УДК 351: 65.012.8 (477) **doi: 10.26906/SUNZ.2025.1.178-183**

О. В. Третьяков, Б. Д. Халмурадов, Н. М. Кічата, А. В. Ремська

Державний університет «Київський авіаційний інститут», Київ, Україна

ПІДХІД ДО КІЛЬКІСНОЇ ОЦІНКИ СТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. Стійкість об'єктів критичної інфраструктури визначається як здатність готуватися до мінливих умов та адаптуватися до них, а також витримувати збої й швидко відновлюватися після них, включно з навмисними атаками, аваріями або природними загрозами. Забезпечення високого рівня безпеки і стійкості об'єктів критичної інфраструктури для України в умовах агресії рф є край актуальним питанням. **Мета досліджень** полягала в розробці методологічного підходу для кількісної оцінки рівня стійкості об'єктів критичної інфраструктури не залежно від секторів критичної інфраструктури, до якого вони належать та усіх видів проєктних загроз. **Об'єкт досліджень** – безпеки і стійкості об'єктів критичної інфраструктури. **Предмет досліджень** – методологія кількісної оцінки рівня стійкості об'єктів критичної інфраструктури.**Отримані результати.** Початкова стадія після небезпечної події це різновид прояву катастрофи «складка», визначеної у теорії катастроф. Такий підхід дозволяє визначити втрати обсягу надання послуги об'єктом критичної інфраструктури внаслідок небезпечної події, що визначають вразливість об'єкту. Стійкість об'єкта критичної інфраструктури можна визначити, як добуток часу на повне відновлення на витрати, пов'язані з відновленням обсягу послуг до вихідного рівня. Чим більше цей показник тим меньше стійкість об'єкту критичної інфраструктури. Застосування її імітаційної моделі для каскадних ефектів, дає можливість отримати ймовірнісні оцінки розвитку подій за визначеними сценаріями і дозволяє здійснити оцінювання загроз для об'єкта критичної інфраструктури за величиною імовірності настання подій і переходів між ними. На основі отриманих значень імовірності настання небезпечних подій для усіх елементів об'єкта критичної інфраструктури визначаєм найбільш вразливі і для них проводимо кількісну оцінку стійкості. Це дає змогу оцінити необхідні ресурси (фінансові, матеріальні, енергетичні, людські, транспортні тощо) для підвищення стійкості. Визначити необхідні елементи резервування для уникнення каскадних ефектів і небажених наслідків. **Висновки.** На основі теорії катастроф розроблено єдиний методологічний підхід для кількісної оцінки рівня стійкості об'єктів критичної інфраструктури не залежно від секторів критичної інфраструктури, до якого вони належать.Запропонований підхід дозволяє проводити аналіз стійкості по усіх елементах об'єкту критичної інфраструктури, проводити співставний аналіз вразливості і стійкості об'єктів сектору, оцінювати розміри небхідних додаткових інвестицій для зниження вразливості і підвищення стійкості елементів об'єкту, розробляти секторальні програми підвищення стійкості об'єктів сектору, визначити необхідні територіальні ресурси резервування та їх обсяги.

Ключові слова: об'єкт критичної інфраструктури, безпека, стійкість, теорія ккатастроф.

Вступ

Основні базові поняття у сфері безпеки критичної інфраструктури, що визначені в нормативних документах і наведені у [1], які відображають сутність поняття «безпека», можуть бути визначені як такі: безпека критичної інфраструктури, цілісність, самодостатність, стійкість, загрози критичній інфраструктурі, небезпека критичній інфраструктурі, технології попередження загрози, технології виявлення загрози, технології ліквідації загроз, технології відновлення діяльності, відшкодування завданих збитків. Зокрема стійкість об'єкта критичної інфраструктури визначена як наявність необхідних умов, елементів та системних зв'язків між ними на рівні, достатньому для стримування дії загроз та відновлення після їх дії [1].

