2021, p.234-244. Available at https://ela.kpi.ua/bitstream/123456789/55128/1/P234-244.pdf

10. Popelo, O., Butko, M., Revko, A., Garafonova, O., Rasskazov, O., (2021). Strategy of the Formation and Development of an Innovative Agroindustrial Cluster of the Region in a Context of Decentralization of the Authoritative Powers. Financial and credit activity: problems of theory and practics, v. 2, n. 37, p. 219-230, 2021. Available at http://fkd1.ubs.edu.ua/article/view/230180

11. Artomova, A., Malkina, M. (2019). The trade balance of Germany in the skilled crisis and post-crisis development of world economy. Journal of economic reforms– 2019. – № 1 (33). – С. 13. Available at http://nbuv.gov.ua/UJRN/Cher_2019_1_5

12. Davydova, I., Artomova, A., & Uvarova, I. (2023). Methodology for Sustainable Development Management of the Power Supply Industry in the Global Market. Adaptive Management: Theory and Practice. Series Economics, 15(30). Available at https://doi.org/10.33296/2707-0654-15(30)-19

13. Fornell, C., Larcker, D. (2021). Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research. 18(1) S. 39–50. Available at DOI: 10.2307/3151312

6.3 Механізми забезпечення стійкості критичної інфраструктури: європейський досвід

Храпкіна В. В.,
доктор економічних наук, професор,
професор кафедри маркетингу та управління бізнесом,
Трушкіна Н. В.,
кандидат економічних наук, старший дослідник,
докторант, старший науковий співробітник сектору
промислової політики та інноваційного розвитку
відділу промислової політики та енергетичної безпеки,
Науково-дослідний центр індустріальних проблем розвитку НАН України

У сучасних умовах критична інфраструктура є основою національної економіки будь-якої країни. Порушення роботи критично важливих систем та основних послуг, таких як телекомунікації, енерго- та водопостачання, транспортні та фінансові системи, може призвести до значних економічних збитків. Ці системи є дуже вразливими до різноманітних потрясінь – від кліматичних і геологічних небезпек до промислових аварій, терористичних атак, кіберзагроз, збройних конфліктів і бойових дій, які можуть спричинити каскадний негативний вплив на місцевому, національному та навіть глобальному рівнях.

Тому стійкість критично важливої інфраструктури в Європейського Союзу визнано насамперед національною відповідальністю кожної країни. Як показує аналіз літератур зарубіжних [1-17] і вітчизняних [18-27] видатних вчених, Стійкість критичної інфраструктури охоплює здатність запобігати, захищати, реагувати, протистояти, пом’якшувати, поглинати, пристосовуватись і відновлюватися після кризових і надзвичайних ситуацій, збройних конфліктів, воєнних подій, які можуть порушити надання основних послуг. Це особливо важливо для критичної інфраструктури, оскільки повний захист, як правило, неможливий.

Отже, коли відбувається кризова ситуація, цілі стійкості критично важливої інфраструктури можна оцінити у двох вимірах: обмеження масштабу пошкоджень та обмеження тривалості перерви у наданні послуг, спричиненої пошкодженнями. Важливо зазначити, що відновлення не обов'язково означає повернення до попереднього стану, який існував до надзвичайної ситуації або інциденту, але може передбачати зміну, адаптацію до нових умов та покращення функціональності систем. У цьому контексті забезпечення стійкості критичної інфраструктури може здійснюватися на основі поєднання декількох ключових якостей:

– надійність (здатність продовжувати роботу або залишатися стійкими. Це передбачає проєктування структур або систем, які є достатньо міцними, щоб витримати передбачувані потрясіння. Це також передбачає інвестування в елементи критично важливої інфраструктури та їх підтримку, щоб вони могли витримати події з низькою ймовірністю, але з високими наслідками);

– резервування (здатність продовжувати роботу завдяки заміні або резервним системам, які можуть бути задіяні, якщо щось важливе вийде з ладу або перестане працювати);

– винахідливість (здатність вміло керувати подією в міру її розгортання. Включає в себе визначення варіантів, пріоритетів, що потрібно зробити, щоб контролювати збитки і почати їх пом'якшувати, а також донесення рішень до людей, які будуть їх виконувати. Винахідливість залежить насамперед від людей, а не від технологій. Швидке відновлення – це здатність повернутися до нормального життя якнайшвидше після катастрофи. Плани на випадок непередбачуваних ситуацій та безперервності бізнесу, ефективні аварійні служби та засоби доставки потрібних людей і ресурсів у потрібне місце мають вирішальне значення);

– адаптивність (засоби для засвоєння нових уроків, які можна винести з катастрофи. Вона передбачає перегляд планів, модифікацію процедур і впровадження нових інструментів і технологій, необхідних для підвищення

надійності, винахідливості та здатності до відновлення до наступної кризової ситуації).

