DOI: 10.35681/1560-9189.2024.26.2.316908

УДК 004.5

О. М. Хоменко[1], В. Р. Сенченко[2], О. В. Коваль[1,2]
[1]НТУУ «КПІ імені Ігоря Сікорського»
Берестейський проспект, 37, 03056 Київ, Україна
[2]Інститут проблем реєстрації інформації НАН України
вул. М. Шпака, 2, 03113 Київ, Україна

Мережевий підхід при дослідженні каскадних ефектів критичних інфраструктур

Каскадний збій у роботі критичної інфраструктури призводить до негативних наслідків, тому важливо вчасно виявити та провести превентивні дії для зменшення наслідків каскаду. У статті представлено аналіз можливостей мережевого підходу при побудові та дослідженні моделі каскаду на основі теорії графів. За допомогою метрик якості графів можливо визначити центральність і важливість вузлів моделі, розрахувати ймовірності переходів між вузлами, настання критичних подій, дослідити різні сценарії розвитку. Графічна модель енергомережі, являє взаємопов'язану мережу вузлів і кінцевих обмежень (лінія електропередачі, трансформаторна підстанція, імпеданс та інші). Розглянуто застосування різних мережевих підходів — мережі Баєса, Петрі, Маркова та наведено результати порівняльного аналізу їхніх можливостей при виникненні каскаду. Це дозволяє більш досконало адаптувати мережеві методи до конкретних потреб моделювання та сформувати вимоги до відповідних програмних засобів.

Ключові слова: *критична інфраструктура, каскадний збій, теорія графів, мережа Баєса, мережа Петрі, ланцюг Маркова, онтологія.*

Вступ

Стійкість (резільєнтність) критичної інфраструктури (КІ) до зовнішніх негативних впливів є важливою умовою функціонування сучасного суспільства. Захист КІ, збільшення її стійкості є актуальною темою дослідження, адже перебої у роботі або виведення з ладу одного або декількох об'єктів КІ негативно впливають на життя всього суспільства. Станом на грудень 2022 року загальна сума задокументованих збитків інфраструктури України внаслідок повномасштабного вторгнення, розпочатого Росією 24 лютого 2022 року, оцінюється в 137,8 мільярда доларів (вартість відновлення); знищено не менше 64 великих і середніх підприємств, 84,3 тис. одиниць сільськогосподарської техніки, 44 соціальних центри, майже 3 тис. мага-

зинів, 593 аптеки, майже 195 тис. приватних автомобілів, 14,4 тис. громадського транспорту, 330 лікарень, 595 адміністративних будівель державної і місцевої адміністрації пошкоджено, зруйновано або захоплено [14]. Станом на 28 грудня 2022 понад 35 тисяч об'єктів в Україні знищено внаслідок атак Росії, з майже 30 000 атак, зафіксованих з моменту вторгнення, було пошкоджено 702 об'єкти критичної інфраструктури: газопроводи, підстанції, мости [44]. Правові й організаційні засади створення та функціювання національної системи захисту критичної інфраструктури регулюються Законом України «Про критичну інфраструктуру» [1].

Однією із небезпечних подій є каскадний збій — процес, який може призвести до виведення з ладу частини об'єктів або всієї КІ. На розвиток каскадного збою впливають зв'язки між об'єктами (залежності), характеристики, унікальні для кожної системи та сукупність подій у різних фазах розвитку каскаду. Складна система (критична інфраструктура) може бути описана у вигляді мережі, що спрощує її аналіз та інтерпретацію. Вивчення каскадних збоїв у мережах є важливою задачею для дослідження того, як структура мережі впливає на її стійкість до каскадів. Розробка підходів для оцінки каскадних ефектів, а також стратегій зупинки, пом'якшення наслідків, відновлення та посилення мереж надає можливість розробити програмні інструменти, які можуть аналізувати, передбачати та застосовуватися для прийняття рішень, щоб запобігати виникненню або зменшити вплив каскадних збоїв на систему.

У статті наведено огляд підходів на основі теорії графів, мережі Баєса, мережі Петрі, ланцюга Маркова, семантичних онтологічних мереж і програмних засобів на базі цих підходів для дослідження каскадних ефектів з метою моделювання і оцінки потенційно небезпечних подій, прогнозування їхніх наслідків, запобігання та зменшення негативних наслідків каскадних ефектів для прийняття рішень.

Каскадні збої та ефект доміно в критичній інфраструктурі

Критичні інфраструктури часто сильно взаємозалежні, тобто збій в одній структурі (наприклад, електромережі) може викликати збої в інших структурах (наприклад, комунікаційних або транспортних). З позиції системного аналізу об'єкти КІ утворюють комплексні мережі, де зв'язки між вузлами мережі утворюють залежності. За характером зв'язки розрізняються [2] на залежності та взаємозалежності.

Залежність — це зв'язок між двома інфраструктурами, за допомогою якого стан однієї інфраструктури впливає або залежить від стану іншої.

Взаємозалежність — це двосторонній зв'язок між двома інфраструктурами, в якому стан кожної інфраструктури впливає або залежить від стану іншої.

Взаємозалежності поділяються на такі типи [2]:

фізичний — стан однієї інфраструктури впливає на роботу іншої і навпаки;

кібернетичний — стан інфраструктури залежить від інформації, яка необхідна для її роботи та передається через інформаційну інфраструктуру;

географічний — інфраструктури розташовані близько одна відносно одної. Локальна екологічна подія може спричинити зміни стану в усіх інфраструктурах;

логічний — стан кожної із інфраструктур залежить від стану іншої через механізм, який не є фізичним, кібернетичним або географічним.

Перелік «залежностей» і «взаємозалежностей» між взаємопов'язаними інфраструктурами, як правило, доволі значний і залежить від особливостей предметної

області, рівня деталізації, складу функціональних задач, які характеризують КІ та багатьох інших факторів. Для візуального представлення та розуміння зв'язки між компонентами КІ, які іноді бувають прихованими, зазвичай зображуються у вигляді графа (рис. 1).

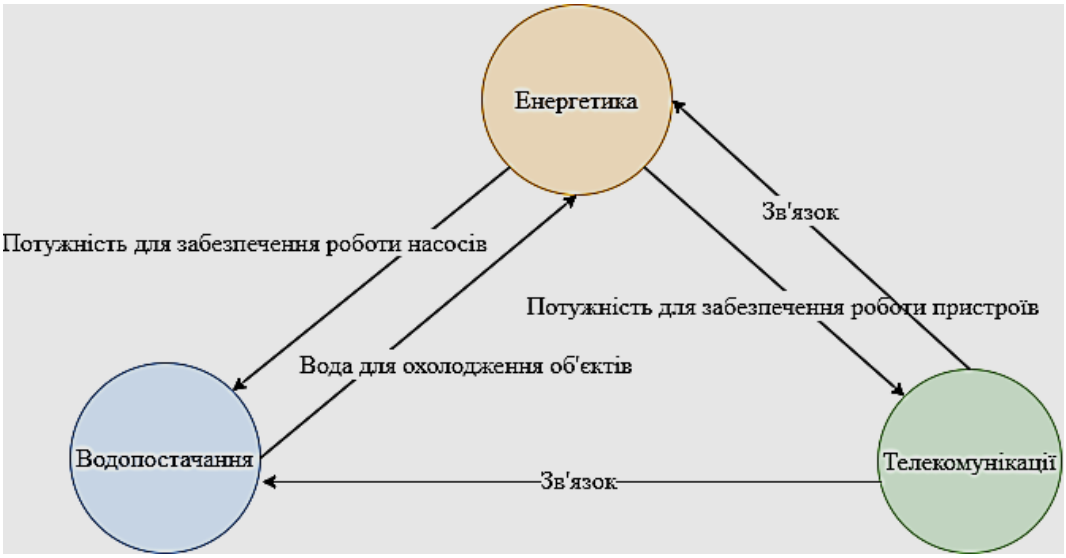

Рис. 1. Приклад зв'язків між критичними інфраструктурами різних сфер

Як свідчить досвід, кожна критична інфраструктура має у своєму складі чутливі до збоїв об'єкти, які реагують на різні початкові (тригерні) події. Загальна класифікація початкових подій, запропонована в роботі [3], поділяє їх на три основні типи: природні, техногенні, антропогенні (фактори, зумовлені діяльністю людини). Безумовно, кожен із перелічених типів тригерних подій може породжувати каскадний ефект або ефект доміно в роботі об'єктів КІ. Слід нагадати, що терміни «каскадний збій» та «ефект доміно» в літературі використовуються як взаємозамінні.

Виникнення каскадного ефекту може призвести до виводу із ладу всієї КІ, впливати на роботу взаємозв'язаних інфраструктур і спричинити негативні наслідки для суспільства, економіки та навколишнього середовища. Наявність взаємозалежності в роботі КІ призводить до збільшення ризиків виникнення повномасштабних збоїв, які розрізняються за характером розвитку та наслідками [2]:

— каскадний збій (ефект доміно) в одній інфраструктурі спричиняє збій компонента в другій інфраструктурі, що згодом спричиняє збій в іншій інфраструктурі. Тобто ефект доміно — ймовірність виникнення або послідовне виникнення аварій на об'єктах, розташованих біля об'єкта підвищеної небезпеки, на якому виникла аварія, що пов'язана із використанням небезпечних речовин [6];

— зростаючий (ескалація). Збій в одній інфраструктурі посилює незалежний збій в іншій, збільшується тяжкість, час для відновлення;

— звичайний (загальна причина) збій двох або більше інфраструктур одночасно, де основна причина збою широко поширена (наприклад, природне явище).

Як показують дослідження останніх років, негативні наслідки в разі виникнення каскадного ефекту або ефекту доміно постійно збільшуються. Так, у роботі [4] наведено результати аналізу сценаріїв розвитку 225 аварій у період з 1961 по

2007 рік, які характеризують ефект доміно. Збільшення негативних наслідків від ефекту доміно пояснюється як збільшенням масштабу самих інфраструктурних систем, так і зростаючою складністю взаємозв'язків і процесів, які реалізовані в інфраструктурі. В роботі [5] запропоновано класифікацію тригерних подій, які викликають ефект доміно це: випадкова подія, технічна подія, навмисна, спричинена пожежею, спричинена вибухом, внутрішнім втручанням, зовнішнім втручанням, часовий фактор, просторовий фактор, послідовна дія, паралельна поява кількох факторів, за тепловим випромінюванням, за надлишковим тиском та інші. Слід підкреслити, що для окремих інфраструктур каскадні ефекти можуть не виникати відразу після настання тригерної події, а проявлятися протягом певного часу в інших об'єктах, які не були джерелом пошкодження, але мають неявні зв'язки.