Концепція стійкості розроблялася і застосовувалася в різноманітних напрямах діяльності (психологія, психіатрія, екологія, соціальні науки, економіка та техніка) протягом кількох десятиліть [2, 3], останнім часом вона привертає дедалі більшу увагу у сфері управління ризиками. Зокрема, спільнота критичної інфраструктури еволюціювала від першочергового акценту на захисті безпеки у 1990-х роках до більш широкого акценту на безпеці та стійкості.

У сфері національної безпеки визначати національну політику щодо зміцнення та підтримки безпечної, функціональної та стійкої критичної інфраструктури в секторах, які є важливими для національної безпеки, громадського здоров'я та безпеки, економічної життєздатності та загальної якості життя. При цьому стійкість визначається як здатність готуватися до мінливих умов та адаптуватися до них, а також витримувати збої й швидко відновлюватися після них, включно з навмисними атаками, аваріями або природними загрозами [4].

Перехід від захисту критичної інфраструктури до забезпечення її стійкості має на меті врахувати ключові зміни в ландшафті ризиків, що характеризуються зростанням невизначеності. Для того, щоб краще інтегрувати складність, взаємозалежність і взаємопов'язаність критичної інфраструктури, прийняття системного підходу до стійкості критичної інфраструктури забезпечує додаткові перспективи [5].

Підвищення стійкості національної та європейської критичної інфраструктури визначено одним із пріоритетів безпекової політики ЄС та закріплено в рішеннях Ради ЄС, спрямованих на посилення заходів із підвищення стійкості критичної інфраструктури [6]. Таким чином, забезпечення високого рівня безпеки і стійкості об'єктів критичної інфраструктури для України в умовах агресії рф є край актуальним питанням.

Аналіз літературних даних та постановка проблеми. Людство захищає критичну інфраструктуру з часів винайдення колеса, однак за останні 20 років більшість національних політик і стратегій у сфері критичної інфраструктури на Заході

еволюціонували від зосередження виключно на захисті критичної інфраструктури до підвищення її безпеки та стійкості. Цей зсув в першу чергу пов'язаний з тим, що перед зацікавленими сторонами стоїть надскладне завдання захистити усі системи критичної інфраструктури від зростаючої кількості факторів ризику, з якими вони стикаються.

Відповідно до концепції Безпеки та стійкості критичної інфраструктури (БСКІ), терміни «*безпека»* і «*стійкість»*, безумовно, підтримують ідею захисту, але вони мають специфічні значення. *Безпека* означає зменшення ймовірності успішних атак на критичну інфраструктуру або наслідків природних чи техногенних катастроф шляхом застосування фізичних засобів або оборонних заходів кібербезпеки. *Стійкість* – це здатність критичної інфраструктури протистояти, поглинати, відновлюватися або успішно адаптуватися до мінливих умов. Відмовостійка інфраструктура є надійною, гнучкою, адаптивною, здатною протистояти і швидко відновлюватися після збоїв, навмисних атак, аварій або природних загроз чи інцидентів. З огляду на зростання природних і техногенних загроз і вразливостей, з якими стикаються сучасні суспільства та які викривають обмеженість традиційної оцінки ризиків і зусиль зі зниження ризиків, концепція БСКІ видається особливо корисною для формування політики, спрямованої на пом'якшення наслідків таких подій, і вказує на життєво важливу потребу країн у розробці та впровадженні всеосяжної стратегії управління ризиками [7]. Основні елементи цього визначення – здатність готуватися до мінливих умов і адаптуватися до них, а також витримувати і швидко відновлюватися після збоїв – можна охарактеризувати чотирма структурними елементами: готовність, заходи з пом'якшення наслідків, реагування і заходи з відновлення [8].

Разом ці чотири складники можуть допомогти фахівцям розкласти концепцію стійкості на практичні кроки та, зрештою, якісно оцінити прогрес у підвищенні стійкості з плином часу. У табл. 1 описані ці складники і наведені приклади для розгляду [9].