Для ЄС критична інфраструктура не лише тісно пов'язана з політикою та законодавством, що забезпечує функціонування внутрішнього європейського ринку, але й із його програмою безпеки та оборони, включаючи стратегічний пріоритет захисту країн-членів Союзу та його громадян, а також Свобода дій ЄС. Критична інфраструктура необхідна для надання основних державних послуг та економічної діяльності на внутрішньому ринку, а також для національної безпеки та оборони [28-30].

З огляду на це, на даний час держави-члени ЄС приділяють особливу увагу посиленню стійкості своєї критичної інфраструктури. Для цього уряди багатьох європейських країн розробляють стратегічні завдання (інституційні, організаційно-економічні, фінансові, інформаційні), реалізація яких сприятиме підвищенню обізнаності шляхом моніторингу та обміну інформацією; запобіганню збоїв за допомогою заходів безпеки та заходів готовності; мінімізації наслідків потенційного збою за допомогою швидкого та ефективного реагування, резервування або резервних заходів, включаючи можливості відновлення/ремонту; забезпеченню своєчасного відновлення після збою за допомогою планування на випадок надзвичайних ситуацій і готовності.

Слід відмітити, що Європейський Союз проголосив нові пріоритети політики забезпечення стійкості функціонування критичної інфраструктури та надання життєво важливих послуг на ринку ЄС. Нові стратегічні цілі та завдання Єврокомісії та держав-членів визначено в Рекомендаціях Ради ЄС, спрямованих на посилення зусиль Європейського Союзу щодо підвищення стійкості критично важливих об'єктів інфраструктури.

У грудні 2022 р. Рада ЄС ухвалила Рекомендації зі скоординованого підходу до стійкості критичної інфраструктури. Зокрема, рекомендовано запровадити необхідні інструменти та забезпечити координацію дій на рівні ЄС з підвищення готовності та реагування на безпекові інциденти, що загрожують порушенню надання життєво важливих послуг на внутрішньому ринку Євросоюзу. Тоді ж Рада ЄС прийняла нову Директиву щодо стійкості критичних об'єктів (Директива CER).

У 2022 році Європарламентом схвалено оновлені правила щодо поліпшення захисту критичної інфраструктури країн Європейського Союзу. Ці правила гармонізують визначення критичної інфраструктури, щоб вона була сумісною для різних країн блоку. Законодавство охоплює 11 критично важливих сфер економічної діяльності: енергетика, транспорт, інфраструктура банківської системи та фінансових ринків, цифрова інфраструктура,

водопостачання та водовідведення, харчова промисловість, система охорони здоров'я, державні установи.

Відповідно до нових правил країни-члени ЄС мають схвалити національні стратегії стійкості та підтримувати певним чином транскордонну комунікацію з цих питань. Для забезпечення прозорості агенти, яких вважають частиною критичної інфраструктури, мають інформувати національні органи влади про будь-які інциденти чи проблеми, а органи влади – повідомляти про це громадськість, якщо це становить суспільний інтерес.

У попередній редакції директиви про критичну інфраструктуру у загальну рамку європейських правил входила лише енергетична інфраструктура та транспорт. Нове законодавство узгоджено також із нещодавно прийнятою директивою про кібербезпеку.

Ухвалені законодавчі акти відображають прихильність країн Європейського Союзу до формування системи забезпечення безпеки та стійкості функціонування критичної інфраструктури на основі ринкових підходів, стимулювання державно-приватного партнерства [31-32] і максимального використання власної зацікавленості операторів життєво важливих об’єктів у сталості надання ними послуг та безперервності бізнес-процесів.

До головних інструментів ЄС для забезпечення стійкості критичної інфраструктури можна віднести такі:

– застосування методології оцінювання ризиків критичної інфраструктури на основі аналізу впливу загроз будь-яких типів (all-hazard approach) при подальшій адаптації національних підходів до ризик-аналізу;

– надання інституційної, методичної та консультативної допомоги;

– розроблення стратегічних документів адаптації до зміни клімату та стійкості критичної інфраструктури;

– сприяння підвищенню кваліфікації персоналу операторів критичної інфраструктури та проведенню стрес-тестів;

– координація зусиль на рівні ЄС у випадку виникнення кризової або надзвичайної ситуації;

– формування механізмів фінансової підтримки діяльності у цій сфері.

