НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА



НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ «КІБЕРБЕЗПЕКА ЕНЕРГЕТИКИ»

Матеріали

28 травня 2025 року

Київ – 2025

УДК [621.3+620.9]::[004[056.53+42+94] + 504.06]
ББК 31
Б-39

Рекомендовано до друку Вченою радою Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України

Б-39 **Кібербезпека енергетики,** науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : матеріали, 28 травня 2025 р. Київ : ІПМЕ ім. Г.Є.Пухова НАН України, 2025. 90 с.

В-39 **Cybersecurity of energy**, scientific-practical conference of the G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine : materials, May 28, 2025. Kyiv: PIMEE NAS of Ukraine, 2025. 90 p.

© Автори публікацій, 2025
© ІПМЕ ім. Г.Є. Пухова НАН України, 2025

В.М. Буняк, В.В. Лукічов

АНАЛІЗ ТЕОРЕТИЧНИХ ВЛАСТИВОСТЕЙ КРИТЕРІЮ ЕФЕКТИВНОСТІ КОНТРЗАХОДІВ В ЕНЕРГОМЕРЕЖАХ

Метою цієї роботи є докладне теоретичне дослідження критерію ефективності контрзаходів η_i, який визначається як відношення абсолютного зниження агрегованого ризику до нормалізованих ресурсних витрат. У межах аналізу сформульовано основні компоненти моделі, встановлено ключові аналітичні властивості функції η_i, а також обґрунтовано необхідність її мультикритеріального розширення ξ_i для гнучкого балансування між абсолютним і відносним зниженням ризику. Особлива увага приділена перевірці поведінки метрики в граничних сценаріях, властивості монотонності та інваріантності до масштабування одиниць виміру.

Для побудови моделі спочатку вводиться поняття агрегованого ризику до застосування контрзаходу, що позначається R_{before} і обчислюється як сума внесків усіх компонентів енергомережі з урахуванням ймовірності настання загрози P і потенційного збитку I для кожного вузла. Після врахування впливу заходу оновлений системний ризик R_{after} визначається за тими ж алгоритмічними кроками, але з модифікованими параметрами P та/або I у відповідних компонентах. Різниця між цими величинами,

$$\Delta R = R_{before} - R_{before}, \tag{1}$$

є показником абсолютного зниження ризику, яке забезпечується конкретним контрзаходом [1].

Паралельно із обчисленням ΔR для кожного заходу визначається його нормалізована вартість C_{norm}. Цей показник формується шляхом ділення фактичних ресурсних витрат на впровадження заходу на максимальну вартість серед усіх доступних опцій. Такий підхід дозволяє привести різнорідні показники витрат — фінансові, трудові, часові — до єдиної безрозмірної шкали, що забезпечує коректне порівняння ефективності заходів незалежно від їхніх початкових одиниць виміру [3]. Безпосередньо критерій η_i формується як відношення абсолютного зниження ризику до нормалізованої вартості заходу:

$$\eta_i = \frac{\Delta R}{C_{norm}}, \tag{2}$$

Це дозволяє оцінити «віддачу на одиницю витрат» для кожного контрзаходу й ранжувати заходи за спаданням цього показника. За значенням η_i вибирають ті заходи, які забезпечують найбільший зниження ризику за найменших ресурсних витрат, що є критичною вимогою за жорстких бюджетних обмежень [1].

Методика ранжування передбачає, що всі контрзаходи впорядковуються за спаданням значень η_i. Такий підхід гарантує оптимальне розподілення ресурсів між заходами: спочатку впроваджуються ті контрзаходи, які забезпечують максимальний приріст безпеки на кожну одиницю витрат, а вже потім — менш ефективні.

Водночас пряме відношення ΔR до C_{norm} не завжди враховує синергетичні ефекти від одночасного застосування декількох заходів. Для вирішення цієї проблеми вводиться мультикритеріальний показник ξ_i, який формується як лінійна комбінація відносного зниження ризику (ΔR до R_{before}) та абсолютного зниження ΔR з ваговими коефіцієнтами w_2 і w_2 [4]:

$$\xi_i = w_1 \cdot \left(\frac{\Delta R}{C_{norm}}\right) + w_2 \cdot \left(\frac{\Delta R}{R_{before}}\right) \tag{3}$$

Цей багатовимірний підхід дозволяє налаштовувати пріоритети залежно від стратегічних чи бюджетних вимог: можна посилити роль абсолютного виграшу в ризику або приділити більше уваги відносному зниженню [2].

Аналіз математичних властивостей критерію показав, що η_i є монотонною функцією від вхідних параметрів. Збільшення ймовірності загрози P або потенційного впливу I завжди призводить до зростання абсолютного зниження ΔR, а отже — до збільшення значення η_i. Це забезпечує логічне ранжування: найбільш критичні сценарії отримують вищий пріоритет у захисній стратегії [1].

