https://orcid.org/0000-0001-5568-7629
https://orcid.org/0000-0002-2552-2839
https://orcid.org/0000-0002-5627-4444

УДК 004.056:005.52:621.311

В.А. ЛИТВИНОВ*, С.В. ГРИБКОВ, К.Ю. ЧОРНОБАЙ****

ПІДХІД ДО СЦЕНАРНО-ОРІЄНТОВАНОГО ОЦІНЮВАННЯ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЕЛЕКТРОЕНЕРГЕТИЧНОГО СЕКТОРУ УКРАЇНИ

*Інститут проблем математичних машин і систем Національної академії наук України, м. Київ
**Національний університет харчових технологій, м. Київ, Україна

Анотація. *Захист енергетичної інфраструктури від кіберфізичних загроз є актуальною проблемою в усьому світі, особливо в умовах воєнного стану в Україні. Наразі в Україні застосовується Методика оцінювання стану та практик кібербезпеки критичної інфраструктури електричних мереж, що ґрунтується на моделі оцінювання зрілості спроможностей у сфері кібербезпеки C2M2. У моделі оцінюються загальні процеси забезпечення кібербезпеки, але не конкретні сценарії загроз. Пропонується і розглядається підхід до можливого розширення застосування моделі C2M2 у напрямі об'єднання оцінки організаційної зрілості об'єкта захисту і сценарного аналізу загроз. Підхід полягає в інтеграції моделей C2M2, MADS/MOSAR і GE/McKinsey Matrix. Інтеграція моделей розглядається як двоетапний процес. На першому етапі для грубого сценарного аналізу застосовується дещо узагальнена матриця Мак-Кінзі зі сценарно-залежними ваговими коефіцієнтами, для якої вісь «зовнішніх» загроз формується експертним шляхом, а для осі «внутрішньої» здатності протистояти загрозам безпосереднім вимірювачем є MIL-значення доменів C2M2. Таке рішення спирається на дані, що вже збираються в C2M2, забезпечує швидкий результат з приоритезації сценаріїв та закладає архітектуру, до якої на наступному етапі може бути інтегровано MOSAR. Самостійна автономна корисність матриці визначається можливістю, в разі критичної необхідності, швидко розподілити захисні ресурси. На другому етапі підключається MOSAR як інструмент поглибленого трудомісткого аналізу для сценаріїв із зони найвищих пріоритетів матриці з можливим подальшим інтегруванням засобів стандарту NIST SP 800-53, що надасть ресурсомістку детальну технічну конкретику. Обґрунтовуються і розглядаються типові процеси першого і другого етапів, недоліки і обмеження підходу, засоби можливої компенсації недоліків. Для практичної реалізації першого етапу необхідно виконання відповідного пілотного проєкту для декількох критичних об'єктів, при позитивному результаті якого здійснюється перехід до другого етапу.*

Ключові слова: *захист енергетичної інфраструктури, сценарно-орієнтоване оцінювання кібербезпеки, C2M2, MADS/MOSAR, GE/McKinsey Matrix.*

Abstract. *Protecting energy infrastructure from cyber-physical threats is a pressing issue worldwide, especially given the current state of martial law in Ukraine. Currently, Ukraine employs the Methodology for Assessing the State and Practices of Cybersecurity in Critical Electrical Grid Infrastructure, which is based on the C2M2 cybersecurity capability maturity assessment model. This model evaluates general cybersecurity processes but does not address specific threat scenarios. An approach to potentially expanding the application of the C2M2 model by combining the assessment of an organization's maturity with scenario-based threat analysis is proposed and examined. The approach involves integrating the C2M2, MADS/MOSAR, and GE/McKinsey Matrix models. Their integration is viewed as a two-stage process. At the first stage, a slightly generalized McKinsey matrix with scenario-dependent weighting coefficients is used for a rough scenario analysis. For this matrix, the «external» threats axis is determined through expert assessment,*

