УДК 342.9
DOI https://doi.org/10.32782/2524-0374/2023-12/70

СТАН НАУКОВОЇ РОЗРОБЛЕНОСТІ ПРОБЛЕМ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА СТІЙКОСТІ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

STATE OF SCIENTIFIC DEVELOPMENT OF ADMINISTRATIVE AND LEGAL PROBLEMS OF SECURITY AND SUSTAINABILITY OF CRITICAL INFORMATION INFRASTRUCTURE

Сокіран М.В., к.ю.н.,
докторант
Науково-дослідний інститут публічного права

У статті проаналізовано положення вітчизняної та зарубіжної літератури на предмет висвітлення питань адміністративно-правового забезпечення безпеки та стійкості критичної інформаційної інфраструктури. Констатовано, що питання адміністративно-правового забезпечення безпеки та стійкості критичної інформаційної інфраструктури стали предметом наукових досліджень в Україні на початку 2000 років, а активізація науково-дослідних робіт щодо означеного відбулося разом із появою низки нормативно-правових актів, які були прийняті на відповідь після захоплення Російською Федерацією Криму та території Донецької та Луганської областей в 2014 році. Визначено, що на відміну від України, в більшості розвинутих країн світу питанням захисту критично важливої інформаційної інфраструктури від збоїв будь-якого роду приділялась значна увага набагато раніше з визначенням її захисту важливим для підтримки внутрішньої стабільності та національної безпеки. Найбільш дискусійним питанням на сьогодні є відмежування термінів «критична інфраструктура» та «критична інформаційна інфраструктура». З'ясовано, що у зв'язку зі зростаючим занепокоєнням щодо потенційної вразливості мережевих угрупувань, а також зі збільшенням кількості збоїв у кібер-сфері багато країн вже зробили кроки для кращого розуміння вразливостей та загроз їх критичної інформаційної інфраструктури та запропонували заходи для захисту цих активів. Зроблено висновок, що попри достатню кількість досліджень у сфері захисту і стійкості критичної інфраструктури, питання адміністративно-правового забезпечення безпеки та стійкості критичної інформаційної інфраструктури досі залишаються практично не дослідженими.

Ключові слова: адміністративно-правове забезпечення, критична інформаційна інфраструктура, захист, безпека, стійкість, кібербезпека.

The article analyzes the provisions of domestic and foreign literature on the subject of coverage of issues of administrative and legal provision of security and stability of critical information infrastructure. It was established that the issues of administrative and legal provision of security and stability of critical information infrastructure became the subject of scientific research in Ukraine in the early 2000s, and the intensification of scientific and research work on this matter took place together with the appearance of a number of regulatory and legal acts that were adopted in response to the seizure by the Russian Federation of Crimea and the territories of Donetsk and Luhansk regions in 2014. It was determined that, unlike Ukraine, in most of the developed countries of the world, significant attention was paid much earlier to the protection of critical information infrastructure from failures of any kind, with the determination of its protection as important for maintaining internal stability and national security. The most controversial issue today is the demarcation of the terms "critical infrastructure" and "critical information infrastructure". It found that with growing concern about the potential vulnerability of network groups, as well as an increase in cyber disruptions, many countries have already taken steps to better understand the vulnerabilities and threats to their critical information infrastructure and have proposed measures to protect these assets. It was concluded that despite a sufficient number of studies in the field of protection and stability of critical infrastructure, the issues of administrative and legal provision of security and stability of critical information infrastructure still remain practically unexplored.

Key words: administrative and legal support, critical information infrastructure, protection, security, sustainability, cyber security.

Вступ. Питання адміністративно-правового забезпечення безпеки та стійкості критичної інформаційної інфраструктури стали предметом наукових досліджень в Україні порівняно нещодавно. Найбільшу кількість з означеного питання складають різні аналітичні доповіді, в першу чергу, що були підготовлені фахівцями Національного інституту стратегічних досліджень.

Так, у 2012 році Д. С. Бірюков й С. І. Кондратов підготували аналітичну доповідь «Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні». У ній автори: обґрунтували необхідність формування єдиної державної політики у сфері захисту критично важливих об'єктів та інфраструктури в Україні, представили огляд досвіду запровадження концепції критичної інфраструктури у провідних країнах світу, проаналізували нормативно-правові акти національного законодавства, що виокремлюють і встановлюють особливі умови захисту низки категорій об'єктів в Україні, які за міжнародними підходами належать до критичної інфраструктури [1].