На початку 2023 р. було оголошено про синхронізацію зусиль ЄС і НАТО щодо забезпечення стійкості критичної інфраструктури. Для посилення співпраці Європейський Союз і Північноатлантичний альянс започаткували Цільову групу щодо стійкості критичної інфраструктури. На даний час дана Цільова група представила остаточний звіт про оцінку, де описано поточні виклики безпеці та стратегічні рекомендації щодо посилення стійкості

критичної інфраструктури. Цей комплекс рекомендацій стосуються необхідності забезпечення стійкості і розвитку співпраці шляхом:

1) посилення взаємодії при повному використанні синергії (наприклад, у разі виникнення серйозної загрози або значних змін у контексті безпеки); сприяння взаємодії між членами Альянсу, державами-членами і приватним сектором, у тому числі щодо безпеки критично важливої інфраструктури [33]; проведення спеціальних дискусій на основі сценаріїв;

2) посилення структурованого діалогу з питань стійкості і структурованого діалогу з питань військової мобільності і розширення існуючих штабних переговорів з питань кібербезпеки, космосу, морських перевезень і енергетики, а також між Міжнародним військовим штабом НАТО і Військовим штабом ЄС;

3) сприяння поширенню найкращих практик, оцінок і посиленню моніторингу впливу на безпеку та співпрацю, у тому числі між цивільними і військовими суб'єктами; проведення регулярного паралельного й скоординованого оцінювання загроз критичній інфраструктурі тощо).

У Європейському Союзі пропонується застосування відповідного інструментарію з управління стійкістю критичної інфраструктури, який дозволяє урядам країн вирішити ряд взаємопов'язаних управлінських завдань, а саме:

1) Створення багатогалузевої структури управління для забезпечення стійкості критичної інфраструктури (уряди мають прийняти загальнодержавний підхід до забезпечення стійкості критичної інфраструктури, що охоплює різні ризики та сектори інфраструктури. Таке управління мало б включати галузеві міністерства та відомства, які контролюють створення і регулювання інфраструктури в багатьох критичних секторах, а також тих, хто відповідає за стійкість до всіх небезпек і загроз. Координація в Урядовому центрі дозволить керувати інтересами всіх зацікавлених сторін і робити відповідні компроміси для ефективної політики стійкості. Наприклад, у Франції Генеральний секретаріат оборони та національної безпеки під керівництвом прем’єр-міністра координує політику стійкості критичної інфраструктури у 8 галузевих міністерствах для 12 секторів інфраструктури та з підходом до багатьох небезпек);

2) розуміння складних взаємозалежностей і вразливостей в інфраструктурних системах для визначення пріоритетності зусиль з розбудови стійкості (урядам необхідно прийняти методології та метрики для визначення критично важливих функцій, систем та активів, які мають бути пріоритетними для інвестицій у розбудову стійкості. Для цього потрібне добре розуміння того, як збої можуть вплинути на інфраструктурні активи та де виявлені залежності

та взаємозалежності, які можуть посилити їхній вплив. Після визначення пріоритетних вузлів і концентраторів у взаємозалежних системах необхідно оцінити їх стійкість за допомогою відповідних показників і порівняти фактичні та очікувані результати, щоб побачити, де є прогалини. У Нідерландах Національний координатор з питань безпеки та боротьби з тероризмом (NCTV) розробив 3-етапну методологію, щоб спочатку визначити критичну інфраструктуру та класифікувати її відповідно до критичності (A або B), по-друге, оцінити їхню вразливість до численних ризиків і, по-третє, встановити пріоритети для інвестиції в стійкість);

3) встановлення довіри між урядом та операторами шляхом забезпечення обміну інформацією про ризики (уряди мають створити платформи для обміну інформацією з операторами критичної інфраструктури для всебічного і спільного розуміння ризиків і вразливостей, забезпечуючи безпеку і конфіденційність інформації, якою вони обмінюються. Вкрай важливо переконатися, що дизайн цих платформ забезпечує безпеку та конфіденційність інформації, що надається, з чіткими правилами доступу, щоб забезпечити довірений обмін конфіденційною інформацією. Обмін інформацією є фундаментальним для урядів, щоб отримати всебічне розуміння вразливостей критичної інфраструктури. Це також допомагає операторам зрозуміти власні вразливості, свою залежність від інших інфраструктур і те, як збої в їхніх послугах можуть вплинути на інші інфраструктури або навіть на них самих. Наприклад, інструмент даних та аналітики для національної інфраструктури Великобританії (DAFNI) надає платформа даних, моделей і технічних інструментів для комплексного аналізу інфраструктури для аналізу продуктивності системи та здійснення розумних інвестицій);