Як наочний приклад породження каскадного ефекту можна розглянути електромережу яка є важливим компонентом КІ. Виникнення двох або більше майже одночасних збоїв (тригерних подій) може ініціювати каскадний ефект. Приклад збігу таких обставин описаний у роботі [9], що призвело до дуже великих відключень електроенергії (приблизно 50 мільйонів людей Північної Америки постраждали від відключення електроенергії 14 серпня 2003 року) [9]. Каскадний збій може бути породжений через множину факторів, наприклад: нестабільність напруги та частоти, приховані збої систем захисту, помилки програмного забезпечення або оператора, кібератаки, перевантаження лінії [8]. На розподіл факторів або тригерів, які призводять до каскадних ефектів, впливають різні елементи енергетичної системи.

Частка факторів, які сприяють каскадним збоям енергопостачання, може змінюватися залежно від конкретних досліджень і контексту. Однак загальні статистичні дані різних досліджень вказують на такі приблизні відсотки для ключових факторів (тригерних подій) у сфері електроенергетики [9]:

1) *технічні збої*: на них припадає 30–40 % каскадних подій. Вони можуть бути викликані незначними несправностями, але призводять до великих відключень через взаємопов'язані системи;

2) *фактори навколишнього середовища*: Близько 20–30 % тригерів, особливо екстремальних погодних явищ і стихійних лих, стають більш частими через зміну клімату;

3) *людські помилки*: спричиняють приблизно 10–20 % каскадних подій, які часто посилюються через погане управління мережею або помилки в обслуговуванні;

4) *економічні/ринкові фактори:* відповідальні за приблизно 10–15 % каскадних ефектів, головним чином, коли збої у постачанні палива або коливання ринку палива впливають на доступність енергії;

5) з*бої у кібербезпеці*: зростаюча загроза, яка становить приблизно 5–10 %, але швидко зростає, оскільки все більше енергетичних систем переходять на цифрові технології;

6) *інтеграція відновлюваних джерел енергії*: зростаюче проникнення відновлюваних джерел створює нові ризики, вносячи приблизно 5–15 % у каскадні збої.

Розуміння розподілу цих тригерів має вирішальне значення для підвищення стійкості електричної мережі, оптимізації технічного обслуговування та підготовки заходів щодо компенсації наслідків каскадних ефектів.

В умовах військових дій в Україні саме електромережі є найбільш уразливими об’єктами, отже існує великий ризик виникнення ланцюгів збоїв (каскадних ефектів), які можуть спричинити незбалансоване навантаження, що в результаті призводить до відключення електроенергії, руйнування електромережі. В електричній мережі каскадний ефект визначається як вихід з ладу одного компонента, який має прямі наслідки для продуктивності мережі, але також може спричинити перевантаження та, як наслідок, часткову або повну відмову інших компонентів [7].

Загальна модель розвитку каскадних збоїв в електричних мережах складається з трьох етапів [10] та показана на рис. 2:

1) *початковий етап*: виникнення збоїв, пошкоджені об’єкти виходять з ладу через обмежену потужність. При вчасному виявленні збоїв можливо вжити відповідних заходів для локалізації і зменшення впливу аварії;

2) *етап розширення*: збої продовжують поширюватися та збільшуються в масштабі, що призводить до зміни навантаження. На етапі розширення ще можливо частково контролювати процес розвитку аварії у мережі;

3) *етап колапсу*: збої накопичуються, значна кількість компонентів системи вже вийшли з ладу, збільшується навантаження, що з часом може призвести до виведення із ладу усієї електромережі.

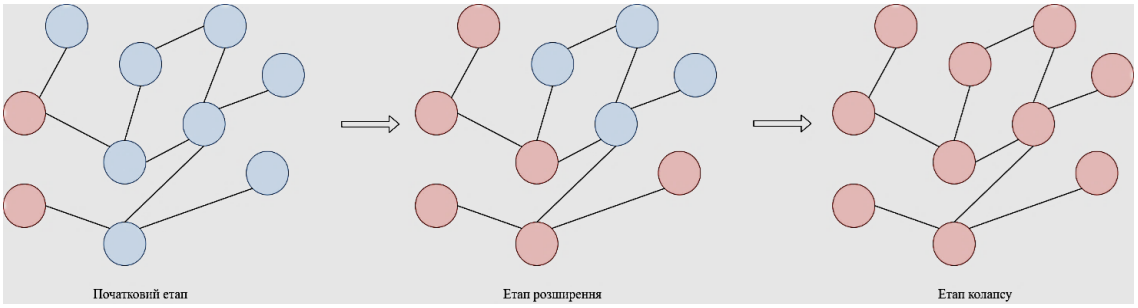

Рис. 2. Загальна модель розвитку каскадних збоїв

На основі аналізу сценаріїв розвитку 37 задокументованих подій (blackout), які мали місце в різних енергосистемах світу, визначено, що знеструмлення енергосистеми (blackout) зазвичай складаються з п’яти фаз:

1) передумови (precondition);
2) початкової події (initiating event);
3) каскадних подій (cascading events);
4) кінцевого стану (final state);
5) відновлення енергосистеми (restoration).

Результатом цього аналізу можна вважати висновок, що для підвищення резильєнтності енергосистеми до прояву каскадних ефектів, превентивні дії мають бути вжиті до того, як відбулися тригерні події, оскільки після початку високошвидкісного каскаду ситуація стає вже неконтрольованою, а blackout може статися протягом дуже короткого часу [36]. Тобто для підвищення резильєнтності критичної інфраструктури мають бути запропоновані додаткові структурні елементи, завдяки яким менеджер (в автоматичному режимі) має можливість змінювати сценарії розвитку процесу.

Застосування теорії графів для аналізу процесів розвитку каскадних ефектів електромереж

Каскадні ефекти стосуються ланцюга збоїв в електромережі, коли збій в одній частині системи поширюється та викликає подальші збої, потенційно призводячи до масштабних відключень або збоїв у всій системі. Використання теорії графів і мережевого аналізу дозволяє енергетикам і системним операторам моделювати та розуміти ці явища, представляючи енергомережу як складну взаємопов'язану мережу вузлів і кінцевих обмежень.

При моделюванні каскадних ефектів об'єкти критичної інфраструктури та зв'язки між ними можливо описати за допомогою графа $G = (V, E)$, де $|V| = n$ — кількість вершин, $|E| = m$ — кількість ребер (дуг).

За допомогою метрик теорії графів можливо визначити вразливі компоненти в мережі та провести аналіз подій, які можуть породжувати каскадні ефекти. Для аналізу графів використовуються матриця суміжності, яка представляє прямі зв'язки між вузлами, і матриця Лапласа, що використовується для підрахунку кістякових дерев графа. На основі матриці суміжності можна сформувати пари вершин з найбільшими зв'язками, тобто виявити найбільш критичні вузли електромережі. Ці матриці обчислюються за такими формулами:

$$A_{ij} = \begin{cases} w_{ij}, \text{якщо } (i,j) \in E, \\ 0 \text{ — в іншому випадку,} \end{cases} \quad (1)$$

де w_{ij} — вага ребра, яка з'єднує вершини *i* та *j*;

$$L_{ij} = \begin{cases} d_i, \text{якщо } i = j, \\ -1, \text{якщо } i \text{ є суміжною з } j, \\ 0 \text{ — в іншому випадку,} \end{cases} \quad (2)$$

де d_i — степінь вершини (degree of node) *i*.

Для аналізу стійкості та вразливості в електромережах використовують концепції теорії складних мереж (Complex Networks), які складаються з двох різних підходів топологічного (topological) та гібридного (hybrid).

Топологічний підхід базується на представлені структури електромережі у вигляді графа, де вершини — станції і підстанції та інші компоненти структури, а ребра — зв'язки між вершинами. Для оцінки характеристик об'єктів мережі в теорії графів використовуються різні метрики. Найбільш відомими є середня довжина шляху (average path length), розмір найбільшого компонента (size of the largest component) та ефективність мережі (network efficiency) [22]. Топологічні метрики (topological metrics) поділяються на три класи і описуються такими характеристиками [15]:

Distance: Hopcount, Closeness, Eccentricity, Diameter, Radius, Girth, Expansion, Betweenness, Central Point of Dominance, Distortion;

Connection: Degree, Entropy, Joint Degree, Assortativity, Coreness, Clique, Clustering coefficient, Rich Club coefficient, Giant component, Reliability, Chromatic number;

Spectra: Algebraic connectivity, Spectral radius, Spectral partitioning, Principal eigenvector.

У гібридному підході використовується поєднання концепцій складних мереж та електротехніки (наприклад, імпеданс електричних ліній, імпульсні перенапруги або відключення генератора) для покращення топологічного підходу. Гібридна модель використовує методи стаціонарного режиму для визначення нормальної роботи та надає можливість переходити до аналізу перехідних процесів для моделювання та вивчення короткочасних збурень, забезпечуючи стабільність системи. Отже модель електромережі представляє собою орієнтований, зважений граф, ребра якого мають різний імпеданс та обмеження потоку електроенергії. Оскільки електроенергія в реальних системах тече від шин генератора до шин навантаження, то метрики із топологічного підходу змінюються на відповідні аналоги, які враховують характеристики реальних систем. У роботі [22] для опису моделі електромережі запропоновано використання характеристик net-ability, electrical degree centrality, electrical betweenness centrality, entropic degree, effective graph resistance, які більш точно передають особливості реальних систем.

При оцінці міцності графів використовують метрики (robustness metrics), які згруповані в шість категорій [16], таких як:

— кластеризація (Clustering);
— зв'язність (Connectivity);
— відстань (Distance);
— пропускна здатність (Throughput);
— спектральні методи (Spectral Methods);
— географічні метрики (Geographical Metrics).