ISSN 1028-9763. Математичні машини і системи. 2026. № 3

while for the «internal» axis of the ability to counter threats, the MIL values of the C2M2 domains serve as the direct metric. This approach relies on data already collected in C2M2, provides rapid results for scenario prioritization, and establishes an architecture into which MOSAR can be integrated at the next stage. The standalone utility of the matrix lies in its ability to rapidly allocate defense resources in cases of critical need. At the second stage, MOSAR is integrated as a tool for in-depth, labor-intensive analysis of scenarios from the highest-priority zone of the matrix, with the possible subsequent integration of NIST SP 800-53 standards, which will provide resource-intensive and detailed technical specifications. The typical processes of the first and second stages, the shortcomings and limitations of the approach, and ways to potentially compensate for these shortcomings are justified and examined. For the practical implementation of the first stage, a corresponding pilot project should be carried out for several critical facilities; if the results are positive, the second stage can be initiated.
Keywords: *energy infrastructure protection, scenario-based cybersecurity assessment, C2M2, MADS/MOSAR, GE/McKinsey Matrix.*

DOI: 10.34121/1028-9763-2026-3-21-30

1. Вступ

Енергетична інфраструктура є одним із ключових елементів функціонування держави, оскільки забезпечує безперервну роботу економіки, систем державного управління, сектору безпеки й оборони та соціальної сфери. Порушення її функціонування здатне спричиняти масштабні каскадні наслідки, які поширюються на інші сектори критичної інфраструктури, зокрема транспорт, зв'язок, водопостачання та охорону здоров'я. У наслідок високого рівня взаємозалежності таких систем навіть локальні інциденти можуть трансформуватися у комплексні кризові ситуації загальнодержавного масштабу. Сучасні загрози енергетичному сектору дедалі частіше набувають гібридного характеру та поєднують кібернетичні, фізичні, інформаційні та організаційні компоненти впливу. Особливу небезпеку становлять кіберфізичні атаки, спрямовані на системи управління технологічними процесами, диспетчерські центри та інші критичні елементи енергетичної інфраструктури. Тому захист енергетичної інфраструктури від кіберфізичних загроз є надзвичайно актуальною проблемою в усьому світі, особливо в умовах воєнного стану в Україні [1–4].

Наразі в Україні офіційно застосовується Методика оцінювання стану та практик кібербезпеки критичної інфраструктури електричних мереж [5], затверджена наказом Міністерства енергетики України № 285 від 05.08.2024 та введена в дію 20.09.2024. Зазначена Методика ґрунтується на адаптованій до українських умов моделі оцінювання зрілості спроможностей у сфері кібербезпеки Cybersecurity Capability Maturity Model (C2M2) та тісно узгоджується з міжнародними рамковими підходами до управління кібербезпекою, зокрема з NIST Cybersecurity Framework [6, 7]. При цьому модель C2M2, розроблена Міністерством енергетики США (DOE), пристосована до операційних технологій саме енергетики — до систем SCADA (Supervisory Control and Data Acquisition), промислових систем управління (ICS) тощо. Методика вбудована в більш широку вітчизняну екосистему засобів і нормативних вимог кіберзахисту — платформу обміну загрозами MISP, обов'язкові вимоги до кібербезпеки ТЕК (наказ Міненерго № 403 від 07.10.2025), рамочні вимоги Держспецзв'язку тощо. Впровадження Методики стало важливим етапом формування системного підходу до оцінювання кіберзагроз і розвитку механізмів забезпечення кіберстійкості об'єктів критичної інфраструктури енергетичного сектору України.

Разом із тим зазначена Методика, будучи одним із перших інструментів практичного впровадження міжнародних підходів до оцінювання кібербезпеки об'єктів критичної інфраструктури в Україні, успадковує низку концептуальних обмежень, пов'язаних із призначенням моделі C2M2. Зокрема, в моделі оцінюються процеси, загальні можливості та засоби забезпечення кібербезпеки, але не конкретні сценарії загроз. Тому Методика орієнтована насамперед на оцінювання організаційних процесів, рівня розвитку практик кібербезпеки та наявних спроможностей суб'єкта захисту.

Мета статті полягає в розгляді запропонованого підходу до можливого розширення застосування моделі C2M2 в напрямі об’єднання оцінки організаційної зрілості об’єкта захисту і сценарного аналізу ризиків.

2. Гібридна схема інтеграції моделей C2M2 — MADS/MOSAR

MOSAR (Method Organized and Systemic Analysis of Risk) є загальною системною методологією аналізу ризиків, розробленою у Франції на базі моделі MADS (Model Analysis of Dysfunctions of the Systems). Методологія пропонує дворівневий системний аналіз [8, 9]:

макроскопічний рівень — декомпозиція системи, ідентифікація джерел загроз, побудова сценаріїв розвитку небажаних подій, оцінка ризиків (кількісна або якісна) за матрицею «Важливість — імовірність»;

мікроскопічний рівень — детальний аналіз окремих ризиків на основі побудови логічних дерев подій і відмов, а також розроблення пропозицій щодо захисних бар’єрів безпеки — технічних та операційних заходів із запобігання/захисту. Методологія застосовується для будь-яких ризиків (фізичних, кібер, організаційних).