4) розбудова партнерств для вироблення спільного бачення та узгодження досяжних цілей у сфері стійкості (уряди мають налагодити постійний діалог з операторами критичної інфраструктури з державного та приватного секторів, взявши за відправну точку очікування громадськості. Розвиток розуміння громадських очікувань щодо потенційної втрати послуг інфраструктури може бути корисним способом ініціювання діалогу. Крім обміну інформацією про ризики та вразливі місця, стійкість критичної інфраструктури залежить від партнерства урядів з операторами інфраструктури з державного та приватного секторів у зусиллях щодо стійкості. У той час як оператори та уряди погоджуються щодо необхідності захисту критично важливих активів і підтримки своїх послуг, погляди можуть відрізнятися щодо необхідного рівня стійкості, засобів її досягнення та нормативних вимог, які мають застосовуватися. Ці заходи мають фінансові наслідки та викликають питання

про те, хто візьме на себе додаткові витрати, щоб інвестувати в стійкість. Так, у Швейцарії національна стратегія захисту критичної інфраструктури, координована Федеральним відомством цивільного захисту, базується на партнерстві та різноманітних платформах з операторами критичної інфраструктури, федеральні та субнаціональні органи влади. Крім аналізу ризиків та обміну інформацією, Керівництво з критичної інфраструктури розробляється спільно й дозволяє встановлювати цілі стійкості для операторів. У Німеччині UP KRITIS є національною ініціативою між державою та носіями Critical Інфраструктури захисту критичних інформаційних інфраструктур. UP KRITIS складається з понад 450 співробітників);

5) визначення комплексу політичних заходів для визначення пріоритетності економічно ефективних заходів з підвищення стійкості на всіх етапах життєвого циклу інфраструктури (уряди мають визначити комплекс політичних інструментів на основі аналізу витрат і вигоди, щоб заохотити операторів інвестувати в забезпечення стійкості та досягти поставлених цілей. Такі заходи мають стосуватися всього життєвого циклу інфраструктури від планування до експлуатації, технічного обслуговування та оновлення або модернізації. Пріоритезація заходів стійкості урядом має ґрунтуватися на аналізі рентабельності з урахуванням наслідків для вартості послуг. Наприклад, у Фінляндії Управління з питань енергетики встановлює вимоги до стандартів безперервності роботи та надійності в секторі електроенергії, а Національне агентство аварійного постачання надає операторам інструменти, вказівки та методи для дотримання цих правил. У Франції держава, оператори критичної інфраструктури та місцеві органи влади погодили заходи для підвищення стійкості критичної інфраструктури до ризику великої повені в Парижі. Це включає в себе обмін інформацією, готовність до надзвичайних ситуацій і зниження вразливості існуючої та майбутньої інфраструктури);

6) забезпечення підзвітності та моніторингу впровадження політики стійкості критичної інфраструктури (уряди мають здійснювати моніторинг впровадження та оцінювати прогрес у досягненні цілей щодо забезпечення стійкості, створивши чітку систему підзвітності для операторів. Перегляд ефективності інструментів політики стійкості має дозволити коригувати динамічний ландшафт ризиків та інновації в інфраструктурі, беручи до уваги потребу в передбачуваній та стабільній нормативній базі, яка сприятиме інвестиціям в інфраструктуру. Так, через 10 років після прийняття Європейська Комісія оцінює свою Директиву про європейську критичну інфраструктуру, щоб визначити, чи залишається вона актуальною та ефективною);

7) врахування транскордонного виміру інфраструктурних систем (уряди мають координувати національну політику стійкості критичної інфраструктури із сусідніми країнами та за її межами, щоб вирішувати питання транскордонної залежності. Необхідно створити міжнародні механізми обміну інформацією для оцінки ризиків і вразливостей через кордони, а також для розробки спільних підходів до стійкості критичної інфраструктури. Наприклад, Європейська програма захисту критичної інфраструктури (EPCIP) є довгостроковою програмою, яка охоплює різні інструменти захисту критичної інфраструктури в ЄС, включаючи регулярні зустрічі національних контактних осіб. Його зовнішній вимір включає регулярні зустрічі зі стратегічними партнерами та нещодавно був розширений за рахунок співпраці з сусідніми країнами).

Виходячи з вищевикладеного можна дійти такого висновку. Сучасна політика забезпечення стійкості критичної інфраструктури має враховувати різноманітні й складні шокові події, більш взаємозалежні системи і країни, а також швидкий темп інновацій в інфраструктурних секторах [34-35]. Інвестиції у розвиток критично важливої інфраструктури зростають у всьому світі, надаючи країнам можливість переглянути свою політику і підвищити стійкість, одночасно посилюючи захист діючих об’єктів інфраструктури.