При виборі метрик для оцінки характеристик графа *G* (мережі), потрібно враховувати тип графа, що досліджується, оцінити співвідношення між точністю та обмеженнями при обчисленні (деякі алгоритми є *NP*-складним, але мають апроксимаційні рішення).

Графові спектральні методи (Graph Spectral Techniques) використовуються для аналізу стану та управління водорозподільними мережами [17]. Методика їхнього застосування зводиться до двох етапів.

1. Виявлення вузьких місць (bottlenecks), які визначаються за допомогою спектрального розриву (spectral gap) $\Delta\lambda$ та являють собою різницю між найбільшим — λ_1 і другим за величиною — λ_2 власними значеннями матриці суміжності *A*:

$$\Delta\lambda = \lambda_1 - \lambda_2. \tag{3}$$

Спектральний розрив відображає міцність зв'язків мережі, що дозволяє виявити вузькі місця, зокрема, міст — ребро, видалення якого збільшує кількість зв'язаних компонентів графа і розділяє мережу на дві або більше частин. Чим більше значення спектрального розриву $\Delta\lambda$, тим більш стійкою є мережа [17].

2. Вимірювання міцності (strength) мережі для розбиття її на підмережі з метою спрощення дослідження графа. Міцність виражається через категорію алгебраїчна зв'язність (Algebraic connectivity). Це друге з найменших власних значень матриці графа *G*, яке обчислюється на основі матриці Лапласа і визначає міцність з'єднань мережі і стійкість до збоїв. Чим більше значення алгебраїчної зв'язності, тим більш стійким є граф *G* (а електромережа до збоїв). Тобто мережу з більшою алгебраїчною зв'язністю важче роз'єднати. Спектральний радіус або індекс (Spectral radius or Index) являє собою найбільше власне значення, яке обчислюється

на основі матриці суміжності і може використовуватись як метрика для оцінки рівня зв'язності мережі. Добре зв'язаний граф характеризується більшим значенням спектрального радіуса, що на практиці асоціюється з більшою міцністю електромережі до збоїв [17].

Важливим критерієм для прийняття рішень при виникненні збоїв у системі є оперативна обробка і аналіз динамічних змін у критичній інфраструктурі. Моделювання і аналіз КІ в режимі реального часу здійснюється шляхом поєднання графів і множини взаємодіючих кінцевих автоматів, де стани змінюються відповідно до вихідних даних інших автоматів. Критична інфраструктура описується як орієнтований граф, який не містить петель і моделює залежності між акторами КІ: вершина — актор (доповнений кінцевим автоматом, який відображає статус), ребро — зв'язок між двома акторами. За допомогою підходу можливо виміряти вплив дискретної події на КІ, загрози зниження продуктивності або виникнення збою [18].

Для розробки та оцінки ефективності альтернативних стратегій зменшення ризику виникнення каскадного збою в КІ застосовуються метрики центральності графа. Методологія зменшення ризиків для критичної інфраструктури на основі аналізу центральності графів складається з трьох етапів [19]:

1) виявлення графа залежностей ризиків (dependency risk graphs) у поєднанні з методологією мультиризикового аналізу залежності (multi-risk dependency) для моделювання можливих каскадних збоїв у КІ;

2) аналіз і дослідження графів залежностей на основі метрики центральності графа;

3) використання методів підбору характеристик ризиків з метою оцінки впливів метрик центральності графа на зниження ризику виникнення каскадного ефекту в КІ.

Визначення центральних вершин у будь-якої досліджуваної мережі є дуже важливою задачею для створення стійкої до збоїв або атак моделі електромережі. Не дивно, що різними школами дослідників запропоновано біля 60 метрик центральності графа, які в роботі [21] класифіковано у три групи метрик:

1) центральність вершини в графі (point centrality metrics);

2) центральність графа (graph centrality metrics);

3) центральність вибору групи найбільш впливових вершин (group selection centrality metrics).

Метрики центральності вершини графа (point centrality metrics) використовуються для оцінки відносної важливості вершини в графі [19] та характеризуються такими показниками як ступінь центральності (Degree centrality) вершин (вузлів) у графі. Ступінь центральності вимірює кількість вхідних або вихідних зв'язків із вузла залежно від орієнтації проекції зв'язку. Ступінь центральності визначається через k_i — число зв'язків, які має вузол на графі:

$$k_i = \sum_{j=1}^{n} A_{ij}, \tag{4}$$

де A_{ij} — матриця суміжності, яка представляє прямі зв'язки між вузлами графа.

Якщо значення degree centrality є високим — вершина в графі вважається центральною. На практиці це означає, що центральна вершина має багато залежностей і, як наслідок, вона є потенційно вразлива для зовнішніх атак (тригерних подій), які можуть призвести до каскадних збоїв. В орієнтованих графах розрізняють

два види ступені центральності: Inbound — коли ребра графа входять у центральну вершину; Outbound — коли ребра виходять з центральної вершини.

Високе значення Inbound вказує на можливість виникнення збою в КІ *з багатьох напрямів* (де вхідні ребра графа асоціюються з тригерними подіями, які можуть потенційно виникнути в КІ), а високе значення Outbound вказує *на ризик розповсюдження збою в різні вузли графа* (де вузли асоціюються зі структурними компонентами КІ).

Центральність за близькістю (Closeness centrality) — це середня довжина найкоротшого шляху між вузлом і всіма іншими вузлами на графі. Таким чином, чим більш центральний вузол, тим ближче він до всіх інших вузлів графа. Closeness centrality $CC(u)$ розраховується за формулою

$$CC(u) = \frac{N-1}{\sum_{v \in V(G)} d(u,v)}, \tag{5}$$

де $d(u, v)$ — відстань (довжина найкоротшого шляху між вершинами графа u та v), а N — число вершину графі.

Іншою метрикою при формальному аналізі мережевих (графових) структур є центральність між вузлами (Betweenness centrality). Метрика, яка кількісно визначає важливість вузла на основі його положення в мережі, надає можливість зрозуміти, як часто вузол діє як міст уздовж найкоротших шляхів між іншими вузлами мережі. Формально метрика розраховується за формулою

$$BC(k) = \sum_i \sum_j \frac{p(i,k,j)}{p(i,j)}, i \neq j \neq k, \tag{6}$$

де $p(i, j)$ — кількість найкоротших шляхів від вершини i до j, а $p(i, k, j)$ — кількість цих найкоротших шляхів, які проходять через вершину i у графі.

При аналізі електромереж дуже корисною метрикою є Bonacich (eigenvector) centrality — це міра, яка визначає важливості вузлів у мережі. По суті, вузол вважається важливим, якщо він з'єднаний з іншими важливими вузлами. Це означає, що вузли, які підключені до високоцентральних вузлів, самі будуть вважатися центральними. Аналогічно діє алгоритм Google PageRank, який ранжує веб-сторінки на основі важливості сторінок, які на них посилаються. Розрахунок цієї метрики виконується за допомогою математичного виразу

$$c_i(\alpha, \beta) = \sum_j (\alpha - \beta c_i) R_{i,j}, \tag{7}$$

де α — коефіцієнт масштабування (scaling factor); β — ступінь зваженості центральності (the extent to which centrality is weighted); R — матриця суміжності вузлів [19].

Ще однією метрикою оцінки вузла в електромережі може бути центральність ексцентриситету (Eccentricity centrality) — показник центральності вузла, який вимірює важливість вузла в мережі на основі його ексцентриситету. Ексцентриситет вузла v у зв'язному графі G визначається як максимальна відстань від v до будь-якого іншого вузла u в мережі:

$$e_G(v) = \max_{u \in G} d(v, u), \tag{8}$$

де $d(v, u)$ — найкоротший шлях між вузлами v та u моделі електромережі.

Центральність ексцентриситету відрізняється від інших метрик, таких як центральність за близькістю, що враховує суму відстаней, а не лише максимальну відстань. Це робить ексцентриситет особливо корисним для розуміння положення вузлів відносно найбільш віддалених ділянок електричної мережі.

Метрика центральність ексцентриситету корисна в сценаріях реагування на надзвичайні ситуації, наприклад, для визначення оптимального розташування екстрених служб відновлення електромереж. Аналізуючи мережу потенційних зон обслуговування при прийнятті рішень, можна мінімізувати час реагування, розмістивши об'єкти ближче до центральних вузлів.

Застосування теорії графів забезпечує потужну основу для моделювання і аналізу складних взаємозв'язків енергосистем, що робить їх безцінними інструментами для розуміння та пом'якшення ефектів каскаду. Як переваги застосування теорії графів при аналізі розвитку каскадних ефектів електричних мереж можна відзначити наступні.

Моделювання електромережі як графа. В цьому підході вершини графа представляють ключові компоненти енергетичної мережі, такі як електростанції, підстанції, трансформатори та центри навантаження, а ребра — лінії передачі або лінії розподілу електроенергії, які з'єднують ці компоненти. Граф може бути або спрямованим з урахуванням напрямків потоку електроенергії та обмежень, або неорієнтованим, де електроенергія може текти в обох напрямках лінії електропередачі.

Топологічний аналіз структури електромережі. Аналіз графа для визначення критичних компонентів (наприклад, центральні вузли або мости), збій яких може мати значні наслідки для загальної цілісності мережі. Для цього теорія графів пропонує набір метрик, таких як ступінь центральності (кількість з'єднань, які має вузол) або центральність між вузлами (як часто вузол діє як міст між іншими вузлами), що можуть визначити найбільш вразливі вузли графа або критичні лінії передачі, де збій може спровокувати каскад у КІ. Ідентифікація цих компонентів дозволяє зосередитися на посиленні механізмів захисту.

Моделювання каскадних відмов, тобто того, як локалізовані збої можуть перерости у системі збої. Наприклад, імітація відмови генератора, підстанції або лінії електропередачі і перерахунок потоку електроенергії, коли додаткове навантаження може призвести до збільшення навантаження на інші лінії або перерозподілу навантаження в мережі. Графи можна розширити до часових Графів, щоб моделювати, як каскад розвивається з часом.

Аналіз вразливості. Теорія графів допомагає оцінити стійкість мережі шляхом моделювання сценаріїв, коли ключові компоненти (вузли/ребра) виходять з ладу, і спостерігати за здатністю мережі протистояти цим збоям або відновлюватися після них.