Попри те, що зазначена робота була одною із перших аналітичних документів, в якій йшла мова про захист критичної інфраструктури як елемента національної безпеки, у ній не приділялась увага інформаційній складовій.

Однак треба віддати належне аналітикам, які ще у 2012 році визначили, що заходи щодо захисту критично важливих об'єктів, систем і ресурсів в Україні здійснюються низкою відомств у межах їх завдань і компетенції, що мають фрагментарний характер. Це створило паралельне існування систем захисту критично важливих об'єктів та інфраструктури, а це в свою чергу, загрожує бюрократизації проблеми та неефективного використання ресурсів на національному рівні [1].

У 2014 році вийшов друком консолідований документ під назвою «Зелена книга з питань захисту критичної інфраструктури в Україні». Цей документ був підготовлений на основі результатів дослідження, проведеного Національним інститутом стратегічних досліджень у 2011 році, зокрема роботи Міжвідомчої експертної робочої групи з протидії загрозам розповсюдження зброї та матеріалів масового знищення та пов'язаних з ними терористичних загроз [2]. У ній також були використані висновки та рекомендації круглого столу, організованого у липні 2012 року, і міжнародної конференції у листопаді 2013 року на тему «Концепція захисту критичної інфраструктури: стан, проблеми та перспективи впровадження в Україні». Розробка Зеленої книги здійснювалася за підтримки Офісу зв'язку НАТО в Україні в рамках виконання Плану дій Україна-НАТО на 2014 рік. Робота над документом включала активну участь вітчизняних та зарубіжних експертів, які брали участь у роботі Національного інституту стратегічних досліджень [2].

Необхідно відмітити, що дійсно з 2011–2014 роки Національним інститутом стратегічних досліджень було

проведено ряд засідань Міжвідомчої експертної робочої групи, за результатом яких було оприлюднено ряд підсумкових матеріалів. Наприклад, «Протидія тероризму, нерозповсюдження зброї та матеріалів масового знищення й захист критичної інфраструктури» (2013 р.) [3], «Концепція захисту критичної інфраструктури: стан, проблеми та перспективи її впровадження в Україні» (2014 р.) [4].

Метою роботи є дослідження та аналіз наукових джерел вітчизняних та зарубіжних авторів щодо забезпечення безпеки та стійкості критичної інформаційної інфраструктури та виокремлення питань, що недостатньо висвітлені.

Виклад основного матеріалу. Необхідно відмітити, що активізація науково-дослідних робіт щодо питань забезпечення безпеки та стійкості критичної інформаційної інфраструктури України відбулося разом із появою низки нормативно-правових актів, які були прийняті на відповідь після захоплення Російською Федерацією Криму та території Донецької та Луганської областей у 2014 році.

У 2014 році було проведено ряд досліджень представниками різних наукових профілів щодо безпеки і захисту критичної інфраструктури. Так, С. О. Гнатюк, М. О. Рябий, В. М. Лядовська, у статті «Визначення критичної інформаційної інфраструктури та її захисту: аналіз підходів», запропонували аналітичне дослідження нормативно-правової бази розвинених держав світу щодо варіацій ключових понять у галузі захисту критичної інформаційної інфраструктури. У результаті проведеного аналізу авторами було виявлено як спільні, так і відмінні особливості підходів до визначення критичної інфраструктури (та інших суміжних понять) низки держав, а також окреслено вітчизняні проблеми у цій галузі [5]. Такі вчені як С. Ф. Гончар, Г. П. Леоненко, О. Ю. Юдін досліджували питання щодо методології забезпечення інформаційної безпеки об'єктів критичної інфраструктури [6]. Крім зазначеного, С. Ф. Гончар також виокремив шляхи удосконалення державної політики щодо забезпечення інформаційної безпеки критичної інфраструктури України [7].

Доцільно відмітити, що на відміну від України, в більшості розвинутих країн світу питанням захисту критично важливої інформаційної інфраструктури від збоїв будь-якого роду приділялась увага набагато раніше з визначенням її захисту важливим для підтримки внутрішньої стабільності та національної безпеки.