Системний підхід має очевидні переваги при розробленні політики щодо розвитку критичної інфраструктури. Така політика має враховувати комплекс ризиків, небезпек і загроз; забезпечувати координацію між різними секторами (державним і приватним); охоплювати весь життєвий цикл критичної інфраструктури та сприяти транскордонному співробітництву. Таким чином, при розробленні державної політики забезпечення стійкості критичної інфраструктури слід базуватися на принципах і підходах системного мислення, до яких можна віднести комплексність небезпек і загроз, системний рівень, багатосекторальний підхід, транскордонний вимір, підхід на основі життєвого циклу, повний цикл управління ризиками, ризик-орієнтований підхід.

При цьому варто відмітити, що державна політика, яку спрямовано на підвищення стійкості критичної інфраструктури, має поєднувати комплекс заходів зі стимулювання, резервування, надійності систем, резервних потужностей, швидкого відновлення та адаптації до нових ризиків і загроз або мінливих чинників ризику. Для вдосконалення управління критичними ризиками на національному рівні та зменшення взаємного та каскадного впливу надзвичайних ситуацій на розвиток критичної інфраструктури необхідно:

1) визначити, де перебої в роботі критично важливої інфраструктури та ланцюгів постачання можуть призвести до перехресного впливу на інші галузі та географічні кордони, а також спричинити каскадні ефекти;

2) розробити фіскальні та регуляторні варіанти, які сприятимуть створенню резервних потужностей, диверсифікації або резервних систем для зменшення ризику збоїв і тривалих періодів перебоїв у роботі систем критичної інфраструктури;

3) координувати проєктування мереж критичної інфраструктури (наприклад, енергетичних, транспортних, телекомунікаційних та інформаційних систем) з політикою містобудування та управління територіями;

4) використовувати можливості приватного сектору для розбудови стійкої інфраструктури;

5) заохочувати бізнес вживати заходів для забезпечення безперервності бізнесу, приділяючи особливу увагу операторам критичної інфраструктури, шляхом розробки стандартів та інструментарію, призначених для управління ризиками, що загрожують операціям або наданню основних послуг;

6) забезпечити функціонування критично важливої інфраструктури, інформаційних систем та мереж після кризової ситуації;

7) забезпечити наявність та застосування планів реагування на випадок надзвичайних ситуацій на випадок інциденту, який порушує функціонування мереж критично важливої інфраструктури.

Стійкість критичної інфраструктури залежить від співпраці урядів з операторами інфраструктури з державного та приватного секторів. Хоча оператори та уряди погоджуються з необхідністю захисту критично важливих активів і підтримки послуг, їхні погляди на рівень необхідної стійкості, засоби її досягнення та регуляторні вимоги, які мають застосовуватися, можуть відрізнятися. Ці рішення мають фінансові наслідки і ставлять питання про те, хто буде нести додаткові витрати, які пов'язано з інвестуванням у стійкість.

Державно-приватна співпраця між урядами та операторами з метою заохочення діалогу з цих питань є корисною для спільного розроблення та впровадження політики забезпечення стійкості та безпеки критичної інфраструктури. Встановлення довіри, забезпечення безпечного обміну інформацією, удосконалення механізмів розподілу витрат і зміцнення міжнародного співробітництва є одними з ключових завдань, які варто вирішити при створенні таких партнерств, і вимагають відповідних механізмів забезпечення їх реалізації.

Уряди європейських країн можуть обирати з безлічі політичних інструментів для посилення стійкості критичної інфраструктури. Опитування Організації економічного співробітництва та розвитку (ОЕСР) визначило 22 інструменти – від нормативно-правових актів і компенсаційних механізмів до добровільних механізмів, заснованих на партнерстві. Цей перелік включає:

надання інформації про небезпеки та загрози; добровільні механізми або платформи обміну інформацією; обов’язкові механізми або платформи обміну інформацією; заходи з підвищення обізнаності та тренінги; рекомендації щодо стійкості для операторів критичної інфраструктури; сприяння розвитку/використанню професійних стандартів; механізм стимулювання для оцінки ризиків і вразливостей; механізми стимулювання інвестування в стійкість; правила забезпечення безперервності діяльності, що базуються на ефективності; обов'язкові плани забезпечення безперервності діяльності; перевірки та оцінка ефективності; штрафи за недотримання вимог стійкості; ранжування за результатами перевірки/виконання; звіт про стійкість операторів; обмін передовим досвідом; державні інвестиції в стійкість інфраструктури; рекомендації для субнаціональних рівнів управління; обов'язкове страхування критичної інфраструктури; рецензування, моніторинг та оцінка; галузеві угоди про взаємодопомогу.