Таблиця 1 – **Складники стійкості**

Складники	Опис	Приклади
Підготовленість	Діяльність, спрямована на передбачення відповідних загроз/небезпек і можливих наслідків від їх виникнення, включно із заходами з попередження та захисту; свідчить про адаптивність інфраструктурних систем і процес інтеграції та врахування здобутого досвіду.	Утримання сил безпеки. Установлення/моніторинг фізичного контролю доступу. Розробка планів безперервності, планів на випадок надзвичайних ситуацій і планів кібербезпеки; навчання персоналу щодо планів. Проведення регулярних навчань для перевірки планів Створення механізмів обміну інформацією.
Пом'якшення наслідків	Діяльність, спрямована на протистояння та/або поглинання негативних наслідків події, зменшення тяжкості або наслідків загрози; свідчить про надійність інфраструктури.	Модернізація підприємств для пом'якшення наслідків різних природних загроз (наприклад, протипаводкове обладнання, протипаводкові бар'єри). Модернізація обладнання, яке буде протистояти передбачуваним небезпекам. Підвищення надійності/резервування систем підтримки інфраструктури. Створення альтернативного резервного майданчика, який може продовжити роботу після інциденту й сприяти відновленню. Розуміння міжгалузевих залежностей від ключових зовнішніх ресурсів (наприклад, електроенергія, паливо, вода, зв'язок). Завбачлива підготовка додаткових запасів (наприклад, палива, резервних генераторів, резервного зв'язку).
Реагування	Заходи та програми, що здійснюються або розробляються для реагування та адаптації до негативних наслідків події; свідчить про винахідливість власників та операторів інфраструктури в управлінні кризовими ситуаціями	Підтримання можливостей реагування на місці на ключові небезпеки (наприклад, розливи хімічних речовин, пожежі, вибухові речовини, збройні напади, надзвичайні ситуації медичного характеру). Побудова відносин з місцевими службами швидкого реагування та міжсекторальними партнерами; наявність можливостей для управління позаштатними ситуаціями на місці, включно з навченим персоналом, функціональним оперативним центром і розумінням міжгалузевих проблем.
Відновлення	Діяльність і програми, спрямовані на те, щоб допомогти організаціям повернути умови роботи до прийнятного рівня та відновитися після події; свідчить про здатність швидко відновити надання послуг.	Укладання угод про першочергове відновлення з ключовими постачальниками послуг; оцінка часу й заходів, необхідних для відновлення повноцінної роботи організації після збою. Стратегії швидкої заміни/ремонту критично важливих компонентів (наприклад, сертифіковані постачальники. Підтримка запасів на випадок надзвичайних ситуацій).

З наведеної в таблиці інформації видно, що стійкість об'єктів критичної інфраструктури є інтегруючим показником, який охоплює практично усі складові функціонування об'єктів і це ускладнює його пряму кількісну оцінку.

Барамі Б. підкреслює складний і багатогранний характер стійкості критичної інфраструктури. Барамі Б. застосовує багаторівневий підхід, що ґрунтується на оцінці ризиків і враховує взаємозалежності складних інфраструктур, розглядаючи при цьому потенційні рішення, які можна застосувати протягом життєвого циклу інфраструктурної системи (тобто, проектування, будівництво та експлуатація). Таким чином, стійкість визначається не як єдиний результат або виключно здатність до відновлення після катастрофи, а скоріше як динамічний процес, який застосовує метод, заснований на ризиках і життєвому циклі, для усунення вразливостей систем критичної інфраструктури, роблячи системи більш відмовостійкими, ефективними, розумнішими і здатними краще адаптуватися до несподіваних викликів [10].

Таким чином, коли відбувається інцидент, цілі стійкості критично важливої інфраструктури можуть бути виміряні 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 інциденту, але може передбачати зміну, адаптацію до нових умов та покращення функціональності систем з плином часу.

Проведена якісна оцінка рівня стійкості об'єктів критичної інфраструктури за запропонованим підходом дійсно допомогає фахівцям розкласти концепцію стійкості на практичні кроки, але не дає кількісної оцінки цього показника, що не дозволяє проводити порівняльний аналіз стійкості об'єктів критичної інфраструктури, тим більше, якщо вони належать до різних секторів критичної інфраструктури.