Ще у 1984 році Стівен Леві опублікував свою працю під назвою «Хакери: герої комп'ютерної революції» [8], в якій автор крім того, що розповідав про подвиги перших хакерів комп'ютерної революції кінця 1950-х – початку 80-х, він підняв такі важливі теми як: хакерська етика, принцип хакерської діяльності – «Інформація має бути безкоштовною» та проблематика прав інтелектуальної власності на інформаційні продукти.

Але найбільша кількість публікацій і досліджень з питань захисту критичної інформаційної інфраструктури, уразливість від кібератак, винайдення оптимальних стратегій та інструментів для забезпечення стійкості як критичної інфраструктури загалом, так інформаційної – зокрема, почалися з кінця 20 століття. А обумовилося це побоюванням усього світового співтовариства переходом у 2000 рік та можливість в наслідок чого руйнування усіх систем, що використовують цифрові технології. Ця проблема широко відома як проблема Y2K. Адже, багато програм представляли чотиризначні роки лише з двома останніми цифрами, що робило 2000 рік невідрізненними від 1900. Нездатність комп'ютерних систем правильно розрізняти дати потенційно могла зруйнувати світову інфраструктуру комп'ютерних галузей [9]. І ці побоювання не були марними, хоча проблеми, що виникли по всьому світу 1 січня 2000 року були оцінені як незначні.

Наведемо лише декілька публікацій з цього питання: Проблема 2000 року: Четверта доповідь Комітету з питань урядової реформи та нагляду разом із додатковими поглядами (Комітет з урядової реформи та контролю США (1998 р.) [10], Корі Джонсон «Криза Y2K Crier» (1999 р.) [11], Тед Розе «Хто винайшов Y2K і чому він став таким універсальним?» (1999 р.) [12].

Після того як ажіотаж навколо цієї теми минув почали з'являтися більш ґрунтовні роботи з питань забезпечення і захисту критичної інформаційної інфраструктури в різних країнах. Так, наприклад, Т. Дж. Парсонс досліджував «Захист критично важливих інформаційних інфраструктур. Координація та розвиток міжсекторальних досліджень у Великобританії» [13], Д. Мотефф, К. Коупленд і Д. Фішер підготували звіт для Конгресу США «Критичні інфраструктури: що робить інфраструктуру критичною?» [14]. На думку авторів, пропозиція адміністрації Буша щодо створення Департаменту внутрішньої безпеки США включає функцію, до обов'язків якої входить координація політики та дій із захисту критичної інфраструктури країни. Однак у пропозиції не було визначено критеріїв визначення критичності або того, які інфраструктури слід вважати критичними. Після цього у низці документів, пов'язаних із захистом критичної інфраструктури, було запропоновано загальні визначення критичної інфраструктури та надано короткий перелік інфраструктур, які слід визначити як такі. Причому передбачалось, що жоден із цих списків чи визначень не вважатиметься остаточним. Тому критерії для визначення того, що може бути критичною інфраструктурою, і які інфраструктури таким чином кваліфікуються, з часом розширилися. Критичною інфраструктурою спочатку вважалися те, чиї тривалі збої можуть спричинити значні військові та економічні наслідки. До критичної інфраструктури тепер належать національні пам'ятки, наприклад монумент Вашингтона, так як атака може призвести до значних людських втрат або негативно вплинути на моральний стан нації [14].

Враховуючи, що як зазначили вище зазначені автори звіту, визначення поняття «критична інфраструктура» не є вичерпним, – наступним дискусійним питанням, яке необхідно висвітлити, є відмежування термінів «критична інфраструктура» та «критична інформаційна інфраструктура».

Так, деякі автори вважають, що їх розмежування є штучною проблемою або просто академічною модою. Інші вважають, що детальне обмірковування термінології не тільки призведе до вкрай необхідного вдосконалення понятійного апарату, але також існує низка переконливих показників того, що головні майбутні виклики полягають у виникненні нових критичних інформаційних інфраструктур, тому спільнота отримає значну користь від чіткого концептуального розмежування між цими поняттями, що дозволить краще зрозуміти проблеми, що пов'язані із їх захистом [15].