Ключовим принципом можливої інтеграції моделей є використання MOSAR для ідентифікації та аналізу кіберфізичних загроз, сценаріїв аварій і захисних бар’єрів, а C2M2 — для оцінки та підвищення зрілості процесів кібербезпеки, які потенційно запобігають цим атакам. Поєднання зазначених моделей формує гібридний підхід до забезпечення безпеки критичної інфраструктури, який поєднує оперативність стандартизованого оцінювання з можливістю глибокого сценарного аналізу складних багатовекторних загроз. Комбінація моделей створює підхід, який відповідає вимогам воєнного часу: швидка обов'язкова оцінка + глибоке моделювання реальних критичних загроз. Інтегрований гібридний цикл оцінювання та управління ризиками містить таку послідовність взаємопов’язаних процесів, спрямованих на виявлення загроз, аналіз вразливостей, оцінювання рівня зрілості захисних механізмів та формування превентивних заходів.

Процес 1. Загальна регулярна обов’язкова самооцінка (C2M2).

Оцінюється поточний стан кіберстійкості — індекси рівнів зрілості MIL (Maturity Indicator Levels), план загальних заходів щодо їх підвищення. Опціонально (при наявності відповідних ресурсів) — періодичний аудит та валідація самооцінок.

Процес 2. Ідентифікація загроз та поглиблений сценарний аналіз кіберфізичних ризиків для обраних високопріоритетних об’єктів (MOSAR).

Виконується побудова сценаріїв небажаних подій, матриць ризиків, наслідків (пріоритетів) і визначення шарів захисту (бар’єрів), а також плану дій, необхідних для зниження ймовірності виникнення та/або наслідків небажаних подій.

Процес 3. Інтеграція результатів сценарного аналізу ризиків із показниками MIL за доменами і конкретними практиками (C2M2, MOSAR).

Об’єднуються дані MOSAR щодо ризиків сценаріїв і потрібних захисних бар’єрів із спроможністю реагувати на відповідні загрози. Проводиться приоритезація сценаріїв, що визначає стратегію точкового вкладання ресурсів у підвищення кіберстійкості, і формується відповідний План її реалізації.

Процес 4. Створення циклу постійного покращення кіберстійкості критичної інфраструктури.

Відстежування виконання Плану, періодичний аудит і валідація самооцінок, повторний аналіз для висококритичних об’єктів — при суттєвих змінах у технології або у характері загроз. Опціонально — тестування на проникнення (penetration testing) із використанням «цифрових двійників» для об’єктів вищої категорії критичності.

Отже, в результаті інтеграції моделі MOSAR і C2M2 доповнюють одна одну і сприяють більш повній оцінці кіберстійкості. MOSAR виявляє, формалізує та оцінює сценарії загроз, а C2M2 оцінює здатність організації протистояти їм. Разом вони утворюють замкнутий

контур оцінки кіберстійкості, переходячи від абстрактних рівнів стійкості MIL моделі C2M2 до конкретних критичних сценаріїв. Можливе подальше розширення інтеграції шляхом підключення і використання положень NIST 800-53 [10], що містить об'ємний каталог конкретних організаційних, технічних та процедурних заходів захисту, орієнтованих на забезпечення стійкості інформаційних систем до широкого спектру кіберзагроз.

Але інтеграція принесе реальну користь лише за достатності даних про операційно-технологічні процеси для побудови модулів MOSAR. Крім того, її реалізація вимагає залучення кваліфікованих профільних фахівців, які володіють тонкощами як моделі C2M2, так і MOSAR. У нинішніх умовах дефіциту відповідних ресурсів це поки що проблематично.

Спрощеною альтернативою моделі MOSAR може бути використання матриці Мак-Кінзі (GE/McKinsey Matrix [11]) для грубого сценарного аналізу загроз (процеси 2, 3).

3. Інтеграція моделей C2M2 – GE/McKinsey Matrix

В основі моделі GE/McKinsey (рис. 1), яка традиційно використовується для оцінювання стратегічних позицій бізнес-одиниць, продуктів або організацій за критеріями «привабливість ринку» та «конкурентоспроможність об'єкта оцінювання», лежить метод експертних оцінок із використанням системи вагових коефіцієнтів [10]. Такий підхід забезпечує можливість комплексного врахування множини факторів різної природи та значущості під час формування інтегральних показників.