На сьогодні в Україні визначено 24-и сектора критичної інфраструктури, чи мало об'єктів в яких потребують додаткових інвестицій для підвищення стійкості [11]. Саме через це державним уповноваженим органом у сфері захисту критичної інфраструктури України затверджені Методичних рекомендацій щодо розроблення та затвердження місцевих програм забезпечення безпеки та стійкості критичної інфраструктури, програм підвищення стійкості територіальних громад до кризових ситуацій, викликаних припиненням або погіршенням надання важливих для їх життєдіяльності послуг чи для здійснення життєво важливих функцій [12]. Для розробки місцевих програм забезпечення безпеки та стійкості критичної інфраструктури та програм підвищення стійкості територіальних громад до кризових ситуацій необхідно серед цих об'єктів визначити пріоритетні, а це без кількісної оцінки стійкості неможлово. Тому край нагальним є розробка методики кількісної стійкості об'єктів критичної інфраструктури та їх елементів.

Мета та задачі дослідження. Мета досліджень полягає в розробці методологічного підходу для кількісної оцінки рівня стійкості об'єктів критичної інфраструктури не залежно від секторів критичної інфраструктури, до якого вони належать та усіх видів проєктних загроз.

Для досягнення мети були поставленні наступні завдання:

– знайти підхід для не прямого кількісного оцінювання стійкості об'єктів критичної інфраструктури;

– оцінити його адекватність з позицій теорії катастроф.

Результати досліджень

Задля подолання складнощів при розгляді складових стійкості і концептуалізації їх у контексті інфраструктурних операцій з точки зору часової перспективи можна розглянути функціонування об'єкту критичної інфраструктури як залежність обсягу надання послуги в часі за різних умов, особливо при дії небезпечного фактору (природного, техногенного, терористичного, воєнного походження), як це означено на рисунку 1.

До моменту прояву небезпезпечної події об'єкт критичної інфраструктури функціонує у сталому режимі і надає послуги у проєктному обсязі. З моменту настання небезпечної події: природного катаклізму (землетрус, зсув, повень тощо), техногенних аварій, несанкціонованного втручання, кібератаки, терористичного акту, воєнного нападу, тощо обсяг надання послуги об'єктом критичної інфраструктури різко знижується, або зовсім припиняється (t_1). Після чого настає період підготовки до відновлення функціонування об'єкту (t_1) (проєктні роботи, зосередження необхідних матеріальних ресурсів, залучення підрядників тощо), що передує відновлюваним роботам, після чого розпочинається відновлення потужностей об'єкту з поступовим виходом на сталий режим надання послуги у проєктному обсязі.

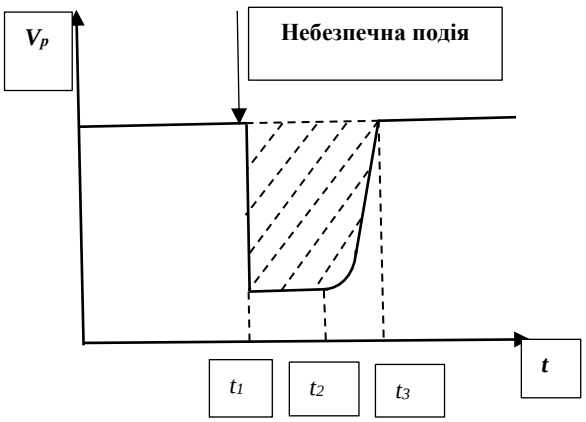

Рис. 1. Залежність обсягу надання послуги об'єктом критичної інфраструктури від часу при дії небезпечного фактору

Початкова стадія після небезпечної події це різновид прояву катастрофи у теорії катастроф [13]. *Катастрофа типу «складка»* ($x^3 + ax$) – одна з найпростіших катастроф. Стандартна деформація (падіння рівня об'єму послуг) в цьому випадку задається формулою:

$$V_p(t) = t^3/3 + a \cdot t, \quad (1)$$

де Vp – обсяг надання послуги; t – час.