Але навіть попри те, що потреба в концептуальній точності очевидна, все одно дуже важко зрозуміти чим є (національна чи глобальна) інформаційна інфраструктура. Це пов'язано з тим, що технології мають не лише фізичну складову, яку досить легко осягнути – наприклад, високошвидкісні, інтерактивні, вузькосмугові та широкосмугові мережі; супутникові, наземні та бездротові системи зв'язку; і комп'ютери, телевізори, телефони, радіо та інші продукти, які люди використовують для доступу до інфраструктури, але вони також мають не менш важливий нематеріальний (іноді дуже невловимий) компонент, – інформацію та контент, що протікає через інфраструктуру, знання, створені з цього, і послуги, які надаються. Тому, на нашу думку, є необхідність у дослідженні ознак, що відрізняють критичну інфраструктуру і критичну інфраструктуру й тих, що їх поєднують.

Історично різні інфраструктури були фізично відокремлені. Однак із швидкими змінами з 1970-х років у галузі технологій, національних регуляторних практик, кон'юнктури ринку та виробничих перетворень критична

інфраструктура прогресивно конвергується. Технологічний прогрес також дозволив значно автоматизувати функціонування та управління критично важливими інфраструктурами. А з дослідженням ефекту «каскадних» наслідків, взагалі почали переглядатись існуючі державні політики щодо захисту критичних інформаційних інфраструктур.

Так, на думку Л. Гемпеля, Б. Крафа та Р. Пельцера критичність інфраструктури є результатом широкого спектра можливих взаємозв'язків між організаційними мережами, коли передача ресурсів через фізичні простори пов`язана з передачею інформації між організаціями та окремими людьми. Тому, навіть поодинокі збої можуть створити каскади, що вплинуть на інші сектори або всього суспільства [16]. Інші автори, проаналізувавши набір даних у 29 європейських країнах, встановили, що на енергетичний сектор припадає 60% усіх каскадів, 28% – на інформаційний сектор (телекомунікацій та Інтернету), 5% – на транспортний сектор, 3% – на водний [17]. Зазначений аналіз показує, що енергетичний та інформаційний сектори є найбільш вразливими, що може також призвести до каскадних збоїв.

Таким чином, у зв'язку зі зростаючим занепокоєнням щодо потенційної вразливості мережевих угрупувань, а також зі збільшенням кількості збоїв у кібер-сфері багато країн вже зробили кроки для кращого розуміння вразливостей та загроз їх критичної інформаційної інфраструктури та запропонували заходи для захисту цих активів.

Першою країною, яка звернула увагу на проблеми захисту критичної інформаційної інфраструктури, була США. Колишній президент США Білл Клінтон розпочав розробку національної стратегії захисту зі своєю Президентською комісією із захисту критичної інфраструктури у 1996 році, і з того часу це питання залишається пріоритетним. Це призвело до створення міжвідомчих комітетів, цільових груп та робочих груп, чиї зусилля призвели до політичних заяв та звітів, в яких викладено основні політичні елементи критичної інформаційної інфраструктри. Така політика мала наслідком створення цілої низки перспективних напрямів, таких як: теоретичні (визначення, що таке «критичні» елементи), організаційні (керівні принципи), законодавчі (наприклад, наказ Президента США № 13010 «Про роботу з дослідження вразливості захисту критичної інфраструктури від кібернетичних і фізичних загроз» (липень 1996 р.)) [5]. А терористична атака 11 вересня 2001 року, змусила політиків США переглянути визначення «інфраструктури» у контексті національної безпеки. Для цього звіти, закони та розпорядження було піддано нормативним уточненням та загалом розширенню кількості секторів інфраструктури та типів активів, які вважаються «критичними» в контексті національної безпеки.

Отже, критичні системи стають більш складними сьогодні ніж рівень взаємозв'язку, що коли-небудь збільшується. Це вимагає нових видів захисту. Пов'язані критичні системи великою мірою залежить від інформаційної інфраструктури. Своєю чергою, захист критичної інформаційної інфраструктури є частиною стратегії національної безпеки держави, адже наслідки нападу лише на одну її частину можуть бути катастрофічними для всіх систем. Тому в наукових колах активізуються дослідження щодо правового забезпечення безпеки та захисту критично важливої інформаційної інфраструктури. У сфері забезпечення безпеки та стійкості критичної інформаційної інфраструктури доцільно виділяти два тісно взаємопов'язаних, але різних за змістом напрями, а саме:

1) техніко-технологічний – формування та забезпечення безпечного функціонування системи відповідно до техніко-технологічних правил і вимог;

2) організаційно-правовий – здійснення правомірної діяльності працівників об'єктів, служби безпеки у взаємодії із співробітниками уповноважених державних органів, іншими юридичними та фізичними особами, щодо реалізації системи правових, організаційних та спеціальних заходів, спрямованих на охорону та захист критично важливої інформаційної інфраструктури та забезпечення дотримання інтересів держави і суспільства (зокрема, реалізація спеціальних заходів, які не зв'язані з інформаційними технологіями: визначення порядку доступу на територію об'єкта, фізична охорона об'єкта тощо) [18].