Визначення переваг і недоліків видів даного інструментарію у різних політичних контекстах може стати великою підтримкою для розроблення політики захисту критичної інфраструктури та стійкості. Регулювання є важливим методом, який забезпечує обов’язкові вимоги та механізми забезпечення стійкості критичної інфраструктури. Регуляторний підхід має сильні сторони в тому, що він передбачає обов’язкові вимоги, але він також може виявитися дорогим і створити часові затримки між технологічними розробками в багатьох секторах, які потребують регулярного оновлення.

Можуть бути застосовані різні нормативні підходи: від директивних галузевих нормативних актів до тих, що базуються на ефективності, що дозволяє операторам самим визначати шляхи досягнення цілей стійкості. Фінансові стимули забезпечують ще один спосіб збільшення інвестицій і планів безперервності для захисту критичної інфраструктури та стійкості. Розроблення механізмів компенсації для клієнтів у разі збою в обслуговуванні або інших типів штрафів може бути використана для інтерналізації переваг стійкості. Це надає операторам вибір шляхів підвищення їх стійкості.

Державне фінансування, яке використовується для стійкості критичної інфраструктури, може встановити стандарти та продемонструвати цінність початкових інвестицій у стійкість. Інтеграція стійкості до великих державних інвестиційних проєктів є прикладом цінності та переваг цих інвестицій і може створити стимули для інших власників і операторів критичної інфраструктури наслідувати їхній приклад. У державних закупівлях дедалі більше враховується стійкість до зміни клімату, що може слугувати підходом до поширення інших ризиків. Створення публічного доступу до оцінок критичної інфраструктури

створює занепокоєння для компаній та їх іміджу. Рейтинги є важливими показниками стійкості та механізмом створення стимулів.

Разом з тим, урядам важливо знайти правильний баланс між обов'язковими та добровільними механізмами, щоб посилити залучення зацікавлених сторін до цього процесу та забезпечити ефективне інвестування у стійкість.

Краща практика Фінляндії є прикладом розроблення рамок успішної співпраці для посилення стійкості критичної інфраструктури. Дана практика наголошує на державно-приватній співпраці, обміні інформацією та досягненні консенсусу щодо розроблення політики та встановлення цілей. Ця модель управління дала вражаючі результати у перші роки її впровадження. Однак з'явилися нові виклики, а саме: необхідність вирішення проблем, пов'язаних з витратами для споживачів, різницею у можливостях великих і малих операторів, діджиталізацією та зміною клімату. Це й стане напрямом подальших досліджень.

Список використаних джерел:

1. Forsberg C.-J., Kourti N. European reference network for critical infrastructure protection – ERNCIP 2020 strategy. JRC Scientific and Policy Reports (JRC85351). Italy, Ispra: European Commission, Joint Research Centre, Institute for the Protection and Security of the Citizen, 2013. 55 p.

2. Poustourli A., Kourti N. Standarts for critical infrastructure protection. Coopepation among standardization organizations and the scientific and academic community: Conference Proceedings / Edited by I. Mijatovic, K. Jakobs. Germany, Aachen: Euras Contributions to Standardisation Research, 2014. P. 181-195.

3. Argyroudis S. A., Mitoulis S. A., Hofer L., Zanini M. A., Tubaldi E., Frangopol D. M. Resilience assessment framework for critical infrastructure in a multi-hazard environment: Case study on transport assets. Science of The Total Environment. 2020. Vol. 714. Article 136854. https://doi.org/10.1016/ j.scitotenv.2020.136854.

4. Clark-Ginsberg A., Rueda I. A., Monken J. et al. Maintaining critical infrastructure resilience to natural hazards during the COVID-19 pandemic: hurricane preparations by US energy companies. Journal of Infrastructure Preservation and Resilience. 2020. Vol. 1. Article 10. https://doi.org/10.1186/s43065-020-00010-1.

5. Galbusera L., Trucco P., Giannopoulos G. Modeling interdependencies in multi-sectoral Critical Infrastructure systems: evolving the DMCI approach. Reliability Engineering and System Safety. 2020. Vol. 203. Article 107072. https://doi.org/10.1016/j.ress.2020.107072.