Числовий коефіцієнт введено, щоб спростити подальші розрахунки. Багаторізновидність M такої катастрофи визначається рівнянням:

$$0 = \frac{d}{dt} V_p(t) = t^2 + a. \quad (2)$$

Втрати обсягу надання послуги об'єктом критичної інфраструктури внаслідок небезпечної події буде визначатися:

$$W = \int_{t_1}^{t_3} V_p(t)dt, \quad (3)$$

і характерізувати вразливість об'єкту критичної інфраструктури.

Вивчення елементарних катастроф починається з переличення основних структур, пов'язаних з катастрофами [13]. Для цього розглянемо самейство функці:

$$V: S \times C \to \boldsymbol{R}, \quad (4)$$

де S – деяка багаторізновидність $\boldsymbol{R^n}$, яка має назву простір станів; C – багаторізновидність $\boldsymbol{R^r}$, що визначається як простір управління, а число $\boldsymbol{r}$ розмірність деформації.

Багаторізновидністю катастрофи M називається підмножина в $\boldsymbol{R^n} \times \boldsymbol{R^r}$, що визначається рівнянням:

$$D \cdot V_c(t) = 0, \quad (5)$$

де $V_c(t) = V(t, c)$ – множина усіх критичних точок потенціалів V_c з сімейства V.

Відзеркаленням катастрофи S називається обмеження M натуральної проєкції:

$$\pi: \boldsymbol{R^n} \times \boldsymbol{R} \to \boldsymbol{R^r}, \quad (6)$$

$$\pi(t, C) = C. \quad (7)$$

Особливою множиною S називається підмножина в M, яка складається з особливих точок відображення χ, де ранг похідної D_χ менше ніж r. Образ особливої множини $\chi(S) \in C$ називають біфуркаційною множиною B.

Існує множина тих точок $(x, c) \in M$, в яких $V_c(x)$ має вирождену критичну точку. Значить, B являє собою місце, де змінюється кількість і природа критичних точок. У зв'язку з структурною усталенністю морсовських функцій така зміна може відбутися лише за умови переходу крізь вирождену критичну точку. У більшості застосувань найбільш важливим є саме біфуркаційна множина, так як вона лежить в просторі управління.

Рівняння (2) показує, що в якості карти для M треба взяти координату t.

Загальна точка багаторізновидності M записується у вигляді:

$$(t, a) = (t - t^2). \quad (8)$$

Розкладення в ряд Тейлора, яке відповідає цій точці на S має наступний вигляд

$$V_p(t + T) = \frac{1}{3}(t + T)^3 + (-t^2)(t + T) =$$

$$+\frac{1}{3}T^3 + tT^2 + 0T - \frac{2}{3}t^3. \quad (9)$$

Таким чином, багаторізновидність катастрофи являє собою параболу, а біфуркаційна множина складається з однієї точки.

Гладкість цієї поверхні не гарантує, що при плавній зміні однієї змінної обидві інші також змінюються плавно.

Виходячи з такого підходу стійкість об'єкта критичної інфраструктури (або його частки, підрозділу тощо) можна визначити, як добуток часу на повне відновлення на витрати, пов'язані з відновленням обсягу послуг до вихідного рівня:

$$S_i = \Delta t \cdot \sum E_i, \quad (10)$$

де Δt – час на повне відновлення об'єкту критичної інфраструктури (або його частки, підрозділу тощо); $\sum E_i$ – усі витрати на відновлення (фінансові, матеріальні, енергетичні, людські, транспортні тощо).

Чим більше цей показник тим меньше стійкість об'єкту критичної інфраструктури ($S_i \to min$).

Для зручності витрати на відновлення об'єкту критичної інфраструктури (або його частки, підрозділу тощо) можна брати не як абсолютну величину, а як частку від проєктної вартості об'єкту.