Ведучи мову про питання забезпечення безпеки і захисту критичної інфраструктури зазначимо, що їм було присвячена досить вагома кількість монографічних досліджень. Умовно їх можна поділити на дві групи – перша група – роботи юристів, а друга – технічного спрямування.

Так, до першої групи, як приклад, можна віднести наступні роботи: В. В. Крикун «Адміністративно-правовий механізм захисту об'єктів критичної інфраструктури» (2021 р.), С. А. Теленик «Адміністративно-правове регулювання державної системи захисту критичної інфраструктури України (2021 р.), І. І. Осипчук «Адміністративно-правові засади діяльності Служби безпеки України як суб'єкта забезпечення критичної інфраструктури» (2021 р.), В. В. Косинський «Адміністративно-правове забезпечення безпеки критичної інфраструктури в Україні (2021 р.). Зокрема І. І. Осипчук у своєму дисертаційному дослідженні обґрунтував позицію, що сама концепція критичної інфраструктури здебільшого передбачає роботу на випередження появі небезпекових складових, які можуть завдати шкоду об'єктам критичної інфраструктури та спрямована на підвищення швидкості реагування на такі загрози в умовах швидкої зміни ситуації шляхом фокусування уваги відповідних державних органів на запобіганні і профілактиці можливих ризиків [19].

Інший блок, як нами було визначено, складають роботи фахівців з технічних наук. Наприклад, Є. В. Брежнєв досліджував «Методологічні основи інформаційної технології забезпечення безпеки критичної інфраструктури в Україні (2017 р.), М. Ю. Комаров – «Метод та засоби захисту інформації від кібервпливів комп'ютерних системах та мережах об'єктів критичної інфраструктури (2021 р.).

Усі зазначені роботи також можна умовна поділити ще на дві підгрупи, перша підгрупа – це роботи, де акцент дослідження робився на захисті критичної інфраструктури (В. В. Крикун, М. Ю. Комаров, С. А. Теленик), друга – де акцент був на безпеці (І. І. Осипчук, В. В. Косинський, М. Б. Домарацький, Є. В. Брежнєв). Отже, стійкість критичної інфраструктури не була предметом дослідження.

Щодо дослідження адміністративно-правового забезпечення безпеки і стійкості критичної інформаційної інфраструктури, необхідно відмітити, що за даними Національного репозитарія академічних текстів, у жодному дисертаційному дослідженні напрямку «право», предмета дослідження «критична інформаційна інфраструктура» немає. На відмінну від технічних наук. Так, протягом останніх п'яти років було проведено ряд досліджень, а саме: В. М. Сидоренко «Методи ідентифікації та оцінювання стану кібербезпеки об'єктів критичної інформаційної інфраструктури авіаційної галузі (2018 р.), С. Ф. Гончар «Методологія оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інформаційної інфраструктури (2020 р.), Я. Ю. Дорогий «Методи підвищення ефективності процесів проектування критичної інформаційної інфраструктури (2021 р.).

Це пов'язано, в першу чергу, із тим, що на законодавчому рівні до 2017 року не було визначено, що таке «критична інформаційна інфраструктура». Тому юристи по теперішній час не обирають предметом своїх наукових пошуків забезпечення безпеки і стійкості критичної інформаційної інфраструктури.

Однак, те, що ця тема привертає увагу дослідників-правників, свідчать інші літературні джерела. Так,

Ю. А. Дорохіна у своїй статті «Розвиток системи захисту критичної інформаційної інфраструктури в Україні» аналізує критичну інформаційну інфраструктуру як елемент критичної інфраструктури та визначає, що її захист потребує більшої уваги з боку держави [20]. М. Б. Домарацький у статті «Нормативне й адміністративне забезпечення державного регулювання критичної інфраструктури в Україні: аналіз і оцінка» висвітлив проблеми неврегульованості забезпечення безпеки критичної інфраструктури України та її інформаційної складової [21].