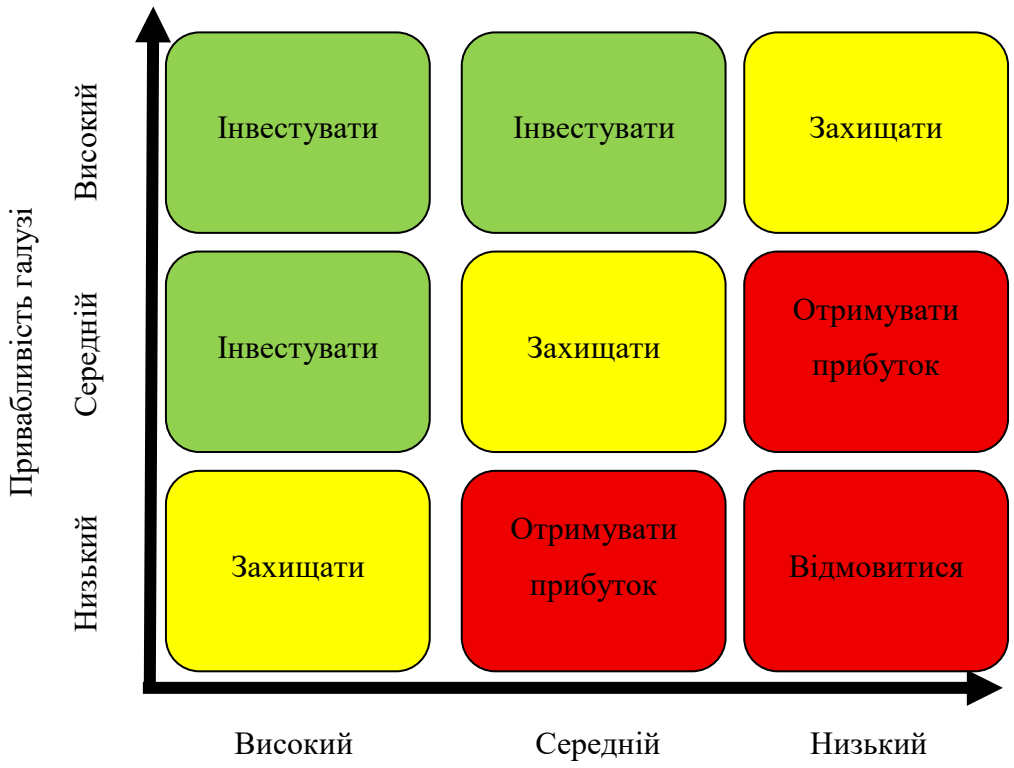

Рисунок 1 — Матриця GE/McKinsey 3*3

На відміну від простішої матриці BCG (Boston Consulting Group) аналогічного призначення, що базується на аналізі двох окремих показників, модель GE/McKinsey передбачає оцінювання двох багатофакторних груп критеріїв. Для кожної з осей матриці формується набір «зовнішніх» і «внутрішніх» факторів, специфічних для бізнес-одиниці, що оцінюється. Наприклад, привабливість ринку може визначатися через оцінку його розміру,

темпів зростання, рентабельності, гостроти конкуренції, а конкурентоспроможність бізнес-одиниці — через зайняту частку ринку, лояльність клієнтів, технологічну перевагу, якість менеджменту.

Дещо узагальнюючи підхід GE/McKinsey, позицію в матриці можна інтерпретувати як індекс співвідношення між «бажанням» (в деякому контексті) і «спроможністю» його задовольнити. У класичній інтерпретації «бажання» — це намір успішно вийти на привабливий ринок, а конкурентоздатність — це відповідна спроможність.

У контексті ризик-менеджменту матриця може бути адаптована для аналізу загроз: вісь Y відображає важливість (impact) загроз ризикового кейсу (сценарію) і бажання йому запобігти, а вісь X — спроможність йому протистояти (resilience).

Потенційна перспективність перенесення класичного інструментарію стратегічного бізнес-аналізу у загальну площину безпекових досліджень, на додаток до традиційної матриці «ймовірність — наслідки», визначається такими аспектами.