Якщо кількісна оцінка ризику реалізації небезпечних подій здійснюється на основі імітаційної моделі для оцінювання загрози виникнення каскадних ефектів для різних сценаріїв розвитку подій у зоні об'єкта критичної інфраструктури, яка передбачає виконання таких процедур:

– визначення подій в сценарії розвитку ситуації (складові елементи сценарію, що здійснюють потенційний вплив на реалізацію загрози);

– визначення множини можливих станів подій, що впливають на рівень загрози;

– формування сценаріїв розвитку загрози (визначення ланок, що складаються з пар: «подія – перехід в заданий стан»), що призводять до реалізації загрози, представлення структурно-логічної моделі розвитку кризової ситуації, що має складну структуру за різними варіантами розвитку сценарію на об'єкті критичної інфраструктури;

– формування оргграфу сценаріїв загроз (структурно-логічна модель, що включає всі сценарії реалізації загрози);

– оцінка ймовірностей станів подій та їх переходів;

– оцінювання ймовірності реалізації сценаріїв загроз.

Застосування такої імітаційної моделі для каскадних ефектів, дає можливість отримати ймовірнісні оцінки розвитку подій за визначеними сценаріями і дозволяє здійснити оцінювання загроз для об'єкта критичної інфраструктури за величиною імовірності настання подій і переходів між ними.

Приклад:

Нехай на трансформаторній підстанції стався вибух з середнім рівнем правдоподібності реалізації загрози. Тоді оцінка наслідків впливу загроз (стійкості) буде мати наступний вигляд:

– час на повне відновлення об'єкту критичної інфраструктури $\Delta t \approx 30$ днів;

– витрати на відновлення об'єкту E_i = 2 млрд грн;

– чисельність населення, яке зазнало ризику втрати – 200 осіб;

– зниження рівня надання життєво важливих функцій/послуг, тривалість зниження рівня здоров'я (фатальність) – 3 дні;

– шкода довкіллю – територія району на термін до 1 року;

– зниження рівня виробництва / надання основної послуги (продукції) (електрозабезпечення) – втрата послуги (електро- забезпечення) для понад 300 тис. абонентів; чисельність ураженого населення (вимушена міграція чи потреба прихистку/допомоги);

– вплив на 100 тис. осіб на термін до 30 днів;

– публічне сприйняття ситуації, спричинене впливом загрози – занепокоєння відчуває 5% населення [14].

Розрахунок стійкості:

$$S_i = \Delta t \cdot \sum E_i = 30 \text{ днів} \cdot 2 \cdot 10^9 \text{грн} = \\ = 6 \cdot 10^{10} (\text{днів} \cdot \text{грн}). \quad (11)$$

Це значення відображає інтегральну оцінку впливу загрози на об'єкт та масштаби витрат, необхідних для його повного відновлення.

Наявність резервної трансформаторної підстанції дозволить скоротити час на повне відновлення надання послуги об'єктом КІ до декількох хвилин, що суттєво забезпечить підвищення стійкості об'єкту (рис. 2).

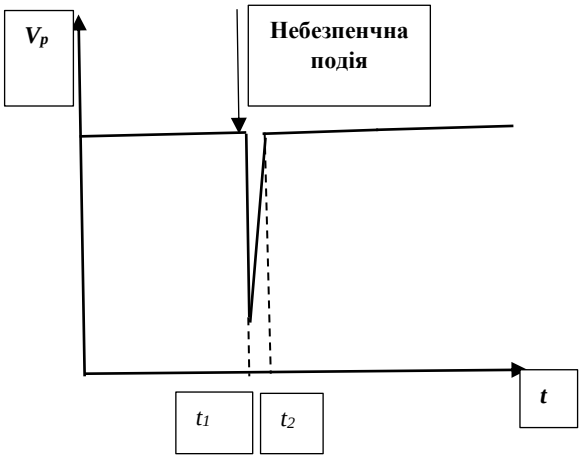

Рис. 2. Залежність обсягу надання послуги об'єктом критичної інфраструктури від часу при наявності резервного елементу об'єкту КІ

На основі отриманих значень імовірності настання небезпечних подій для усіх елементів об'єкта критичної інфраструктури визначаєм найбільш вразливі і для них проводимо кількісну оцінку стійкості. Це дає змогу оцінити необхідні ресурси (фінансові, матеріальні, енергетичні, людські, транспортні тощо) для підвищення стійкості.