Методи візуалізації. Інструменти візуалізації, що засновані на теорії графів, дозволяють ефективно представляти і аналізувати каскадні ефекти для їхнього кращого сприйняття. Ці інструменти можуть проілюструвати, як збої поширюються мережею, полегшуючи розуміння вразливостей і допомагаючи планувати заходи протидії.

Моделювання управлінських рішень. На основі аналізу графів можна визначити стратегії зменшення навантаження, тобто які частини мережі слід відключити першими під час каскадної події, щоб запобігти поширенню збоїв. Вузли з меншою центральністю або меншою важливістю можуть бути визначені для контрольованого відключення, щоб зберегти найбільш критичні частини мережі.

На основі визначених характеристик мережі можливо провести динамічний аналіз вузьких місць у транспортних мережах [20]. Отже, за допомогою теорії графів можливо провести оцінку характеристик об'єктів, моделювання сценаріїв розвитку подій, враховуючи каскадні ефекти, взаємодії критичних інфраструктур.

Застосування Bayesian Network для аналізу та моделювання каскадних ефектів

Застосування байєсівських мереж для аналізу та моделювання каскадних ефектів у критичній інфраструктурі, зокрема в енергосистемах, пропонує надійну основу для розуміння складних взаємозалежностей у КІ та прогнозування поширення відмов. Мережа Баєса та її модифікації використовуються для оцінки ризиків, моделювання сценаріїв ефектів доміно [27], аналізу та збільшення стійкості КІ [30]. Для аналізу ризиків і моделювання загроз в інфраструктурі застосовуються різні методи, частина яких основана на мережах Баєса та їхніх модифікаціях [29].

Мережа Баєса (Bayesian Network, BN) — це ймовірнісна графова модель (рис. 3), яка є одним із інструментів для аналізу, отримання знань із даних, може використовуватися для моделювання складних недетермінованих систем і визначається як орієнтований ациклічний граф $G(V, E)$, де V — множина вершин, а $E \subseteq V \times V$ — множина орієнтованих ребер. Кожна вершина $X_i \in V$ відповідає випадковій величині X_i, а кожне ребро $(X_i, X_j) \in E$ представляє прямий вплив X_i на X_j.

Тобто X_i є батьком (parent) X_j, а X_j є дочірнім (child) елементом X_i.

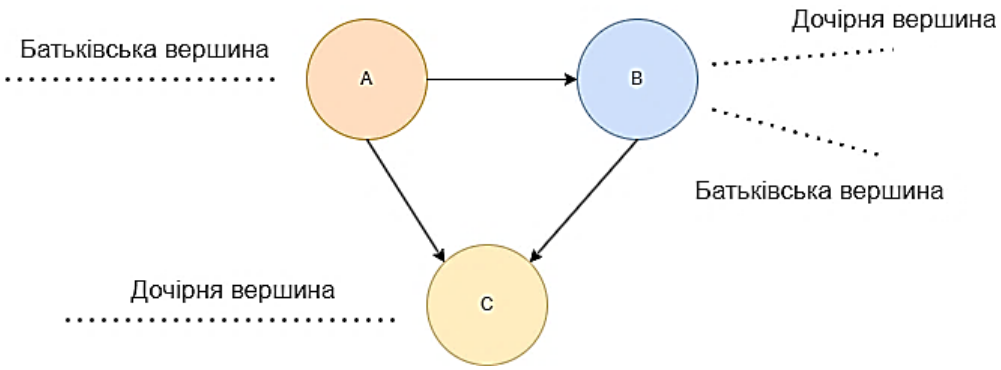

Рис. 3. Приклад Мережі Баєса

Кожна вершина X_i має відповідний розподіл імовірностей $P(X_i|pa(X_i))$, де $pa(X_i)$ — множина батьків X_i в $G(V, E)$.

Спільний розподіл імовірностей (joint probability distribution) за всіма величинами $P(X)$ у мережі визначається як [23]:

$$P(X_1, \dots, X_n) = \prod_{i=1}^{n} P(X_i|pa(X_i)). \quad (9)$$

Концепція BN побудована на теоремі Баєса, за допомогою якої можна сформувати висновок і прийняти рішення:

$$P(A|B) = \frac{P(A)P(B|A)}{P(B)}, \tag{10}$$

де $P(A)$ та $P(B)$ — імовірність виникнення події A та B відповідно; $P(B|A)$ — умовна імовірність виникнення події B за умови виникнення події A; $P(A|B)$ — умовна ймовірність виникнення події A за умови виникнення події B.

Існують різновиди мережі Баєса, які використовуються у випадках, коли потрібна розширена структура досліджень між компонентами КІ [24]:

1) моделі причинної взаємодії (Causal interaction models): модель Noisy-Or [25] використовується в байєсівських мережах для опису зв'язку між набором незалежних причин і одним наслідком. Ці мережі спеціально зосереджені на представленні причинно-наслідкових зв'язків між змінними. Вони забезпечують основу для розуміння того, як зміни однієї змінної впливають на інші. Їх доцільно застосовувати для моделювання причинно-наслідкових ефектів і висновків про потенційні небезпеки каскадних події;

2) динамічні мережі Баєса (Dynamic Bayesian networks) використовуються для моделювання динамічних і часових процесів [24], вводячи часові зрізи та тимчасові залежності між змінними. Найбільш часто динамічні мережі використовуються для аналізу (діагностування та прогнозування) кіберстійкості енергетичних систем, визначення причинно-наслідкових і часових залежностей, виявлення аномалій і вчасного реагування на них [28];

3) діаграми впливу (Influence diagrams) — це тип графічного представлення, який використовується для моделювання процесів прийняття рішень в умовах невизначеності. Вони тісно пов'язані з BN, але більше зосереджуються на тому, як взаємодіють рішення, невизначені події і результати, забезпечуючи структурований спосіб аналізу складних проблем прийняття рішень. При застосуванні Influence diagrams BN доповнюється двома типами вершин: прийняття рішень (decision) і корисності (utility) [24].

Побудова BN для дослідження каскадних ефектів, що спостерігаються в таких КІ як електромережі або мережі зв'язку, передбачає застосування методології структуризації процесів. Дотримання такої методології дозволяє змоделювати причино-наслідкові події у КІ, тобто показати як збої в одній частині КІ можуть поширюватися та викликати подальші збої в інших частинах, що призводить до каскаду подій. Ключові кроки залишаються такими ж, як і для загальних байєсівських мереж, але застосовуються спеціально для аналізу взаємозалежностей і каскадних ефектів у складних системах.

Методологія побудови байєсівської мережі складається з наступних кроків.

1. Визначення проблеми та змінних (подій), які описують каскадний ефект. Це передбачає визначення зовнішніх факторів (тригерних подій), які можуть ініціювати каскад (перебої в електропостачанні, збої обладнання або перебої і комунікаційних мережах) і позначити їхні наслідки.

2. Визначення залежностей і зв'язків у структурі мережі (Network Structure). Визначення різних типів залежностей (прямих, функціональних і логічних), тобто як взаємодіють події, що пов'язані між собою з точки зору причини та наслідку. На

цьому етапі формується структура BN, яка представляється як спрямований ациклічний граф (Directed Acyclic Graph — DAG). На практиці визначення взаємозалежності між різними компонентами системи являє собою розуміння каскаду на семантичному рівні, наприклад, робочий або несправний статус трансформатора, стан лінії електропередачі, погодні умови (звичайні або штормові) тощо.

3. Призначення умовних імовірностей (Conditional Probabilities — $P(X_i)$). Тобто кількісне визначення кожного зв'язку між змінними шляхом призначення умовного розподілу ймовірностей $P(X_i)$ кожному вузлу. Для цього формується таблиця умовної ймовірності (Conditional Probability Tables — CPT). Значення цієї таблиці кількісно визначають імовірність кожного можливого стану змінної з урахуванням станів її батьківських змінних. Джерелами розподілу ймовірностей можуть бути історичні данні (бази накопиченого досвіду), умовні ймовірності, коли реальні дані недоступні або Експертні оцінки. Наприклад, CPT для трансформатора може визначати ймовірність відмови, враховуючи, що підключена до нього лінія електропередач вийшла з ладу (наприклад, *P*(Відмова трансформатора|Відмова лінії електропередач) = 0,7).

4. Перевірка байєсівської мережі (Validate the Network). Тобто переконання у тому, що BN точно моделює каскадні ефекти. Це передбачає тестування моделі каскадного ефекту на відомих випадках каскадних збоїв, для переконання, що вона точно прогнозує поведінку аналогічно системі реального світу. Експертна оцінка реалістичності мережевої структури та її корегування, якщо за результатами тестових випробувань таки зміни потрібні.

5. Моделювання і аналіз. Використання BN для аналізу різних сценаріїв розвитку каскадних ефектів. У процесі моделювання виконується розрахунок імовірності конкретних відмов, враховуючи ознаки відмов певних компонентів або зовнішніх подій (наприклад, якщо вийшла з ладу лінія електропередачі, яка ймовірність того, що наступною вийде з ладу підстанція?). Це дозволяє визначити ймовірність різних сценаріїв майбутніх відмов, враховуючи поточний стан системи (наприклад, якщо трансформатор перебуває під навантаженням, яка ймовірність відмови лінії електропередачі нижче за течією?). BN може бути використана для оцінки ймовірності того, що сусідня підстанція вийде з ладу через збільшення навантаження, у зв'язку з атакою дронів на лінії передач. На підставі моделювання можна вжити попереджувальних заходів для зменшення негативних наслідків.

На цьому кроці також проводиться аналіз чутливості BN, який дає можливість визначити критичні вузли в мережі, де найбільш імовірно поширеться каскадний збій (наприклад, які компоненти, якщо вийдуть з ладу, найбільш імовірно призведуть до масових відключень електроенергії?).

6. Удосконалення мережі та підвищення точності BN на підставі нових даних про каскадні збої. Накопичений досвід дозволяє проводити коригування таблиці умовної імовірності (CPT), що безумовно підвищує якість моделювання в цілому.