Загалом аналіз наявних публікації дає можливість констатувати, що динамічні зміни у технологічній сфері, розширення мережевого взаємозв'язку та збільшення обсягу обміну інформацією породжують нові виклики та загрози щодо забезпечення безпеки і стійкості критичної інформаційної інфраструктури. Тому значний обсяг монографічних досліджень у сфері права, присвячено протидії, боротьбі та профілактиці кіберзлочинності і хоча такі роботи прямо не досліджують питання забезпечення безпеки та стійкості критичної інформаційної інфраструктури, але кіберзлочинність відноситься до тих факторів, що створюють загрозу та ризик заподіяння шкоди зазначеній інфраструктурі. Важливо відзначити ключові аспекти цієї проблеми у наукових дослідженнях: 1) зростання кількості та складності кіберзагроз призводить до потреби розробки новітніх методів та технологій захисту критичної інформаційної інфраструктури в умовах глобального кіберпростору, тому акцент робить на кіберзахисті інформаційних систем (А. О. Корченко, В. А. Козачок, А. І. Гізун [22]; І. В. Манжул [23]; Д. Г. Бобро, С. П. Іванюта, С. І. Кондратов, О. М. Суходоля [24]; В. В. Бухарєв [25]; О. К. Волох [26]); 2) розвиток міжнародних стандартів та законодавства для забезпечення кібербезпеки та стійкості інформаційних систем, що стає важливим елементом глобального управління (О. Бусол [27]; О. Л. Доброжанська та А. А. Демцов [28]); 3) впровадження передових технологій, таких як штучний інтелект, блокчейн та квантові обчислення, для підвищення рівня захисту та стійкості критичної інформаційної інфраструтктури (М. Сокиран [29]); 4) розробка методів аналізу та прогнозування кіберзагроз для своєчасного виявлення та запобігання можливим атакам на критичну інформаційну інфраструктуру (Д. Г. Бобро [30], М. Б. Домарацький [31], І. В. Діордіца [32], А. А. Русецький [33]; І. М. Ткаченко та Г. Г. Мягких [34]); 5) розбудова механізмів міжнародного співробітництва та обміну досвідом між країнами для ефективного вирішення загальних проблем безпеки інформаційних систем (Д. В. Дубов та М. А. Ожеван [35]; Р. Г. Бєляков [36]); 6) гуманітарні аспекти, дослідження соціокультурних та етичних вимірів забезпечення безпеки критичної інформаційної інфраструктури, враховуючи вплив глобалізації на сучасне суспільство (Л. Сорока та М. Сокиран [37]); (7) військові аспекти, дослідження у сфері забезпечення безпеки і стійкості критичної інформаційної інфраструктури в умовах збройного конфлікту (О. Г. Гаврилюк,В. О. Ткач та С. А. Паламарчук [38]).

Висновки. Усі вище зазначені напрямки наукових досліджень свідчить про постійну активність та потребу у наукових пошуках щодо інноваційних підходів у забезпеченні стійкості і безпеки критичної інформаційної інфраструктури у глобальному інформаційному середовищі. Однак, щодо питань адміністративно-правового забезпечення безпеки та стійкості критичної інформаційної інфраструктури, – вони залишаються недостатньо дослідженими.