6. Galbusera L., Cardarilli M., Giannopoulos G. The ERNCIP survey on COVID-19: Emergency & Business Continuity for fostering resilience in critical infrastructures. Safety Science. 2021. Vol. 139. Article 105161. https://doi.org/10.1016/j.ssci.2021.105161.

7. Arvidsson B., Johansson J., Guldåker N. Critical infrastructure, geographical information science and risk governance: A systematic cross-field review. Reliability Engineering & System Safety. 2021. Vol. 213. Article 107741. https://doi.org/10.1016/j.ress.2021.107741.

8. Kumar N., Poonia V., Gupta B.B., Goyal M. K. A novel framework for risk assessment and resilience of critical infrastructure towards climate change. Technological Forecasting and Social Change. 2021. Vol. 165. Atricle 120532. https://doi.org/10.1016/j.techfore.2020.120532.

9. Mottahedi A., Sereshki F., Ataei M., Qarahasanlou A. N., Barabadi A. Resilience estimation of critical infrastructure systems: Application of expert judgment. Reliability Engineering & System Safety. 2021. Vol. 215. Article 107849. https://doi.org/10.1016/j.ress.2021.107849.

10. Osei-Kyei R., TamV., Ma M., Mashiri F. Critical review of the threats affecting the building of critical infrastructure resilience. International Journal of Disaster Risk Reduction. 2021. Vol. 60. Article 102316. https://doi.org/10.1016/ j.ijdrr.2021.102316.

11. Markopoulou D., Papakonstantinou V. The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular. Computer Law & Security Review. 2021. Vol. 41. Article 105502. https://doi.org/10.1016/j.clsr.2020.105502.

12. Rathnayaka B., Siriwardana C., Robert D., Amaratunga D., Setunge S. Improving the resilience of critical infrastructures: Evidence-based insights from a systematic literature review. International Journal of Disaster Risk Reduction. 2022. Vol. 78. Article 103123. https://doi.org/10.1016/ j.ijdrr.2022.103123.

13. Rehak D., Hromada M., Onderkova V., Walker N., Fuggini C. Dynamic robustness modelling of electricity critical infrastructure elements as a part of energy security. International Journal of Electrical Power & Energy Systems. 2022. Vol. 136. Article 107700. https://doi.org/10.1016/ j.ijepes.2021.107700.

14. Shen L., Li J., Suo W. Risk response for critical infrastructures with multiple interdependent risks: A scenario-based extended CBR approach. Computers & Industrial Engineering. 2022. Vol. 174. Article 108766. https://doi.org/10.1016/j.cie.2022.108766.

15. Urlainis A., Ornai D., Levy R., Vilnay O., Shohet I. M. Loss and damage assessment in critical infrastructures due to extreme events. Safety Science. 2022. Vol. 147. Article 105587. https://doi.org/10.1016/j.ssci.2021.105587.

16. Wells E. M., Boden M., Tseytlin I., Linkov I. Modeling critical infrastructure resilience under compounding threats: A systematic literature review. Progress in Disaster Science. 2022. Vol. 15. Article 100244. https://doi.org/10.1016/j.pdisas.2022.100244.

17. Wang D., Gryshova I., Balian A., Kyzym M., Salashenko T., Khaustova V., Davidyuk O. Assessment of Power System Sustainability and Compromises between the Development Goals. Sustainability. 2022. Vol. 14. Iss. 4. Article 2236. https:// doi.org/10.3390/su14042236.

18. Зелена книга з питань захисту критичної інфраструктури в Україні: зб. матеріалів міжнар. експерт. нарад / упоряд. Д. С. Бірюков, С. І. Кондратов; за заг. ред. О.М. Суходолі. Київ: НІСД, 2016. 176 с.

19. Бобро Д. Г. Методологія оцінки рівня критичності об'єктів інфраструктури. Стратегічні пріоритети. 2016. № 3(40). С. 78-86.

20. Бірюков Д. Концепція захисту критичної інфраструктури як елемент загальноєвропейської безпекової політики. Наукові записки ІПіЕНД ім. І. Ф. Кураса НАН України. 2018. Вип. 6(68). С. 106-115.

21. Єрменчук О. Оцінка загроз критичній інфраструктурі як важлива складова частина діяльності із захисту державної безпеки. Jurnalul juridic national: teorie şi practică. 2018. Декабрь. С. 50-54.

22. Єрменчук О. П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України: монографія. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.

23. Газдайка-Васильшин І. Б. Основні терміни проєкту Закону України «Про критичну інфраструктуру та її захист». Міжнародний журнал «Право і суспільство». 2019. Вип. 9. С. 15-20.