Для побудови та моделювання BN використовуються різні інструментальні засоби, які полегшують представлення, висновок та аналіз імовірнісних зв'язків між змінними від *R* пакетів, методів графічного моделювання, алгоритмів навчання та формування висновку. Алгоритми побудови структури мережі Баєса (structure learning algorithms) умовно поділяються на два основні класи [26]:

1) методи на основі обмежень (constraint-based methods), які усувають і орієнтують ребра мережі на основі серії тестів умовної незалежності (conditional independence);

2) методи на основі оцінок (score-based methods) пошук структури, яка максимізує цільову функцію.

Існують гібридні алгоритми, які поєднують підходи на основі оцінок і обмежень. Навчання мережі Баєса є *NP*-складною проблемою частково тому, що множина розв'язків графів зростає надекспоненціально (super-exponentially) з кількістю вершин (випадкових величин), тому для побудови BN великої розмірності використовують евристичний метод [26]. При збільшенні кількості випадкових величин і їхніх можливих станів розмір таблиць CPT, що визначають імовірності можливих станів випадкової величини з урахуванням станів її батьківських випадкових величин, може зростати експоненціально, що ускладнює їхні визначення та підтримку. Відсутність даних може спричинити упереджені або неточні результати, а складність структури мережі може ускладнити її інтерпретацію.

Застосування BN для аналізу та моделювання каскадних ефектів у KI, зокрема в енергосистемах, пропонує надійну основу для розуміння складних взаємозалежностей і прогнозування поширення відмов.

Мережі Петрі (Petri nets)

Використання мереж Петрі (МП) у дослідженні каскадних ефектів, зокрема в критичній інфраструктурі, такій як енергосистеми, забезпечує структурований метод для моделювання складних одночасних процесів [31], наприклад, можливо зробити висновки про структуру та динамічну поведінку системи при виявлені каскаду.

Мережа Петрі — це орієнтований, зважений дводольний граф, який складається з двох типів вершин, що називаються позиціями та переходами, де дуги йдуть або від місця до переходу, або від переходу до місця (рис. 4). Мережа Петрі визначається таким математичним виразом [32]:

$$PN = (P, T, F, W, M_0). \tag{11}$$

де $P = \{p_1, p_2, p_3, \dots, p_m\}$ — скінчена множина позицій (m — кількість позицій), які графічно зображуються колом;

$T = \{t_1, t_2, t_3, \dots, t_n\}$ — скінчена множина переходів (n — кількість переходів), графічно зображується прямокутною смугою;

$F \subseteq (P \times T) \cup (T \vee P)$ — скінченна множина дуг від позицій до переходів або переходів до позицій.

$W: F \to \{1,2,3, \dots\}$ — вагова функція (цілі додатні числа), де k — зважена дуга може інтерпретуватись як множина з k паралельних дуг;

$M_0: P \to \{1,2,3, \dots\}$ — початкове маркування моделі МП, що представляє кількість маркерів (ціле невід'ємне число) у кожній позиції моделі, графічно зображується чорними крапками на позиції.

МП можуть ефективно моделювати динаміку каскадних відмов, представляючи стани різних компонентів (наприклад, ліній електропередач, трансформаторів) і їхні взаємодії. Кожен компонент можна моделювати як місце, тоді як переходи представляють такі події як збої або перевантаження. У моделюванні використовуються [32] поняття умов (позиції) і подій (переходи), де перехід (подія) має певну кількість

вхідних і вихідних позицій, що представляють відповідно передумови (які повинні бути виконані для спрацювання переходу) та постумови (результат переходу) події, наявність маркерів у позиції може означати кількість доступних ресурсів, стан або маркування в МП змінюється відповідно до правила переходу (рис. 4).

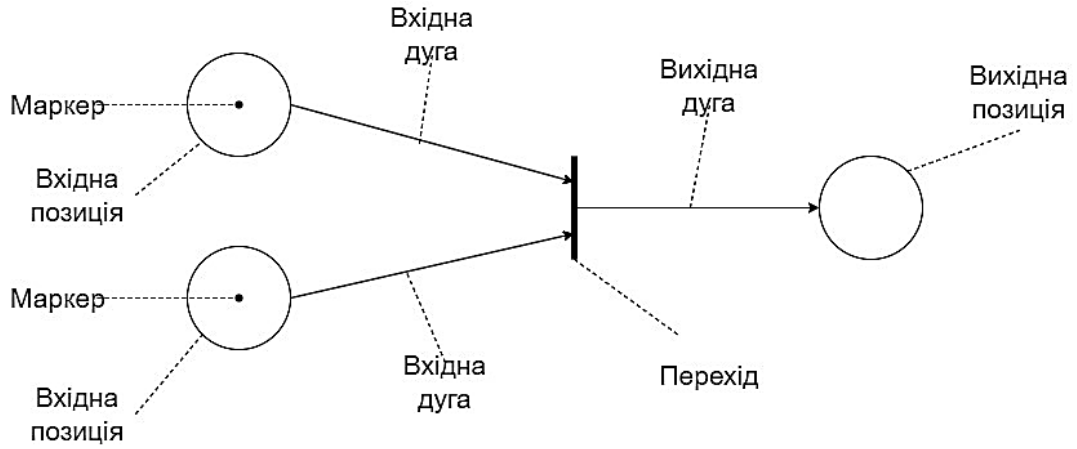

Рис. 4. Приклад мережі Петрі

При моделюванні комплексних процесів може виникнути проблема обмеженості функціональності мережі Петрі. Для подолання обмежень та розширення можливостей моделювання були розроблені різні модифікації: стохастична мережа Петрі (Stochastic Petri Net), часова мережа Петрі (Timed Petri Net), кольорова мережа Петрі (Colored Petri Net), нечітка мережа Петрі (Fuzzy Petri Net), гібридна мережа Петрі (Hybrid Petri Net) [33], узагальнена стохастична мережа Петрі (Generalized Stochastic Petri Net) [34], часова стохастична кольорова мережа Петрі (Timed Stochastic Colored Petri Net) [35]. DOMINO-GSPN — узагальнена стохастична мережа Петрі використовується для моделювання ймовірності аварії (ефект доміно) та патерна її поширення, графічного представлення взаємодії між компонентами, прийняття рішень, щоб запобігти майбутнім аваріям [34].

Мережі Петрі та її модифікації (розширені мережі Петрі) використовуються для аналізу продуктивності та стійкості телекомунікаційних мереж [35], моделювання та аналізу складної динаміки в розумних електромережах (Smart Grid): управління (management), надійність (reliability), networking та безпека (запобігання можливим каскадним ефектам) [33]. Вибір типу МП залежить від вимог і характеристик системи. Але при збільшені кількості компонентів системи та їхніх зв'язків збільшується складність та підтримка МП, ризик можливої помилки при змінах в існуючій моделі.

Ланцюги Маркова (Markov chains)

Ланцюг Маркова (ЛМ) — це математична модель стохастичного процесу, який моделює послідовність можливих подій, де ймовірність кожної події залежить лише від стану, досягнутого в попередній події. У контексті каскадних ефектів ЛМ використовуються для моделювання ймовірнісної поведінки відмов, що поширюю-

ться критичною інфраструктурою. Представляючи стани та переходи в КІ, дослідники можуть аналізувати, наскільки ймовірно, що збій в одній частині КІ спричинить наступні збої, що призведе до каскаду. ЛМ використовується для оцінки стохастичних процесів, аналізу надійності комплексних систем, прогнозування ланцюгів каскадних збоїв в енергосистемах [37].

Для спрощення моделювання і аналізу каскадних ефектів використовуються interaction graphs, за допомогою яких зображають базові взаємодії і впливи між компонентами під час каскадних ефектів (рис. 5). При моделюванні та аналізу розвитку розміру каскадів використовується модель ланцюга Маркова із використанням community structures у графі взаємодії електромережі [38]. Ланцюг Маркова визначається як послідовність випадкових величин $\{X_1, X_2, X_3, \dots\}$, яка задовольняє Марківську властивість: імовірність переходу до наступного стану (X_{t+1}) залежить лише від поточного стану (X_t — стан у момент часу t, де $t \in N$), а не від попередніх ($X_{t-1}, X_{t-2}, \dots$) описується за допомогою матриці перехідних імовірностей:

$$P(X_{t+1} = x_{t+1} \mid X_t = x_t, \dots, X_1 = x_1) = P(X_{t+1} = x_{t+1} \mid X_t = x_t). \quad (12)$$

Методологія дослідження каскадних ефектів КІ за допомогою ланцюгів Маркова передбачає послідовність кроків, яка охоплює всі етапи, починаючи із визначення цілей дослідження та закінчуючи звітністю. Отже етапи дослідження каскадних ефектів за допомогою ланцюгів Маркова включають:

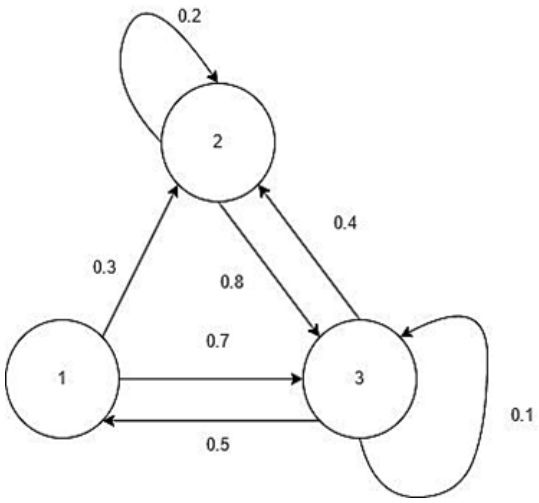

Рис. 5. Приклад ланцюга Маркова

— визначення особливостей КІ та розуміння типу та динаміки розповсюдження каскадного ефекту (наприклад, електромережі, транспортні мережі). На підставі розуміння особливостей предметної області встановлюються цілі аналізу, такі як прогнозування ймовірності відмови, розуміння або розробка стратегій пом'якшення;

— визначення змінних, які описують усі стани КІ, зокрема, в електромережі стани можуть представляти робочий, несправний різних компонентів (ліній, трансформаторів). Обов'язково визначається простір станів, який включає всі можливі комбінації цих змінних;