ЛІТЕРАТУРА

1. Бірюков Д. С., Кондратов С. І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. К. : НІСД, 2012. 96 с.
2. Зелена книга з питань захисту критичної інфраструктури в Україні (друга версія проекту документа). Національний інститут стратегічних досліджень, 2014. URL: https://niss.gov.ua/sites/default/files/2014-11/1125_zelknuga.pdf
3. Протидія тероризму, нерозповсюдження зброї та матеріалів масового знищення й захист критичної інфраструктури : зб. матеріалів засідань Міжвідом. експерт. робоч. групи, створеної при НІСД. За ред. О. Д. Маркєєвої, Ю. М. Скалецького; Нац. ін-т стратег. дослідж. К. : НІСД, 2013. 101 с.
4. Концепція захисту критичної інфраструктури: стан, проблеми та перспективи її впровадження в Україні : зб. матеріалів міжнар. наук.-практ. конф. (7–8 листоп. 2013 р., Київ – Вишгород). Нац. ін-т стратег. дослідж. Упоряд. : Д. С. Бірюков, С. І. Кондратов. Київ : НІСД, 2014. 147 с.
5. Гнатюк С. О., Рябий М. О., Лядовська В. М. Визначення критичної інформаційної інфраструктури та її захисту: аналіз підходів. *Зв'язок*, № 4, 2014. С. 3–7.
6. Гончар С. Ф., Леоненко Г. П., Юдін О. Ю. Теоретико-методологічний аспект забезпечення інформаційної безпеки об'єктів критичної інфраструктури. *Вісник Національного університету «Львівська політехніка». Комп'ютерні системи та мережі*, 2014. № 806. С. 34–39.
7. Гончар С. Ф. Шляхи удосконалення державної політики забезпечення інформаційної безпеки критичної інфраструктури України : матеріали круглого столу «Державне реагування на загрози національним інтересам України: актуальні проблеми та шляхи їх розв'язання». К.: НАДУ, 2014. С. 92–95.
8. Levy, Steven. Hackers: Heroes of the Computer Revolution. New York: Anchor Press, 1984.
9. Year 2000 problem. Wikimedia Foundation, 2023. URL: https://en.wikipedia.org/wiki/Year_2000_problem
10. The year 2000 problem. Fourth report by the committee on government reform and oversight together with additional views. U.S. Government Printing Office, 1998. URL: https://www.congress.gov/105/crpt/hrpt827/CRPT-105hrpt827.pdf
11. Johnson, Cory. Y2K Crier's Crisis. The Arena Media Brands, Llc Thestreet is a Registered Trademark of Thestreet, INC., 1999. URL: https://www.thestreet.com/opinion/y2k-criers-crisis-839189
12. Rose, Ted. Who invented Y2K and why did it become so universally popular? Baltimore Sun, 1999. URL: https://www.baltimoresun.com/1999/12/22/who-invented-y2k-and-why-did-it-become-so-universally-popular/
13. Parsons, T. J. "Protecting Critical Information Infrastructures. Th e Co-ordination and Development of Cross-Sectoral Research in the UK". Plenary address at the Future of European Crisis Management conference (Uppsala 2001).
14. Moteff, John, Claudia Copeland, and John Fischer. Critical Infrastructures: What Makes an Infrastructure Critical? Report for Congress Received through the CRS Web. Order Code RL31556, 2003. URL: https://apps.dtic.mil/sti/pdfs/ADA467306.pdf
15. Dunn, Myriam. Understanding Critical Information Infrastructures: An Elusive Quest. Handbook, 2006. URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-2006-2-27-53.pdf
16. Leon Hempel, Benjamin Dominic Kraff, Robert Pelzer. Dynamic Interdependencies: Problematising Criticality Assessment in the Light of Cascading Effects. *International Journal of Disaster Risk Reduction*, 2018. No 30(3). URL: https://www.researchgate.net/publication/324559004_Dynamic_Interdependencies_Problematising_Criticality_Assessment_in_the_Light_of_Cascading_Effects
17. Luiijf E, Nieuwenhuijs A, Klaver M, Van Eeten M, Cruz E (2009) Empirical findings on critical infrastructure dependencies in Europe. In: Setola R, Geretshuber S (eds) CRITIS 2008, LNCS 5508, pp. 302–310.
18. Єсімов С., Скриньковський Р., Ковалів М., Крет І. Правові аспекти формування системи безпеки об'єктів критично важливої інформаційної інфраструктури в Україні. *Path of Science: International Electronic Scientific Journal,* 2018. Vol. 4, № 7. URL: https://pathofscience.org/index.php/ps/article/view/530
19. Осипчук І. І. Адміністративно-правові засади діяльності Служби безпеки України як суб'єкта забезпечення критичної інфраструктури: дис. … канд. юрид. наук: 12.00.07. Київ, 2021. 210 с.

20. Дорохіна Ю. А. Розвиток системи захисту критичної інформаційної інфраструктури в Україні. *Право і суспільство*, 2018. № С. 69–73.

21. Домарацький М. Б. Нормативне й адміністративне забезпечення державного регулювання критичної інфраструктури в Україні: аналіз і оцінка. *Вісник Національного університету цивільного захисту України*, 2020. Вип. 1(12). С. 470–475.

22. Корченко А. О., Козачок В. А., Гізун А. І. Метод оцінки рівня критичності для систем управління кризовими ситуаціями. *Захист інформації*, 2015. № 1. Т. 17. С. 86–98.

