібліометричного аналізу ключових слів за темою критична інфраструктура (на основі даних Scopus, VOSviewer).

Проте найбільшими кластерами за кількістю елементів (тобто ключових слів) є червоний (56 елементів) - що відображає весь масив досліджень критичної інфраструктури та її стійкості, зелений (31 елемент) - вказує на тематики публікацій пов'язаних із кібербезпекою, машинним навчанням, промисловими системами управління та синій (28 елементів) - охоплює наукові пошуки у сфері безпеки та захисту інформації, криптографії, приватності в мережі інтернет. Які формують основне ядро досліджень в даній тематиці.

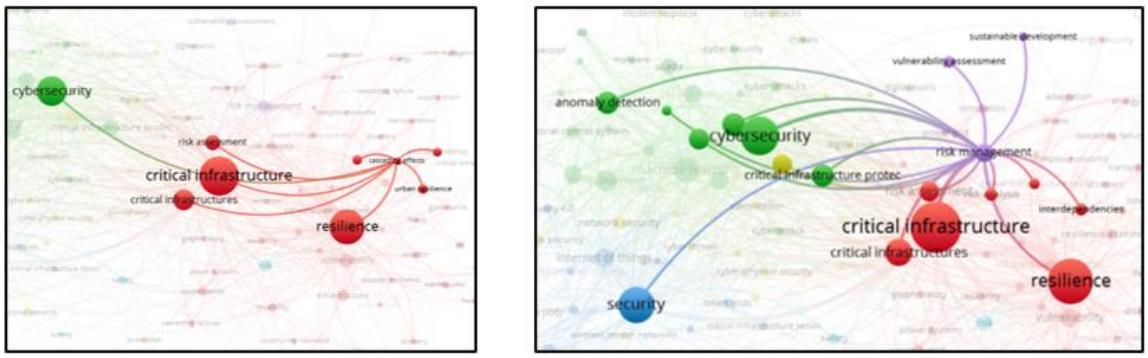


Рисунок 2 – Структура взаємозв’язків терміну risk management (управління ризиком) та cascading effects (каскадний ефект) (на основі даних Scopus, VOSviewer).

Важливо звернути увагу на те, що малодослідженим залишається питання каскадного ефекту і управління ризику в умовах сучасних фізичних небезпек і кіберзагроз. Як свідчить аналіз карти Рис.2, терміни, пов'язані з ефектом доміно та взаємозалежністю систем, розглядаються переважно в межах тематики критичної інфраструктури і жодним чином не включений в питання розвитку методів управління ризиками.

Основні підходи до управління ризиками все ще малоінтегровані із новітніми технологічними рішеннями, зокрема впровадження штучного інтелекту та інших програмних рішень, при оцінках вразливості критичної інфраструктури. На практиці це може вплинути на спроможність захисту від комплексних гібридних загроз. Оскільки прихований збій чи кібератака на цифрові протоколи або системи SCADA в комплексі із фізичним руйнуванням окремих елементів системи, може стати тригером масштабної, неконтрольованої відмови життєво важливих функцій критичної інфраструктури.

Відсутність щільних міжкластерних зв’язків доводить, що інтеграція предиктивних алгоритмів машинного навчання та сучасних систем криптографічного захисту в традиційні моделі розрахунку каскадних відмов є критичною прогалиною в дослідженнях. Подолання цього розриву шляхом впровадження сучасних технологій в оцінки ризиків формує найбільш актуальний та перспективний напрямок для подальших наукових досліджень у сфері цивільного захисту.

ЛІТЕРАТУРА

1. Van Eck N. J., Waltman L. Software survey: VOSviewer, a computer program for bibliometric mapping. Scientometrics. 2010. Vol. 84, No. 2. P. 523–538. DOI: 10.1007/s11192-009-0146-3.

2. *VOSviewer*.URL:https://app.vosviewer.com/?json=https%3A%2F%2Fdrive.google.com%2Fuc%3Fid%3D1CpoFO54T3dbXb8iHDHFz7TLk0RmNAFIa