Визначити необхідні елементи резервування для уникнення каскадних ефектів і небажаних наслідків.

Такий підхід для об'єкта критичної інфраструктури дозволяє:

– провести аналіз стійкості по усіх елементах об'єкту;

– визначити вразливість і стійкість кожного при реалізації будь яких загроз у кількісному вимірі;

– означити найбільш вразливі і найменш стійки елементи об'єкту;

– оцінити розмір небхідних додаткових інвестицій для зниження вразливості і підвищення стійкості елементів об'єкту;

– визначити необхідні ресурси резервування та їх обсяг.

Для секторального органу у сфері захисту критичної інфраструктури:

– проводити співставний аналіз вразливості і стійкості об'єктів сектору;

– визначити найбільш вразливі і найменьш стійки;

– розробити секторальну програму підвищення стійкості об'єктів сектору;

– визначити пріоритети інвестування для підвищення стійкості об'єктів сектору.

Для територіальних громад:

– провести аналіз стійкості по усіх об'єктах критичної інфраструктури;

– визначити найбільш вразливі і найменьш стійки на території громади;

– розробити територіальну програму підвищення стійкості об'єктів критичної інфраструктури;

– визначити необхідні територіальні ресурси резервування та їх обсяг.

Висновки

На основі теорії катастроф розроблено єдиний методологічний підхід для кількісної оцінки рівня стійкості об'єктів критичної інфраструктури не залежно від секторів критичної інфраструктури, до якого вони належать.

Запропонований підхід дозволяє:

проводити аналіз стійкості по усіх елементах об'єкту критичної інфраструктури,

проводити співставний аналіз вразливості і стійкості об'єктів сектору,

оцінювати розміри небхідних додаткових інвестицій для зниження вразливості і підвищення стійкості елементів об’єкту,

розробляти секторальні програми підвищення стійкості об’єктів сектору та визначити необхідні територіальні ресурси резервування та їх обсяги.

СПИСОК ЛІТЕРАТУРИ

1. 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. Випуск 3 (13). С. 142-148.
2. Реншлер, Кріс С., Емі Е. Фрейзер, Люсі А. Арендт, Джан-Паоло Чімелларо, Андрій М. Рейнхорн та Мішель Брюно, «Структура для визначення та вимірювання стійкості на рівні громади: концепція стійкості людей», Національний інститут стандартів і технологій. 2010 р. 73 р. Дата перегляду 13 лютого 2020 р. www.hsdl.org/?view&did=790013.
3. Rose, A., 2009, Economic Resilience to Disasters, CARRI Research Report 8. Available at http://www.resilientus.org/library/Research_Report_8_Rose_1258138606.pdf, accessed on November 2, 2010.
4. АПКБІ, «Національний план захисту інфраструктури (НПЗІ) 2013: партнерство заради безпеки та стійкості критичної інфраструктури». 2013 р. Дата перегляду: 13 лютого 2020 року. www.cisa.gov/national-infrastructure-protection-plan
5. OECD (2019), Належне врядування для забезпечення стійкості критичної інфраструктури, Огляди політики управління ризиками OECD, Публікація OECD, Париж. https://doi.org/10.1787/02f0e5a0-en.
6. Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure. Brussels, 9 December 2022 (OR. en) 15623/22. URL: https://data.consilium.europa.eu/doc/document/ST-15623-2022-INIT/en/pdf
7. Сприянняколективнійобороні НАТО: Безпекатастійкість критичної інфраструктури. Посібник НАТОCOE-DAT/ К. Андерсон, М. Бейкер, Р. Бірс та ін. 2022. 469 р.
8. Methodology for assessing regional infrastructure resilience (CISA). May 2021. Version 1.0.
9. Карлсон, Дж. Лон, Ребекка А. Хаффенден, Гілберт В. Бассет, Вільям А. Берінг, Майкл Д. Коллінз, III, Стівен М. Фолга, Фредерік Петі, Джулія А. Філліпс, Дуейн Р. Вернер і Рональд Вітфілд, «Стійкість: Теорія та застосування». 2012 р. США. doi:10.2172/1044521. www.osti.gov/biblio/1044521-resilience-theory-application.
10. Барамі Б. Відмовостійкість інфраструктури: структура на основі ризиків Департамент США Транспорт, https://www.volpe.dot.gov/sites/volpe.dot.gov/files/docs/Infrastructure%20Resiliency_A%20 Risk-Based%20Framework.pdf (дата доступу: 25 лютого 2019 р.).
11. Деякі питання об’єктів критичної інфраструктури. Постанова КМ України від 09.10.2020 р. № 1109 (зі змінами) https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text.
12. Про затвердження Методичних рекомендацій щодо розроблення та затвердження місцевих програм забезпечення безпеки та стійкості критичної інфраструктури, програм підвищення стійкості територіальних громад до кризових ситуацій, викликаних припиненням або погіршенням надання важливих для їх життєдіяльності послуг чи для здійснення життєво важливих функцій. Наказ Адміністрації Держспецзв’язку України видала наказ від 30.11.2023 № 997. https://www.cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczvyazku-vid-30-listopada-2023-roku-997.
13. Thompson, J. Michael T. Instabilities and Catastrophes in Science and Engineering. New York: Wiley, 1982. 256 p.
14. Суходоля О. М. Стійкість критичної енергетичної інфраструктури та життєдіяльності громад. Нац. ін-т стратег. дослідж., 2024. – с.160. URL: https://doi.org/10.53679/niss-analytrep.2024.04