— формування ймовірності переходів КІ з одного стану в інший на основі попередніх подій відмови. Ці ймовірності можна отримати з історичних даних (бази знань — накопиченого досвіду), експертних оцінок або онтології. Цей етап також передбачає чітке розуміння того, як відмова одного компонента впливає на інші, враховуючи взаємозалежності між компонентами;

— побудову математичної моделі ЛМ (графа переходів), де стани моделі представляють різні ймовірності переходів (сценарії розвитку каскадних процесів) залежно від значень початкових відмов (тригерних подій) і призводять до наступних відмов на основі визначених імовірностей;

— аналіз динаміки переходів для розуміння, як збої поширюються в КІ з часом. Для цього використовуються рекурсивні алгоритми для обчислення ймовірностей переходу і управління складністю простору станів через потенційне експоненціальне зростання в каскадних сценаріях. Це передбачає визначення нескінченно малої генераторної матриці, яка фіксує швидкості переходів між станами;

— моделювання та тестування різних сценаріїв відмов за допомогою моделі ЛМ, щоб спостерігати, як каскадні ефекти розгортаються за різних умов (наприклад, випадкові початкові відмови, цілеспрямовані атаки). Оцінка таких результатів моделювання як розмір каскаду та час відновлення, щоб зрозуміти стійкість системи;

— формування прогнозів сценаріїв розвитку на основі оцінки ймовірності різних наслідків каскаду та їхній вплив на стійкість КІ. Для цього можуть використовуватися такі показники як імовірність зупинки каскаду, щоб охарактеризувати, наскільки ймовірно припинення каскаду після досягнення певного стану;

— формування управлінських рішень, спираючись на знання, що отримані в результаті моделювання та аналізу, розробляються стратегії пом'якшення каскадних ефектів. Це може передбачати посилення критичних компонентів або впровадження систем моніторингу в реальному часі;

— перевірку і аналіз чутливості моделі ЛМ з метою визначення, як зміни ймовірностей переходів або початкових умов впливають на каскадну поведінку порівняно з реальними даними або накопиченими знаннями про події, щоб забезпечити точність моделі;

— вироблення рекомендацій щодо підвищення стійкості КІ до каскадних збоїв.

Використання ланцюгів Маркова у вивченні каскадних ефектів забезпечує структурований підхід до розуміння складних взаємодій між компонентами КІ. Дотримуючись цих кроків, дослідники можуть ефективно моделювати і аналізувати, як початкові збої поширюються через взаємопов'язані мережі, що призводить до цінних ідей для управління ризиками та підвищення стійкості систем критичної інфраструктури.

Порівняння можливостей мереж Петрі та Маркова при дослідженні каскадних ефектів

Як мережі Петрі $PN = (P, T, F, W, M_0)$, так і мережі Маркова є потужними інструментами для дослідження каскадних ефектів, але вони суттєво відрізняються за можливостями моделювання, областями фокусування та тим, як вони обробляють динаміку складних систем. Їх можна порівняти за наступними факторами.

А. Структура та представлення моделі.

Мережі Петрі — це інструмент графічного та математичного моделювання, який використовується для опису дискретних систем, де стани та події мають бути представлені явно. Каскадні ефекти можна моделювати, показуючи, як подія в одній частині системи викликає переходи в іншій. Мережі Маркова базуються на ймовірнісних переходах між станами, де майбутній стан залежить лише від поточного стану (властивість Маркова), тому вони зосереджуються на переходах між станами, а не на конкретних подіях. Це робить їх більш абстрактними порівняно з мережами Петрі, які явно моделюють причинно-наслідкові події.

B. Обробка каскадних ефектів.

Мережі Петрі явно моделюють причинно-наслідкові залежності між подіями, дозволяючи детально відстежувати, як один збій призводить до іншого. Наприклад, при каскадному збої в електромережі кілька одночасних перевантажень можна моделювати одночасними переходами в МП. Мережі Маркова фіксують імовірність того, що один стан (наприклад, несправний компонент) призведе до іншого (наприклад, відмови сусідніх компонентів). Це робить їх ефективними для кількісної оцінки ризику в КІ, де каскадні збої є стохастичними, дозволяючи дослідникам обчислити ймовірність досягнення системою критичного збою після каскадних ефектів.

C. Дослідження одночасних події.

Мережі Петрі дозволяють моделювати синхронізацію подій, додаючи часовий вимір до аналізу каскадних ефектів. Це корисно для дослідження КІ, в яких час виникнення збоїв впливає на загальний результат (наприклад, наскільки швидко один збій поширюється на інші). Моделі ЛМ менш підходять для обробки одночасних подій оскільки вони зосереджені на послідовних переходах між станами, тобто одночасні збої або події важче моделювати. Тобто ЛМ не вистачає явних можливостей паралелізму та синхронізації порівняно з МП.

D. Можливості аналітики та моделювання.

Мережі Петрі пропонують як якісний (структурні властивості — доступність, живучість), так і кількісний аналіз ефективності з часовим поясненням. Моделювання допомагає визначити вузькі місця, точки збоїв або місця, де каскадні ефекти можуть посилитися. Моделі Маркова в основному використовуються для кількісного ймовірнісного аналізу, що робить їх ідеальними для вивчення ймовірності каскадних відмов і розрахунку ймовірностей різних станів відмов поряд з розрахунком очікуваного часу до виникнення відмови.

Байєсовські мережі (BN) можуть бути більш ефективними, ніж ланцюги Маркова, у кількох сценаріях моделювання каскадних ефектів, зокрема завдяки їхній здатності обробляти складні залежності та невизначеності.

Порівняння можливостей моделювання каскадних ефектів методами Баєса, мережами Маркова та Петрі наведено в таблиці.

Характеристика	**Мережа Баєса**	**Ланцюг (мережа) Маркова**	**Мережа Петрі**
Тип моделі	Баєсовська мережа описує умовні залежності через орієнтований ациклічний граф (DAG), що дозволяє чітко зрозуміти, як стан однієї змінної впливає на інші.	Створює ймовірнісну (стохастичну) модель каскаду, на основі можливих станів подій у каскаді (експертна оцінка, накопичений досвід, онтології)	Формує графічну модель каскаду, на основі причинно-наслідкового опису події, процесів які викликають каскад
Можливість обробки паралельних процесів	Обмежена можливість, оскільки метод зосереджується на моделюванні умовних залежностей між подіями	За своєю суттю метод не призначений для паралельності, фокусується на переходах станів	Метод відмінно моделює паралельні процеси та їхню взаємодію на основі причинно-наслідкового опису події
Динамічне моделювання поведінки КІ	Може моделювати динамічні зміни в КІ за допомогою динамічних байєсівських мереж	Моделі каскаду можуть розрахувати зміни з часом, але не можуть дати чіткого представлення	Мережа може ефективно моделювати динамічну поведінку та каскадні події з часом

Характеристика	Мережа Баєса	Ланцюг (мережа) Маркова	Мережа Петрі
	(DBN) або БМ безперервного часу (CTBN)	при моделюванні одночасних подій в КІ	
Представлення сценаріїв розвитку каскадних ефектів	Може фіксувати каскадні ефекти через імовірнісні залежності, але це може потребувати складних структур для опису взаємодій	Моделює каскадні збої як серію переходів станів на підставі таблиць імовірності. Метод ефективний для простих сценаріїв поширення каскаду	Надає чітке візуальне уявлення про різні сценарії розвитку каскаду на підставі причинно-наслідкових залежностей, тобто як початкові збої призводять до наступних збоїв через переходи
Імовірнісний аналіз виникнення каскаду	Аналіз виникнення каскаду на основі розрахунку через імовірнісні залежності події. Також може кількісно визначити невизначеність каскадних ефектів.	Модель дозволяє проводити кількісний аналіз імовірностей переходів на основі експертних оцінок або накопиченого досвіду	Обмежені ймовірнісні можливості, якщо їх не поширити на ймовірнісні мережі Петрі (PPN)
Ідентифікація критичних компонентів	Визначає критичні стани, які можуть ініціювати каскади за допомогою ймовірнісного висновку.	Може ідентифікувати критичні стани, аналізуючи ймовірності переходу, але не має прямого представлення компонентів.	За допомогою структурного аналізу ідентифікує критичні компоненти, несправність яких може призвести до значних впливів.
Сфера застосування	БМ надає інструментарій для вивчення каскадних ефектів у широкому діапазоні областей, від енергетичних систем до транспортних, соціальних, фінансових та екологічних. Їхня перевага полягає в моделюванні ймовірнісних зв'язків і невизначеності, що важливо для КІ, де каскадні збої відбуваються за невизначених умов.	Універсальний інструмент для вивчення каскадних ефектів у КІ, де локальні взаємодії та залежності є ключовими факторами поширення збоїв або подій у таких сферах як КІ, електромережі, комп'ютерні та соціальні мережі, де стан кожного вузла значною мірою залежить від сусідніх вузлів.	МП дозволяє моделювати одночасні процеси та взаємодії, що особливо цінне для розуміння складних систем, де каскади можуть швидко поширюватися у різних областях (хімічні процеси, оцінку безпеки, виробництво, транспорт, телекомунікації та біологічні системи).

Байєсовські мережі особливо ефективні в сценаріях, що включають складні взаємозалежності, невизначеність, динамічні зміни та причинно-наслідкові зв'язки під час вивчення каскадних ефектів. Їхня ймовірнісна структура та графічне представлення роблять їх потужним інструментом для розуміння та прогнозування того, як збої поширюються через взаємопов'язані системи, порівняно з ланцюгами Маркова, які можуть бути більш придатними для простіших сценаріїв із чітко визначеними переходами між станами.

Ланцюги Маркова чудово підходять для кількісного аналізу переходів станів і ефективні для простих каскадних сценаріїв, але можуть мати проблеми зі складними взаємозалежностями. Вони краще підходять для кількісного визначення ймовірності відмови і аналізу довгострокової поведінки каскадних систем.

Мережі Петрі забезпечують надійну структуру для моделювання одночасних процесів і візуалізації динаміки каскадних відмов, що робить їх ідеальними для розуміння складних взаємодій у системах, таких як електромережі чи хімічні процеси.