По-перше, модель забезпечує багатофакторне оцінювання різнорідних загроз з урахуванням технічних, економічних, воєнних та соціальних чинників.

По-друге, підхід дає змогу комплексно враховувати стійкість системи (resilience), включаючи не лише засоби пасивного й активного захисту, але й організаційні та управлінські фактори забезпечення функціонування системи.

По-третє, матриця характеризується високою наочністю, надає інтуїтивно зрозумілу карту пріоритетів, спільну мову для керівництва та міжвідомчої координації, структуровану аргументацію рішень для аудиторів. Візуальне представлення результатів у вигляді матриці забезпечує формування єдиного інформаційного простору для керівництва, профільних експертів та регуляторних органів, сприяючи обґрунтованому визначенню пріоритетів щодо розподілу ресурсів і реалізації захисних заходів.

Важливим аргументом на користь адаптованої моделі є також її багаторічне успішне застосування у сфері стратегічного управління та бізнес-ризик-менеджменту для балансування співвідношення між потенційними вигодами та ризиками. В умовах функціонування складних децентралізованих систем критичної інфраструктури така модель може бути використана для підтримки ризик-орієнтованого розподілу обмежених ресурсів захисту, включаючи засоби протиповітряної оборони, резервне обладнання, канали зв’язку, енергетичні потужності та інші критично важливі ресурси.

Загалом у наведеній узагальнюючій інтерпретації матриця GE/McKinsey (звичайно 3*3 або 5*5) може бути використана для оцінювання і приоритезації безпекових кейсів у різних секторах критичної інфраструктури — в електроенергетиці, системах водопостачання, транспортній галузі та інших сферах.

Процес побудови матриці включає такі стереотипні етапи:

1. Вибір груп факторів, що формують осі матриці. Їх склад визначається призначенням моделі, загальною постановкою завдання та особливостями предметної області дослідження.

2. Визначення вагових коефіцієнтів факторів, що характеризують відповідну вісь оцінювання.

3. Оцінювання значущості факторів для досліджуваного випадку (варіанта рішення).

4. Визначення індексу оціночної зони досліджуваного випадку за осями інтегральних показників та визначення положення досліджуваного об’єкта в межах відповідної оціночної зони матриці.

Як приклад результатів першого етапу побудови матриці наведемо гіпотетичні сукупності факторів для сектору електроенергетики, який належить до найбільш стратегічно важливих складових критичної інфраструктури держави та характеризується підвищеною чутливістю до реалізації кіберфізичних загроз.

Вісь Y — інтегральний індекс важливості ризикового сценарію (Impact). Значення індексу формується на основі багатокритеріального оцінювання наслідків реалізації загрози та її стратегічної значущості для об’єкта критичної інфраструктури.

Y1. Масштаб прямого ураження, що характеризує безпосередні наслідки реалізації сценарію для енергетичної системи та може оцінюватися за обсягом втраченої генеруючої або передавальної потужності в МВт; кількістю споживачів, які залишилися без електропостачання; тривалістю порушення енергопостачання тощо.

Y2. Масштаб каскадних ефектів, що відображає потенціал поширення негативних наслідків на взаємопов’язані сектори критичної інфраструктури, зокрема транспорт, водопостачання, зв’язок, охорону здоров’я тощо.

Y3. Ймовірність реалізації загрози, що визначається з урахуванням наявних розвідувальних даних, стратегічної цінності об’єкта для противника, історичної частоти аналогічних інцидентів тощо.

Y4. Оборотність наслідків, що характеризує складність і тривалість відновлення функціонування системи після реалізації загрози та може оцінюватися за очікуваним часом відновлення або можливістю повного усунення наслідків.

Y5. Соціально-гуманітарні наслідки, що відображають вплив сценарію на населення, включаючи погіршення умов життєдіяльності, ризики для здоров’я та безпеки громадян, можливі міграційні процеси та прояви соціальної нестабільності.

Y6. Вплив на обороноздатність держави, що характеризує потенційний вплив сценарію на забезпечення функціонування військових формувань, систем протиповітряної оборони, об’єктів військової інфраструктури та інших елементів сектору

безпеки й оборони.

Вісь X — інтегральний індекс стійкості (Resilience). Значення індексу формується на основі оцінювання сукупності технічних, організаційних та ресурсних спроможностей об'єкта критичної інфраструктури щодо протидії загрозам, збереження функціональності та відновлення після інцидентів.