Критерій також демонструє однорідність нульового порядку, тобто інваріантний до масштабних перетворень одиниць виміру витрат чи ризику. Якщо витрати виражаються в різних умовних одиницях — тисячах чи мільйонах гривень, днях або енергетичних одиницях — відношення ΔR до C_{norm} залишається незмінним, оскільки обидві складові масштабуються пропорційно. Це спрощує практичне застосування метрики у різних проєктах без необхідності адаптації формул.

Граничний аналіз поведінки η_i у крайових сценаріях доводить її коректність та внутрішню узгодженість. При $P \to 0$ або $I \to 0$ абсолютне зниження $\Delta R \to 0$, отже $\eta_i \to 0$, що відображає відсутність користі від контрзаходів за відсутності реальної загрози чи збитку. Натомість коли $P = 1$ та $I = 1$, абсолютне зниження ризику досягає максимальної величини, а η_i наближається до свого верхнього граничного значення, що гарантує правильне оцінювання «віддачі» навіть у надзвичайно критичних умовах.

Нерідко трапляються випадки, коли кілька контрзаходів застосовуються одночасно, і їхній комбінований ефект виявляється неадитивним: сумарне ΔR комбінації може бути більше або менше суми індивідуальних ΔR через перетинні чи синергетичні ефекти. Саме з метою врахування таких нелінійних взаємодій і було

розроблено мультикритеріальний показник ξ_i, який здатен коригувати приоритезацію заходів залежно від їхньої спільної дії та визначати оптимальні комбінації.

Практична реалізація критеріїв η_i і ξ_i передбачає їхню інтеграцію в моделі оптимізації кібер-фізичного захисту систем ICS/SCADA. Обидві метрики можуть бути безпосередньо включені в цільову функцію, поряд з технічними, економічними й часовими обмеженнями, що дозволяє одночасно мінімізувати системний ризик та оптимізувати розподіл ресурсів у складних мережевих середовищах із великою кількістю вузлів і потенційних загроз [1].

Критерії також можуть застосовуватися в режимі реального часу з використанням телеметрії SCADA-IDS. Потокові дані про події та зміну параметрів дозволяють оперативно коригувати значення P і I для кожного елемента мережі, перераховувати η_i та ξ_i та перегруповувати пріоритети контрзаходів у відповідь на динамічні зміни в кібер-фізичному середовищі. Це відкриває можливості для створення автоматизованих систем моніторингу та адаптивного управління безпекою [1].

Висновки. У результаті проведеного аналізу встановлено, що критерій η_i є міцно обґрунтованим інструментом для кількісного ранжування контрзаходів у енергомережах, забезпечуючи прозоре й інтуїтивно зрозуміле порівняння «віддачі на одиницю витрат». Мультикритеріальне розширення ξ_i додає необхідну гнучкість для стратегічного балансування між абсолютним і відносним зниженням ризику, що є ключовим для формування оптимального портфеля заходів.

Перспективи подальших досліджень включають валідацію описаних властивостей на цифрових двійниках та реальних сценаріях інтелектуальних енергомереж, розробку програмних модулів автоматизації розрахунку η_i і ξ_i для інтеграції в платформи SCADA-IDS, адаптацію алгоритмів до онлайн-режиму з урахуванням економічних показників CAPEX/OPEX та метрик стійкості типу MTTR/MTTF, а також дослідження синергетичних ефектів комбінованих заходів для підвищення резильєнтності енергосистем [5].

1. Kavallieratos G., Sppathoulas G., Katsikas S. Cyber Risk Propagation and Optimal Selection of Cybersecurity Controls for Complex Cyberphysical Systems // Sensors. — 2021. — Т. 21, № 5. — Арт. 1691. — DOI: 10.3390/s21051691.
2. Ahmad A., Hadwan M. H. M. Multi-criteria decision-making approaches for cybersecurity control selection in smart grids // Int. J. Crit. Infra. Prot. — 2020. — Т. 28. — С. 100–115. — DOI: 10.1016/j.ijcip.2020.100415.
3. Lahaye S., Borgianni Y., Guerriero F. Bayesian risk assessment framework for cyber-physical energy systems // Energies. — 2020. — Т. 13, № 18. — Арт. 4700. — DOI: 10.3390/en13184700.
4. Mousavi S., Sarreshtedari H. G. A fuzzy MCDM approach to cybersecurity control selection in power utility networks // Electr. Power Syst. Res. — 2019. — Т. 170. — С. 171–183. — DOI: 10.1016/j.epsr.2019.01.006.
5. Hosseini S., Barker K., Ramirez-Marquez J. E. A review of definitions and measures of system resilience // Reliab. Eng. Syst. Saf. — 2016. — Т. 145. — С. 47–61. — DOI: 10.1016/j.ress.2015.08.006.