24. Підюков П. П., Калиновський О. В. Система державного захисту критичної інфраструктури України: генеза, сучасний стан і перспективи оптимізування в умовах подальшого забезпечення національної безпеки країни. Часопис Київського університету права. 2020. № 4. С. 355-359. https://doi.org/10.36695/2219-5521.4.2020.63.

25. Теленик С. С. Державна система захисту критичної інфраструктури України: концептуальні засади адміністративно-правового регулювання. Херсон: Видавничий дім «Гельветика», 2020. 602 с.

26. Ганкевич К. Б., Левчук В. Д., Корольов С. С. Особливості становлення правових засад існування об'єктів критичної інфраструктури України в системі Міністерства оборони України. Юридичний науковий електронний журнал. 2021. № 11. С. 79-82. https://doi.org/10.32782/2524-0374/2021-11/15.

27. Франчук В. І., Пригунов П. Я., Мельник С. І. Безпека об'єктів критичної інфраструктури в Україні: організаційно-нормативні проблеми та підходи. Соціально-правові студії. 2021. Вип. 3(13). С. 142-148. https://doi.org/10.32518/2617-4162-2021-3-142-148.

28. Лойко В. В., Храпкіна В. В., Маляр С. А., Руденко М. В. Економіко-правові засади забезпечення захисту критичної інфраструктури. Financial and Credit Activity Problems of Theory and Practice. 2020. № 4(35). С. 426-438. https://doi.org/10.18371/fcaptp.v4i35.222453.

29. Кизим М. О., Хаустова В. Є., Трушкіна Н. В. Сутність поняття «критична інфраструктура» з позицій національної безпеки України. Бізнес Інформ. 2022. № 12. С. 58-78. https://doi.org/10.32983/2222-4459-2022-12-58-78.

30. Bezpartochnyi M., Khaustova V., Trushkina N. Bibliometric analysis of the relationship between the concepts of "critical infrastructure" and "national security". Management of socio-economic transformations of business processes: current realities, global challenges, forecast scenarios and development prospects: scientific monograph. Sofia: Professor Marin Drinov Publishing House of Bulgarian Academy of Sciences, 2023. P. 177-193. https://doi.org/10.5281/zenodo.10463183.

31. Хаустова В., Жукова І., Трушкіна Н. Закордонний досвід фінансового забезпечення відбудови та модернізації критичної інфраструктури». Věda a perspektivy. 2023. No. 7(26). Str. 178-192. https://doi.org/10.52058/2695-1592-2023-7(26)-178-192.

32. Кизим М. О., Хаустова В. Є., Трушкіна Н. В. Фінансове забезпечення розвитку критичної інфраструктури в умовах повоєнної відбудови економіки України. Бізнес Інформ. 2023. № 8. С. 263-274. https://doi.org/10.32983/2222-4459-2023-8-263-274.

33. Пушак Я. Я., Хаустова В. Є., Трушкіна Н. В. Безпекова стратегія розвитку критичної інфраструктури в умовах повоєнної відбудови економіки України. Науковий вісник Львівського державного університету внутрішніх справ. Сер.: Економічна: зб. наук. праць. Львів: ЛьвДУВС, 2023. Вип. 1. С. 68-78. https://doi.org/10.32782/2311-844X/2023-1-10.

34. Концепти інноваційного розвитку підприємництва: колективна монографія / за заг. ред. д.е.н., проф. В. В. Храпкіної; Національний університет «Києво-Могилянська академія». Київ: Інтерсервіс, 2018. 263 с.

35. Храпкіна В., Трушкіна Н. Застосування штучного інтелекту у цифровому маркетингу. Поведінкова економіка: від теорії до практики: міждисц. навч. посіб. / за наук. ред. І. Л. Татомир, Л. Г. Квасній; Прикарпатський ін-т імені Михайла Грушевського ПрАТ ВНЗ «МАУП». Трускавець: ПОСВІТ, 2022. С. 300-311.

6.4.Нечіткий алгоритм прийняття рішень: схема Беллмана-Заде оцінки альтернатив

Дебела І.М.,
кандидат сільськогосподарських наук, доцент,
доцент кафедри менеджменту, маркетингу та інформаційних технологій
Херсонський державний аграрно-економічний університет

Проблеми моделювання процесів в соціально-економічних системах принципово відрізняються від проблем автоматизованого управління технічними системами. Ця відмінність полягає в тому, що в технічних системах цілі управління є екзогенними - зовнішніми по відношенню до об'єкта управління, що означає пасивність об'єкта управління, відсутність в ньому ендогенних цілей і як наслідок, простота формалізації процесу управління.