Євген МОРЩ,
доктор технічних наук, завідувач відділу науково-технічної експертизи, Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації, Київ, Україна
ORCID: https://orcid.org/0000-0003-0131-2332
e-mail: yevhen.phd@gmail.com,

Павло ПОЗДНЯКОВ,
кандидат технічних наук, старший дослідник, начальник інституту, Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації, Київ, Україна
ORCID: https://orcid.org/0000-0003-4188-9486
e-mail: pozdner86@gmail.com,

Валерій ПОПЕЛЬ,
доктор філософії, провідний науковий співробітник відділу науково-технічної експертизи, Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації, Київ, Україна
ORCID: https://orcid.org/0000-0001-5544-3544
e-mail: v.popel@cip.gov.ua,

DOI: https://doi.org/10.32620/pls.2025.67.19

ЗАСТОСУВАННЯ ПІДХОДУ ЕКОНОМІЧНОГО БАЛАНСУ ПРИ ВИМІРЮВАННІ ТА УПРАВЛІННІ РИЗИКАМИ В СИСТЕМІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація: *В тезах доповіді аналізуються складові системи захисту критичної інфраструктури, визначається пріоритетність ризик-орієнтованого підходу до оцінки та вимірювання ризиків критичної інфраструктури, проводиться розгляд і аналіз методів оцінки ризиків, що застосовуються в практиці країн Європейського Союзу, та обґрунтовується доцільність застосування економічного підходу до процесів вимірювання ризиків з метою подальшого використання отриманих результатів для побудови системи захисту критичної інфраструктури, як важливої складової сучасного управління захистом об'єктів критичної інфраструктури держави. Наводяться приклади застосування економічних вимірювань при плануванні захисту критичної інфраструктури у країнах ЄС, перелічуються відомі методики оцінки ризиків, які дозволяють перейти до економічного вимірювання. Вказується на необхідність застосування підходу економічного балансу та моделювання сталого розвитку об'єктів критичної інфраструктури.*

Ключові слова: *критична інфраструктура, оцінка ризиків, національна безпека, економічний підхід.*

Відповідно до [1, 2] сукупність органів управління, сил та засобів центральних і місцевих органів виконавчої влади (військово-цивільних адміністрацій - у разі утворення), органів місцевого самоврядування, операторів критичної інфраструктури, на які покладається формування та/або реалізація державної політики у сфері захисту критичної інфраструктури, є національною системою захисту критичної інфраструктури.

Одночасно, під системою захисту критичної інфраструктури розуміється сукупність організаційних, технічних, програмних, інженерних та інших заходів, засобів і рішень, спрямованих на забезпечення стійкості, безпеки та безперервності функціонування критичної інфраструктури, тобто об'єктів і систем, від яких залежить національна безпека, здоров'я населення, економіка та суспільне життя.

В системі захисту критичної інфраструктури можливо визначити такі основні компоненти (складові):

нормативно-правова база, яка включає закони, підзаконні акти, стандарти;

інституційний рівень, до якого входять уповноважений орган, секторальні та функціональні органи управління, об'єкти критичної інфраструктури, оператори інфраструктури;

комплекс організаційних заходів, які включають ідентифікацію об'єктів критичної інфраструктури, створення і ведення їх реєстру, оцінка ризиків критичної інфраструктури,

розробка планів захисту, планів реагування на надзвичайні ситуації, навчання персоналу;

комплекс технічних заходів, в тому числі фізичний захист, кіберзахист, інженерно-технічні рішення;

процеси управління, до яких належать моніторинг загроз, інцидент-менеджмент, взаємодія з державними органами, аналіз ефективності заходів.

Таким чином, система захисту критичної інфраструктури є управлінською системою, що об'єднує людей, процеси та засоби для запобігання загрозам, мінімізації шкоди та відновлення роботи після інцидентів.

Під час дії воєнного стану, а також протягом 12 місяців після його припинення чи скасування повноваження уповноваженого органу у сфері захисту критичної інфраструктури України здійснюються Державною службою спеціального зв'язку та захисту інформації України [2, 23]. Одним з повноважень вказаного уповноваженого органу є підготовка щорічної оцінки ризиків і загроз критичній інфраструктурі національного рівня [1, 8].

З метою забезпечення якісної оцінки ризиків і загроз критичній інфраструктурі існує необхідність застосування підходу економічного балансу та моделювання сталого розвитку об'єктів критичної інфраструктури.

Економічний підхід до побудови системи захисту критичної інфраструктури є важливою складовою сучасного управління ризиками. Він дозволяє ухвалювати зважені рішення, коли кожна інвестиція в захист обґрунтована конкретним показником зниженням ризику й запобіганням економічним втратам.

Принципова перевага економічного підходу полягає у прозорості та аргументованості рішень. Оператор або держава можуть обґрунтувати, чому певний захід впроваджується або, навпаки, чому деякі ризики залишаються прийнятними. Це також дає змогу впроваджувати страхування ризиків там, де зниження ризику технічними або організаційними засобами є занадто дорогим.

Ще одним важливим моментом є можливість пріоритизації заходів. Необхідно розуміти, які загрози є найбільш критичними, а які несуть меншу небезпеку, і розподіляти бюджет відповідно.

Наприклад, у багатьох країнах ЄС широко використовується підхід cost-benefit analysis (CBA) та cost-effectiveness analysis (CEA) при плануванні захисту критичної інфраструктури. Європейська комісія, зокрема, у своїй Стратегії захисту критичної інфраструктури (EU CIIP Strategy) [3], підкреслює важливість інтеграції оцінки витрат і вигоди у процес ухвалення рішень.