23. Манжул І. В. Захист енергетичної безпеки у контексті концепції створення державної системи захисту критичної інфраструктури України. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*, 2018. № 1-2 (10–11). С. 87–94.

24. Бобро Д. Г., Іванюта С. П., Кондратов С. І., Суходоля О. М. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України : Аналітична Доповідь. Київ : НІСД, 2019. 224 с.

25. Бухарєв В. В. Зарубіжний досвід забезпечення кібербезпеки та можливості його використання в Україні. *Науковий вісник Ужгородського національного університету. Право*, 2021. Вип. 43. Т. 3. С. 128–133.

26. Волох О. К. Питання кібернетичної безпеки в умовах розбудови інформаційного суспільства. *Юридичний науковий електронний журнал*, 2016. № 4. С. 104–107.

27. Бусол О. Інформаційна безпека США: законодавче регулювання та перспективи співпраці для України. Офіційний web-сайт Центру досліджень соціальних комунікацій НБУВ. URL: http://www.nbuviap.gov.ua/index.php?option=com_content&view=article&id=2988:informatsijna-bezpeka-ssha-zakonodavche-regulyuvannya-ta-perspektivispivpratsi-dlya-ukrajini&catid=8&Itemid=350.

28. Добржанська О. Л., Демцов А. А. Кібербезпека як феномен міжнародних відносин на прикладі Федеративної Республіки Німеччини. *Актуальні проблеми міжнародних відносин*, 2011. Вип. 102 (1). С. 111–116.

29. Sokiran, Maksym. Space Critical Infrastructures as Part of Critical Infrastructures: Threats and Methods of Protection. *Advanced Space Law*, 2020. Volume 5, 101-107. https://doi.org/10.29202/asl/2020/5/11

30. Бобро Д. Г. Удосконалення методології ранжування об'єктів критичної інфраструктури та їх віднесення до критичної інфраструктури: аналітична записка. URL: http://www.niss.gov.ua/content/articles/files/krutuchna_infra-a7636.pdf

31. Домарацький М.Б. Аналіз загроз у процесі категоріювання об'єктів критичної інформаційної інфраструктури на державному рівні. Інноваційне підприємництво, менеджмент, фінанси: стан, аналіз тенденцій та науково-економічний розвиток: матеріали міжнародної науково-практичної конференції. Львів: ЛЕФ, 2019. Ч. 2. С. 104–105.

32. Діордіца І. В. Класифікація кіберзагроз та їх легітимізація у нормативно-правових актах України. *Підприємництво, господарство і право*, 2017. № 10. С. 206–211.

33. Русецький А. А. Аналіз стану загроз критичній інфраструктурі в Харківській області. *Актуальні проблеми вітчизняної юриспуденції*, 2017. № 1. Т. 2. С. 18–20.

34. Ткаченко І. М., Мягких Г. Г. Використання теорії катастроф для оцінки стану кібербезпеки об'єктів критичної інформаційної інфраструктури: збірник тез «Системи і технології зв'язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку» : І Міжнародна науково-технічна конференція (25 – 26 листопада 2021 року). Київ, 2021. URL: https://sprotyvg7.com.ua/wp-content/uploads/2023/09/c_2021.pdf

35. Дубов Д. В., Ожеван М. А. Майбутнє кіберпростору та національні інтереси України: нові міжнародні ініціативи провідних геополітичних гравців : аналітична доповідь. К. : НІСД, 2012. С. 22.

36. Бєляков Р. Г. Взаємодія Управління боротьби з кіберзлочинністю МВС України з іншими правоохоронними органами : питання сьогодення. *Право і Безпека*, 2014. № 4 (55). С. 85–88.

37. Сорока Л. В., Сокіран. М. В. Технологічний прогрес та права людини. Кібербезпека в сучасному світі: актуальні виклики: збірник матеріалів Всеукраїнської науково-практичної конференції (м. Одеса, 29 жовтня 2019 року). Одесса, 2019. С. 25–28.

38. Гаврилюк О. Г. Ткач В. О. Паламарчук С. А. Обґрунтування основних напрямів забезпечення кібернетичної безпеки мереж спеціального призначення: збірник тез «Системи і технології зв'язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку» : І Міжнародна науково-технічна конференція (25–26 листопада 2021 року). Київ, 2021. URL: https://sprotyvg7.com.ua/wp-content/uploads/2023/09/c_2021.pdf