Вибір методу моделювання залежить від характеру каскадних ефектів, що досліджуються, а саме — якщо увагу зосереджено на детальному моделюванні причинно-наслідкових зв'язків — мережі Петрі, або більш зацікавлені в імовірнісній оцінці переходів при виникненні каскаду — мережі Маркова. Баєсовська мережа описує умовні залежності через орієнтований ациклічний граф і зосереджується на моделюванні умовних залежностей між подіями, використовуючи механізм умовних імовірностей виникнення події залежно від стану попереднього вузла.

Онтологія критичної інфраструктури

Для аналізу процесів розвитку каскадних ефектів доцільно використовувати їхню семантику, застосовуючи накопичений досвід у предметній області — знання, що надають можливість будувати сценарії розвитку каскадних ефектів і розробляти рішення для пом'якшення наслідків. Аналіз предметної області, структурування знань, їхнє зберігання та візуалізація полегшують процес розробки програмного забезпечення [45–47] для дослідження каскадних ефектів у КІ.

Онтологія — формалізоване представлення знань про певну предметну область [48, 49] містить: класи або поняття (classes/concepts), відношення (relations), функції (functions), аксіоми, екземпляри. Залежно від мети та цілей дослідження використовуються різні типи онтологій: Knowledge Representation, General/Common ontologies, Top-Level Ontologies, Meta-ontologies, Domain ontologies, Illustrative linguistic ontologies, Task ontologies, Domain-Task ontologies, Method ontologies, Application ontologies [50].

При розробці онтології використовується ітеративний підхід [49], який складається з таких кроків:

1) визначити домен і область онтології;

2) розглянути можливість повторного використання існуючих онтологій;

3) перелічити важливі терміни онтології;

4) визначити класи та ієрархію класів;

5) визначити властивості класів;

6) визначити обмеження властивостей;

7) створити екземпляри для наповнення бази знань.

Іншим підходом для прискорення розробки онтології є застосування відомого інструментарію METHONTOLOGY [51]. Процес розробки онтології за цією методологією включає:

1) *формування специфікації*: тобто визначення вимог до онтології, які враховують особливості предметної області;

2) *набуття знань*: вивчення різних джерел знань для розуміння предметної області та визначення термінів (формування таксономії), які описують відношення між об'єктами;

3) *концептуалізація*: структурування знання про предметну область у концептуальній моделі, яка описує проблему та її рішення;

4) *інтеграція*: повторне використання існуючих онтологій у можливих ситуаціях;

5) *реалізація*: перетворення результатів у формальну мову;

6) *оцінка*: перевірка коректності онтології;

7) *документація*: відбувається протягом усього процесу життєвого циклу розроблення функціоналу.

Враховуючи запропоновані методології була розроблена загальна онтологія критичної інфраструктури, яка дозволяє адаптувати її для визначеної предметної області (**subject domen, SD)**. Таксономія класів — це дерево термінів (класів предметної області), яке має ієрархічну структуру та містить такі основні класи (сутності) предметної області як: <**КритичнаІнфраструктура>**; <**ТипПослуги>**; <**Збій>** з підкласами <Каскадний>, <Зростаючий>, <Звичайний>; **<Сектор**>; **<Метрика>;** <**Подія>** з підкласами <Антропогенна>, <Техногенна>, <Природна>; **<Підсектор>** з підкласами <КомунальніПослуги>, <Електроенергетика> та багато інших сутностей і відношень між ними.

На рис. 6 наведено фрагмент графа онтології, яка описує сутності предметної області <Критична інфраструктура>. Відображення графа онтології отримано завдяки використанню редактора онтології Protégé 5 в інструментальній панелі **<Візуалізація**>.

Окрім основних класів (концептів) кожна онтологія описується через їхні властивості <Data properties>, <Object properties> та властивості екземплярів <Individuals>. Саме ці механізми і визначають атрибути властивостей класів і відношення між класами в будь-якій онтології. При опису відношень між класами <Object Properties> залучаються механізми формування предикатів мови OWL2 у вигляді дієслів. Назва предиката враховує функціональність відношень між концептами КІ, наприклад, <МаєМетрикуКритичності> або **<**маєМетрикуРизику**>** та багато інших властивостей, що визначають відношення між класами онтології у визначеній предметної області. На рис. 7 наведено приклад опису властивостей класів онтологічної моделі через механізми <Data properties> та <Object properties>.

Для побудови запитів щодо отримання знань з онтології використовують мови формування запитів SPARQL або DL Query. Приклад запиту DL Query для пошуку об’єктів, які відносяться до 1 категорії критичності:

маєЗначенняКритичності some xsd:double[> "0.8"^^xsd:double , <= "1.0"^^xsd:double].

За допомогою запитів можливо детальніше дослідити зв’язки та властивості класів, екземплярів, що може бути корисним при створенні аналітичних моделей у вигляді мережі. Застосування сценаріїв надає можливість розгляду кількох імовірних варіантів розвитку подій (каскадних збоїв) при прийнятті рішень у динамічному середовищі, враховуючи невизначеності та ризики критичної інфраструктури.

Одним із підходів для формування сценаріїв аналітичної діяльності є використання методології на основі онтології, її адаптації до специфіки задач предметної області [45]. При моделюванні сценаріїв прийняття рішень використовуються BPMN, Knowledge Graph та OWL-моделі для забезпечення семантичного аналізу сценарію, що допомагає уникнути помилок, які пов’язані із семантичною сумісністю компонентів. Методологія процесно-орієнтованого моделювання складних сценаріїв на основі BPMN 2.0, використання знання-орієнтованих інструментів Knowledge Graph NEO4J+Cypher та онтології OWL-Protégé допомагає зменшити кількість помилок, які виникають при опису предметної області аналітиком [46].

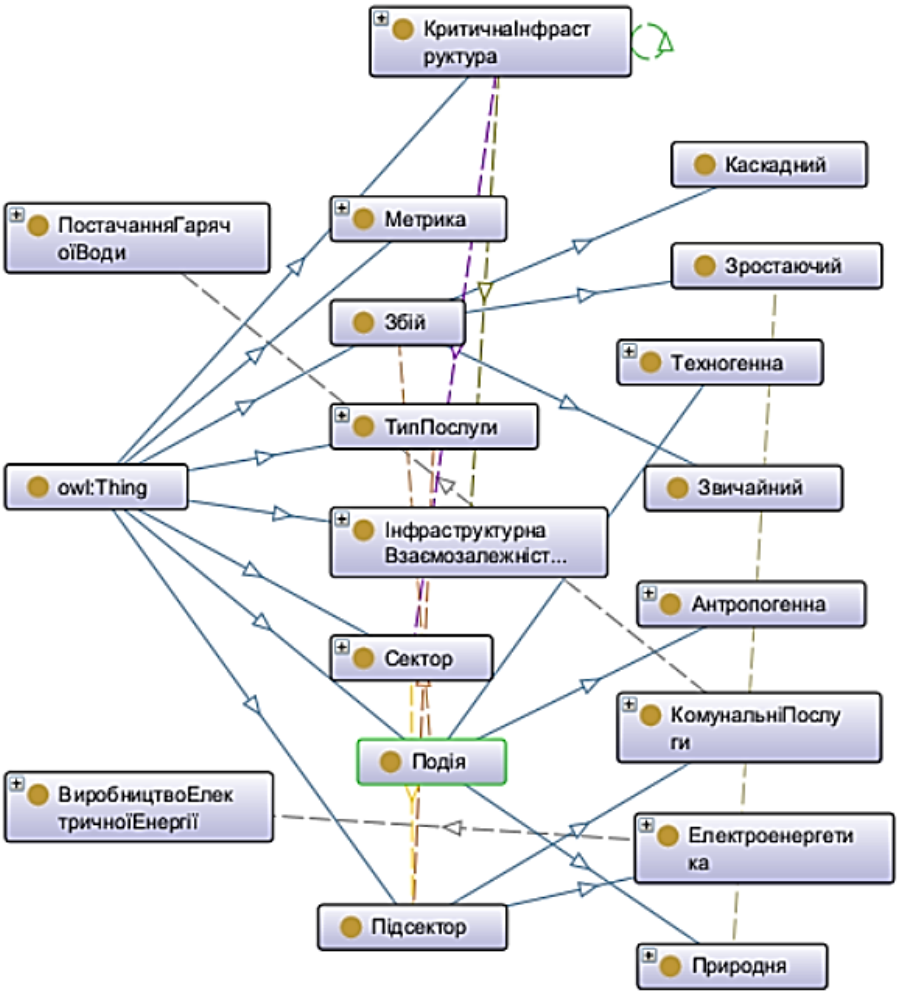

Рис. 6. Граф онтології критичної інфраструктури

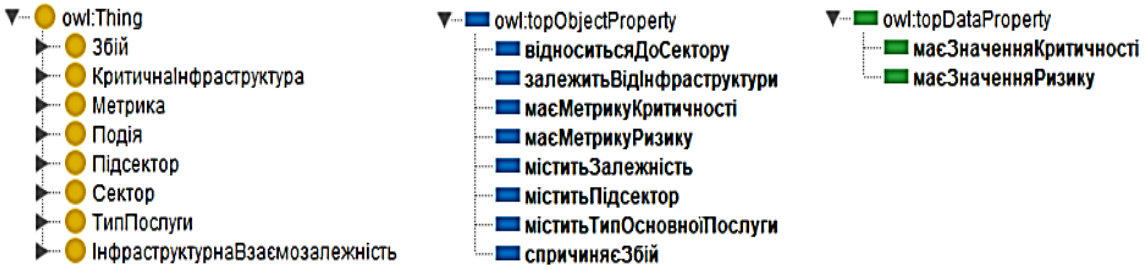

Рис. 7. Приклад опису властивостей класів онтології критичної інфраструктури

Стійкість інфраструктури

Аналіз стійкості КІ є важливим чинником для прийняття рішень, оцінки витрат у можливих сценаріях розвитку каскадних процесів. У контексті критичної інфраструктури для оцінки кількісних і якісних аспектів поведінки системи та стійкості до функціональних збоїв доцільно використовувати Криві стійкості. Ці криві

важливі для розуміння того, як КІ може протистояти каскадним ефектам, відновлюватися та адаптуватися до них. Вони відносяться до графічних засобів аналізу складних систем, які ілюструють стійкість систем з часом, особливо у відповідь на збої. Основною метою застосування цих кривих є кількісна оцінка стійкості КІ шляхом аналізу емпіричних даних про перерви в штатному функціонуванні КІ, включаючи їхню тривалість і наслідки.