Наступним прикладом є методологія, що застосовується у Великій Британії в рамках National Infrastructure Protection Plan (NIPP), де одним з основних підходів є оцінка ризиків з їх подальшим монетарним виміром для формування державних інвестиційних програм.

Крім того, багато європейських операторів критичної інфраструктури використовують моделі Total Cost of Ownership (TCO) для розрахунку повних витрат на заходи безпеки протягом життєвого циклу активів, які дають змогу включати в оцінку не лише первісні витрати, але й витрати на обслуговування, модернізацію, навчання персоналу тощо.

Таким чином, економічний підхід дає можливість раціонального розподілу ресурсів, обґрунтування бюджетів, створює прозорість перед державними органами, суб'єктами економіки та населенням.

Визначення й вимірювання ризиків на об'єктах критичної інфраструктури є основою ефективної роботи всієї системи захисту. Без якісної оцінки ризиків захист перетворюється на хаотичний набір заходів, часто заснованих на інтуїції, минулому досвіді або політичному тиску, а не на реальній картині загроз.

Вимірювання ризиків в грошовому еквіваленті відкриває шлях до аргументованого визначення пріоритетів, економічного обґрунтування витрат на безпеку, створює можливість порівняння ефективності альтернативних заходів, побудови партнерських відносин між державою і бізнесом.

Серед визнаних методик оцінки ризиків, які дозволяють перейти до економічного вимірювання, можна виділити:

ISO 31000 / ISO 27005 – міжнародні стандарти, що задають принципи побудови системи управління ризиками, вони включають визначення контексту, ідентифікацію ризиків, оцінку й обробку, але не прив'язують користувача до жорстких формул, дозволяючи адаптувати під конкретну сферу [4];

NIST SP 800-30 – орієнтована на IT-системи методологія оцінки ризиків, що передбачає використання кількісних і якісних параметрів, включаючи очікувані економічні наслідки [5];

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) – методика, яка широко застосовується для оцінки IT-ризиків у критичній інфраструктурі, включає етапи визначення активів, загроз, вразливостей й аналізу можливих збитків [6];

FAIR (Factor Analysis of Information Risk) – методика, яка спеціально фокусується на економічному вимірюванні IT-ризиків, включаючи ймовірність подій, частоту, середній збиток, варіанти сценаріїв, що ідеально підходить для побудови фінансових моделей ризиків [7];

EU Risk Assessment and Mapping Guidelines for Disaster Management – рекомендації Європейської Комісії, що пояснюють, як оцінювати природні й техногенні ризики в масштабах національної критичної інфраструктури, з урахуванням економічних наслідків [8].

Отже, економічне вимірювання ризиків є основою, яка дає змогу перевести захист критичної інфраструктури на рівень реального управління, де кожне рішення має економічне обґрунтування, а система стає прозорою, гнучкою й підзвітною.

Бібліографічні посилання

1. Закон України «Про критичну інфраструктуру», від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 09.05.25).

2. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України», від 23.02.2006 № 3475-IV. URL: https: //zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 09.05.25).

3. Green Paper on a European programme for critical infrastructure protection. Brussels, 17.11.2005. URL: https://eur-lex.europa.eu/legal-content/EN/ TXT/?uri=CELEX%3A52005DC0576 (дата звернення: 09.05.25)

4. Міжнародний стандарт ISO 31000. URL: https://www.iso.org/iso-31000-risk-management.html (дата звернення: 09.05.25)

5. Guide for Conducting Risk Assessments. NIST SP 800-30 Rev. 1. September 2012. URL: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final (дата звернення: 09.05.25).

6. Operationally Critical Threat, Asset, and Vulnerability Evaluation SM (OCTAVESM). URL: https://insights.sei.cmu.edu/documents/1210/1999_005_001 _16769.pdf (дата звернення: 09.05.25).

7. What Is The FAIR Institute? URL: https://www.wallarm.com/what/what-is-factor-analysis-of-information-risk-fair (дата звернення: 09.05.25).

8. Risk Assessment and Mapping Guidelines for Disaster Management. Commission staff working paper. URL: https://ec.europa.eu/echo/files/about/COMM_PDF_SEC_2010_1626_F_staff_working_document_en.pdf (дата звернення: 09.05.25).

E. Morsh, P.Pozdnjakov, V.Popel

Application of the economic balance approach in risk measurement and management within the critical infrastructure protection system.

Abstract: The conference paper abstracts analyze the components of critical infrastructure protection systems, emphasize the priority of a risk-based approach to the assessment and measurement of critical infrastructure risks, and review and analyze risk assessment methodologies applied in the practice of European Union member states. The paper substantiates the relevance of employing an economic approach to risk measurement processes, with the aim of further utilizing the results to design a critical infrastructure protection system as an essential element of modern critical infrastructure management at the national level. Examples are provided of the application of economic measurement in critical infrastructure protection planning in EU countries, along with a list of well-known risk assessment methodologies that facilitate the transition to economic measurement. The paper highlights the necessity of applying the concept of economic balance and modeling for the sustainable development of critical infrastructure assets.

Keywords: critical infrastructure, risk assessment, national security, economic approach.

Зразок для цитування:

Морщ Є., Поздняков П., Попель В. Застосування підходу економічного балансу при вимірюванні та управлінні ризиками в системі захисту критичної інфраструктури. Пропілеї права та безпеки, 2025. №6-7. С. 74-76. DOI: https://doi.org/10.32620/pls.2025.67.19.