X1. Інженерна захищеність об’єкта, що характеризує рівень пасивного захисту критичних елементів інфраструктури, включаючи захист від прямого ураження, просторове розосередження критичного обладнання, фізичне резервування, маскування тощо.

X2. Спроможність активної протидії загрозам, що відображає наявність засобів активного захисту, зокрема прикриття засобами протиповітряної оборони, засобами радіоелектронної боротьби (блокування GPS/ГЛОНАСС), а також механізмів кіберзахисту систем управління технологічними процесами (SCADA/ICS).

X3. Експлуатаційна стійкість та резервування, що оцінює наявність резервних ресурсів і можливість функціонування системи в деградованих режимах, включаючи резерви критичних компонентів, альтернативні маршрути енергопостачання, резервні підстанції тощо.

X4. Людський фактор та ремонтопридатність, що характеризує рівень підготовки персоналу до дій в умовах надзвичайних ситуацій, забезпеченість аварійно-відновлювальними бригадами (здатність працювати під повторними обстрілами вночі), наявність типових процедур реагування та очікувану швидкість відновлення функціонування об’єкта.

X5. Організаційна та координаційна спроможність, що відображає ефективність взаємодії між суб’єктами забезпечення безпеки (Міненерго — Укренерго — ЗСУ — бізнес), наявність планів реагування, кризових штабів, результатів стрес-тестування та сценарного моделювання надзвичайних ситуацій.

У цілому наведені положення дають підстави розглядати адаптовану матрицю GE/McKinsey як прийнятний інструмент стратегічного оцінювання та визначення пріоритетності безпекових сценаріїв у різних сферах захисту критичної інфраструктури.

Отже, ця матриця може бути застосована і для оцінювання та приоритезації загроз у зв’язці з моделлю C2M2 замість MOSAR.

Концептуальна ідея запропонованого рішення полягає в побудові осей матриці на основі експертних оцінок загроз (вісь Y) та MIL-значень доменів C2M2, які стають безпосереднім вимірювачем для осі «здатність протистояти» (вісь X), без проміжного MOSAR-аналізу захисних бар’єрів.

З одного боку, відмова від MOSAR призводить до втрати глибокої структурної декомпозиції об’єкта, аналізу бар’єрів безпеки, виявлення прихованих залежностей та дослідження комбінованих сценаріїв. Водночас такий підхід відкриває можливість оперативно побудувати робочу методику, визначити пріоритети та першочергові заходи щодо підвищення спроможності протистояти загрозам, а також обґрунтувати необхідність проведення ретельного/детального аналізу саме там, де це критично потрібно. MOSAR передбачає витрати часу на рівні кількох місяців із залученням інженерів-технологів та побудовою десятків дерев відмов. Натомість матрицю Мак-Кінзі на основі C2M2 та експертних оцінок можна сформувати протягом кількох днів або тижнів. Крім того, вище керівництво об’єктів та Міненерго значно гірше сприймають логічну мову дерев MOSAR, ніж наочну матрицю пріоритетів, що акцентує увагу на головному.

Ключові положення запропонованого рішення полягають у такому.

По-перше, розвиток Методики Міненерго розглядається як двоетапний процес, а саме: швидкий скринінг із подальшим глибоким моделюванням критичних точок. Використання матриці для пріоритезації загроз становить перший, пілотний етап розвитку Методики. Запропоноване рішення спирається на дані, що вже збираються, забезпечує управлінський результат із документованим обґрунтуванням та закладає архітектуру, до якої на наступному етапі може бути інтегровано MOSAR. Отже, таке рішення видається доцільним не лише як спрощувальний тимчасовий компроміс, але й як інструмент подальшого відбору найбільш критичних сценаріїв для поглибленого аналізу у поєднанні з MOSAR. Водночас самостійна цінність матриці визначається тим, що в умовах динамічної зміни загроз необхідний оперативний зріз, який дозволяє, у разі потреби, швидко розподілити інженерні, ремонтні та захисні ресурси.

По-друге, не всі домени C2M2 однаково релевантні для кожного сценарію, тобто під час оцінювання спроможності протистояти загрозам необхідне сценарно-залежне зважування доменів.

У табл. 2 наведено приклад експертно обґрунтованих ненормованих ваг доменів для чотирьох сценаріїв:

S_1 — кібератака на системи SCADA/EMS;

S_2 — відмова систем керування (основної та резервної);

S_3 — компрометація ланцюга постачання;

S_4 — гібридний удар (фізичний та кібернетичний).