Received (Надійшла) 11.12.2024
Accepted for publication (Прийнята до друку) 26.02.2025

Approach to quantitative assessment of the resilience of critical infrastructure facilities

O. Tretyakov, B. Khalmuradov, N. Kichata, A. Remska

Abstract. The resilience of critical infrastructure facilities is defined as the ability to prepare for and adapt to changing conditions, as well as to withstand and recover quickly from failures, including deliberate attacks, accidents or natural threats. Ensuring a high level of security and resilience of critical infrastructure facilities for Ukraine in the face of russian aggression is an extremely urgent issue. **The purpose of the research** was to develop a methodological approach for quantifying the level of resilience of critical infrastructure facilities, regardless of the critical infrastructure sectors to which they belong and all types of project threats. **The object of research** is the safety and resilience of critical infrastructure facilities. **The subject of research** is the methodology for quantifying the level of resilience of critical infrastructure facilities. **Results obtained.** The initial stage after a dangerous event is a type of manifestation of the "fold" catastrophe defined in the theory of catastrophes. This approach allows you to determine the losses in the volume of service provision by a critical infrastructure facility as a result of a dangerous event, which determine the vulnerability of the object. The higher this indicator, the lower the stability of the critical infrastructure facility. The use of the simulation model for cascading effects makes it possible to obtain probabilistic estimates of the development of events according to certain scenarios and allows to assess threats to a critical infrastructure facility by the probability of occurrence of events and transitions between them. Based on the obtained values of the probability of occurrence of dangerous events for all elements of the critical infrastructure facility We identify the most vulnerable and quantify resilience for them. This makes it possible to assess the necessary resources (financial, material, energy, human, transport, etc.) to increase resilience. Determine the necessary redundancy elements to avoid cascading effects and unintended consequences. **Conclusions.** On the basis of the theory of disasters, a single methodological approach has been developed for quantifying the level of resilience of critical infrastructure facilities, regardless of the critical infrastructure sectors to which they belong.The proposed approach allows to conduct a stability analysis for all elements of a critical infrastructure facility, to conduct a comparative analysis of vulnerability and resilience of sector facilities, to assess the amount of additional investments needed to reduce vulnerability and increase the resilience of facility elements, to develop sectoral programs to increase the resilience of sector facilities, to determine the necessary territorial resources of reservation and their volumes.

Keywords: critical infrastructure facility, safety, resilience, theory of disasters.