Таблиця 1 — Приклад ваг доменів для конкретних сценаріїв

Домен	Сценарії			
	S_1	S_2	S_3	S_4
ASSET	5	5	4	3
THREAT	4	2	5	2
RISK	3	4	4	5
ACCESS	5	2	3	4
SITUATION	5	3	3	4
RESPONSE	4	5	3	5

Продовж. табл. 1

THIRD-PARTIES	3	3	5	2
WORKFORCE	3	4	3	4
INFORMATION	3	2	3	4
PROGRAM	3	3	3	4

При реалізації підходу з автономним використанням матриці процеси 2 і 3 попередньої схеми набувають такого змісту.

Процес 2.1. Генерація сценаріїв загроз S_j на основі експертного досвіду, підходу «Що буде, якщо…?» і сценарного моделювання дерев подій та ймовірностей. Формування переліку факторів f_{yi}, що характеризують можливі наслідки загроз (вісь *Y*) для сектору електроенергетики

Процес 2.2. Визначення нормованих ваг w_{yij}, що характеризують важливість загроз для сценарію S_j факторів f_{yi} за умови дотримання правил (1).

$$w_{yij} = (0...1), \quad \sum_{\text{i}} w_{yij} = 1. \tag{1}$$

Визначення вкладу c_{yij} факторів f_{yi} у загальну оцінку C_{yi} факторів сценарію S_j за умов (2).

$$c_{yi} = (0...5), \quad c_{yj} = \sum_{\text{i}} c_{yi} * \ c_{yi} \ . \tag{2}$$

Процес 3.1. Визначення нормованих ваг w_{xij} доменів C2M2 для протистояння сценарію S_j за дотриманням умов (3).

$$w_{xij} = (0...1), \ \sum_{\text{i}} w_{xij} = 1. \tag{3}$$

Визначення загальної оцінки R_{xj} спроможності протистояння сценарію S_j. Відбувається за виразом (4) та умовою (5).

$$R_{xj} = \sum_{\text{i}} MIL_{ij} * w_{xij} * r_{норм}. \tag{4}$$

$$MIL_{ij} * r_{норм} = (0...5). \tag{5}$$

Процес 3.2. Побудова матриці пріоритезації сценаріїв S_j за комбінацією значень C_{yj} та R_{xj}, аналіз можливостей та шляхів підвищення MIL на рівні конкретних практик доменів для критичних S_j (великі значення C_{yi} та низькі значення R_{xj}).

На етапі 1 (базовому) матриця використовується автономно з урахуванням таких основних недоліків та обмежень підходу.

1. Усереднення при обчисленні R_{xj}, що може приховати небезпечну ситуацію за окремими доменами. Для запобігання таким випадкам можливе введення правила-«запобіжника»: якщо для досліджуваного сценарію $MIL = 0$ за будь-яким доменом із найвищою вагою (у табл. 2 для сценарію S_1 це домени ASSET, ACCESS та SITUATION), сценарію в Процесі 3.2 автоматично присвоюється найвищий пріоритет.

2. Відсутність фізичної складової захищеності (захисні споруди, ППО) у доменах C2M2. Для компенсації цього недоліку можливе введення додаткового умовного домену ФІЗЗАХИСТ у Процес 3.2 для кіберфізичних загроз (у табл. 2 це сценарій S_4).

3. Суб'єктивність ваг доменів за сценаріями та динамічність загроз. З цим недоліком доводиться змиритися. Суб'єктивність оцінок є початковою принциповою особливістю C2M2, а динамічність загроз в умовах безперервних воєнних дій має неминучий характер. Для впорядкування процесів оцінювання доцільно створити та періодично переглядати методичний документ у вигляді базової бібліотеки сценаріїв із рекомендованими вагами доменів і факторів загроз, що може коригуватися експертами залежно від особливостей конкретного об'єкта та появи нових сценаріїв.

4. MIL оцінює зрілість процесів захисту, а не ефективність захисних бар'єрів. Це є принциповим припущенням етапу 1, яке для критичних сценаріїв із найвищими пріоритетами має бути усунуто на етапі 2.

На етапі 2 (розвинутому) підключається MOSAR як інструмент поглибленого аналізу для сценаріїв із зони найвищих пріоритетів матриці. Тобто виконуються процеси 1, 2.1, 2.2, 3.1, 3.2 (обмежений пріоритезацією), 2, 3, 4.

4. Висновки

Запропонований двоетапний підхід і конкретні рішення щодо його здійснення (використання матриці Мак-Кінзі для попередньої приоритезації і моделі MOSAR для подальшого поглибленого аналізу) може, на аргументовану вище думку авторів, бути покладено в основу розвитку C2M2-Методики в ресурсоощадному напрямі сценарно-орієнтованого оцінювання кібербезпеки електроенергетичного сектору України. Для практичної реалізації першого етапу необхідно виконання пілотного проєкту для декількох критичних об'єктів, а саме: створення експертної групи (енергетики, військові, кіберспеціалісти), виконання для обраних об'єктів процесів 2.1–3.2 з узгодженим калібруванням факторів і вагових коефіцієнтів, всебічна оцінка результатів тестування за узгодженими критеріями і прийняття рекомендаційних рішень щодо подальшої долі проєкту і запропонованого підходу в цілому. При позитивному результаті можливий поступовий перехід до другого етапу й надалі — підключення до схеми інструментів стандарту NIST 800-53, що надасть детальну технічну конкретику, але і вимагатиме відповідних ресурсів.

СПИСОК ДЖЕРЕЛ

1. Maliarchuk T., Danyk Y., Briggs C. Hybrid Warfare and Cyber Effects in Energy Infrastructure. *Connections: The Quarterly Journal*. 2019. Vol. 18, N 1. P. 93–110. DOI: https://doi.org/10.11610/Connections.18.1.0 (дата звернення: 19.05.2026).

2. Borychenko O., Cherniavskyi A., Muliarevych O., Shelekh Y., Sabat M. Cybersecurity in the energy industry of Ukraine: protection measures and challenges in the context of energy security. *Revista Gestão & Tecnologia*. 2024. Vol. 24 (4). P. 67–90. DOI: https://doi.org/10.20397/2177-6652/2024.v24i4.2876 (дата звернення: 19.05.2026).

3. Mehta U. Cybersecurity GRC in Energy & Utilities: Trends, Gaps, and Solutions. LinkedIn, 2025. URL: https://www.linkedin.com/pulse/blog-188-cybersecurity-grc-energy-utilities-trends-gaps-umang-mehta-fyndf/ (дата звернення: 19.05.2026).

4. Єрмак С.О. Методологічні орієнтири аналізу критичної інфраструктури та критично важливих виробничих підприємств. *Бізнес Інформ*. 2025. № 12. С. 31–39. DOI: https://doi.org/10.32983/2222-4459-2025-12-31-39.

5. Кібербезпека. Міністерство енергетики України. URL: https://www.mev.gov.ua/storinka/kiberbezpeka (дата звернення: 19.06.2026).

6. U.S. Department of Energy. Cybersecurity Capability Maturity Model (C2M2) Version 2.0. July 2021. URL: https://www.energy.gov/sites/default/files/2021-07/C2M2%20Version%202.0%20July%202021_508.pdf (дата звернення: 19.05.2026).
7. U.S. Department of Energy. Cybersecurity Capability Maturity Model (C2M2) Version 2.1. June 2022. URL: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2 (дата звернення: 19.05.2026).
8. Perrin L., Munoz-Giraldo F., Dufaud O., Laurent A. Normative barriers improvement through the MADS/MOSAR methodology. *Safety Science*. 2012. Vol. 50, N 7. P. 1502–1512. DOI: https://doi.org/10.1016/j.ssci.2012.02.002 (дата звернення: 19.05.2026).
9. Fošner A., Bertoncelj B., Poznič T., Fink L. Risk analysis of critical infrastructure with the MOSAR method. *Heliyon.* 2024. Vol. 10, N 4. P. e26439. DOI: https://doi.org/10.1016/j.heliyon.2024.e26439 (дата звернення: 19.05.2026).
10. Joint Task Force. Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53 Revision 5. Gaithersburg, MD: National Institute of Standards and Technology, 2020. 495 p. DOI: https://doi.org/10.6028/NIST.SP.800-53r5 (дата звернення: 19.06.2026).
11. McKinsey GE Matrix: A Powerful Strategic Tool for Business Growth. The Strategy Institute. 2025. URL: https://www.thestrategyinstitute.org/insights/mckinsey-ge-matrix-a-powerful-strategic-tool-for-business-growth (дата звернення: 19.05.2026).

Стаття надійшла до редакції 23.06.2026 / прийнята до друку 13.08.2026