Найбільш продуктивною є концептуальна модель стійкості у вигляді Трапеції багатофазної стійкості (The multi-phase resilience trapezoid), яка використовується для оцінки стійкості КІ, зокрема у відповідь на руйнівні наслідки від каскадних ефектів. Ця модель покращує традиційні оцінки стійкості шляхом включення кількох фаз продуктивності інфраструктури під час і після порушень. Трапеція стійкості складається з трьох фаз (рис. 8) [11]: 1) прогрес збою (disturbance progress); 2) погіршений стан після збою (post-disturbance degraded); 3) стан відновлення (restorative state).

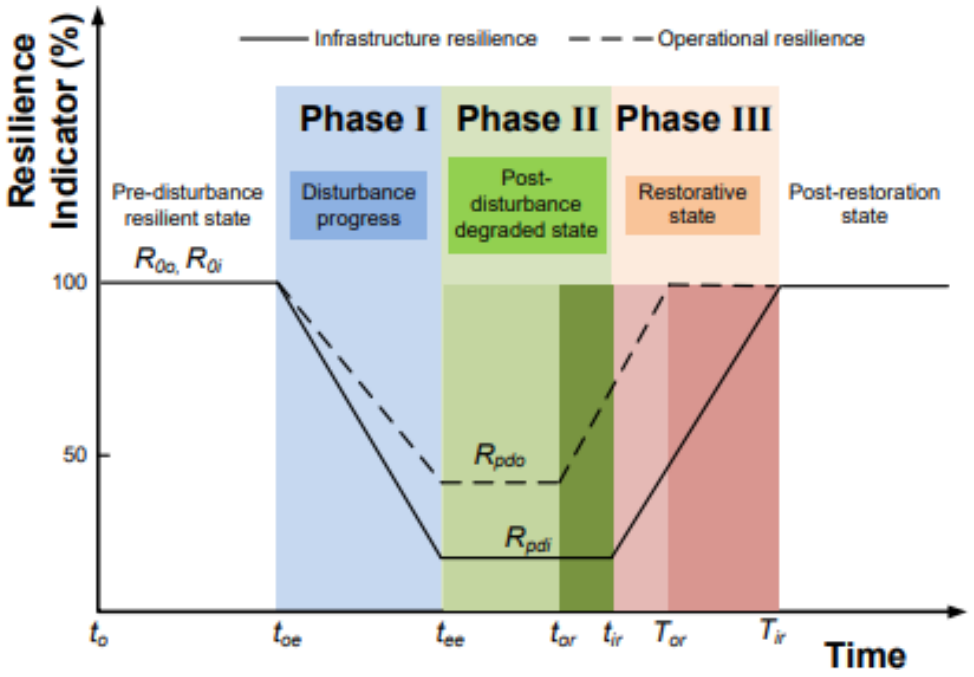

Рис. 8. Трапеція багатофазної стійкості (The multi-phase resilience trapezoid) [11]

Для оцінки якості моделі стійкості КІ використовуються ряд метрик (рис. 9). Ці показники допомагають кількісно визначити, наскільки добре інфраструктура може протистояти збоям і відновлюватися після них. Метрики продуктивності розташовані на вертикальній осі кривої стійкості, а на горизонтальній — час та поділені на три категорії: доступність (availability), продуктивність (productivity), якість (quality), але кілька метрик можуть бути об'єднані в ансамблеву (ensemble) метрику [13]. Одним із підходів до оцінки стійкості є використання фреймворку на основі концепції трапеції стійкості, що описує фази, в яких може перебувати критична інфраструктура, переходи між цими станами.

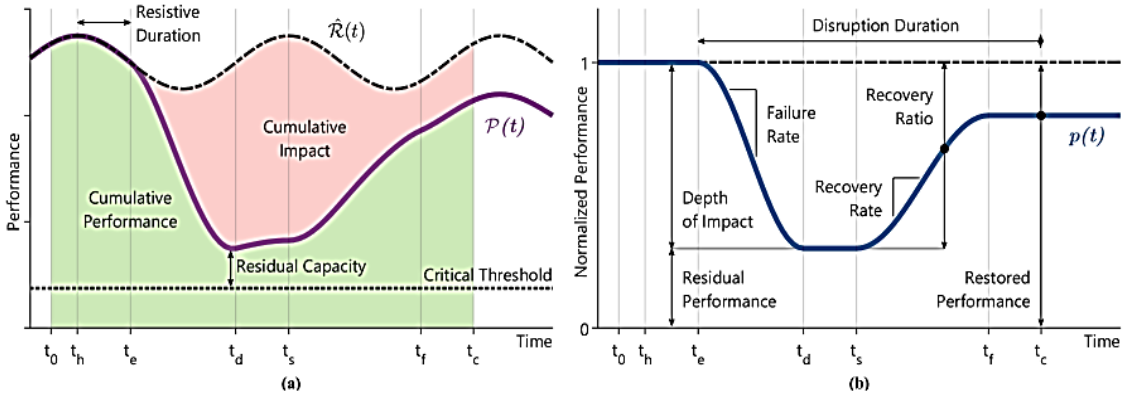

Рис. 9. Метрики для кривої стійкості: а) у фактичних одиницях (actual units); б) у нормалізованих одиницях (normalized units) [13]

Для визначення стійкості енергосистеми використовується набір метрик стійкості «ФΛЕП» [11], де:

Ф: швидкість зменшення стійкості (I фаза);

Λ: рівень падіння стійкості (I фаза);

Е: час, протягом якого система залишається в стані погіршення (фаза II) після збою;

П: швидкість відновлення системи до стану стійкості, до виникнення збою (фаза III).

На основі метрик «ФΛЕП» можливо обчислити площу трапеції — додаткову метрику для оцінки стійкості інфраструктури та впливу різних стратегій підвищення інфраструктурної та операційної стійкості [11].

Для порівняння стійкості однієї системи до різних збоїв або різних систем до одного збою використовується загальна метрика стійкості (GR), яка базується на кількісній оцінці основних можливостей системи [12]. GR може застосовуватися для порівняння різних стратегій покращення стійкості: в результаті більш ефективні стратегії повинні збільшити значення GR, більш стійка система має більш високе значення GR.

Програмні засоби для аналізу ефекту доміно та каскадних ефектів

На даний час для аналізу складних динамічних систем на ринку інформаційних технології існують методології, програмні засоби та інструменти, які дозволяють суттєво скоротити сам процес моделювання і аналізу каскадних події для КІ. Найбільш відомими є таки засоби: The Neo4j Graph Data Science Library, MAXCRED, DOMIFFECT, ARIPAR, ATLANTIDE, DOMINOXL, GeOsiris, MiniFFECT, DomPrevPlanning [39]. Для аналізу каскадних збоїв в електромережах використовується MATCASC — інструмент на основі MATLAB, який має функціонал для: оцінки потоку електроенергії у лінії, оцінки пропускної здатності лінії, застосування варіантів видалення лінії (випадкове або на основі атаки), моделювання каскадних відключень через перевантаження лінії, визначення збитків через каскадні збої [8]. Для аналізу, оцінки вразливості, міцності графів є обмежена кількість доступних (відкритих) програмних рішень, які мають різноманітний функціонал.

Tiger — відкритий набір інструментів (toolbox), розроблений на Python для оцінки вразливості та міцності графів (функціональні можливості описано в документації, є приклади використання), який містить: 22 показники надійності графа з оригінальними та швидкими наближеними версіями; 17 стратегій збоїв та атак; 15 евристичних та оптимізаційних методів захисту; 4 інструменти симуляції [40].

Протягом останніх років машинне навчання (machine learning) та глибоке навчання (deep learning) стрімко розвиваються, з'являються нові підходи, методи, які можуть бути використані для аналізу каскадних збоїв у енергосистемах [41]. Нейронні мережі можна масштабувати для обробки великих наборів даних, адаптувати до різних завдань, змінивши архітектури, функції активації або методи навчання. Але вони мають і недоліки: перенавчання (наприклад, навчальні дані обмежені), складність навчання (обчислювальні ресурси для великих моделей), чутливість до гіперпараметрів (наприклад, архітектура мережі та функції активації). Але попри описані недоліки нейронні мережі мають великий потенціал для розв'язання складних задач.

Для прогнозування каскадних збоїв використовують графові нейронні мережі (Graph Neural Networks) [42]. Модель GNN демонструє точність (accuracy) та збалансовану точність (balanced accuracy) понад 96 % на тестових даних і використовується в прогнозуванні каскадних збоїв в електромережах у режимі реального часу [43]. Оскільки зв'язки в критичній інфраструктурі стають дедалі складнішими, збільшується масштабування об'єктів, логіка їхньої взаємодії стає складнішою, тому використання методів машинного навчання або глибокого навчання є перспективним напрямком дослідження. Розробка інструментарію (програмного забезпечення) для аналізу великих обсягів даних за допомогою моделей машинного або глибокого навчання потенційно може допомогти вирішити прогалини в аналізі каскадних збоїв в інфраструктурі: моніторинг, аналіз подій і прийняття рішень на різних етапах розвитку каскадних збоїв.

Висновки

Захист КІ є важливою та комплексною задачею, для розв'язання якої потрібно проаналізувати предметну область, визначити характеристики об'єктів, зв'язки між ними, виявити вплив подій на функціонування об'єктів. Враховуючи складність більшості існуючих в Україні КІ, найбільш доцільним є мережевий підхід, який дозволяє представити КІ у вигляді мережі (графа), використовуючи різноманітні методи аналізу і оцінки поведінки КІ при виникненні каскадних ефектів.

Для аналізу та моделюванню каскадних збоїв у КІ запропоновано алгоритми теорії графів, мережі Баєса, мережі Петрі, ланцюги Маркова. Проведено порівняльний аналіз можливостей та особливостей застосування цих методів при дослідженні каскадних ефектів КІ. Доведено, що вибір методу моделювання залежить від характеру каскадних ефектів, наприклад, якщо зосереджено увагу на детальному моделюванні причинно-наслідкового опису події каскадного ефекту — мережі Петрі, якщо увага приділяється оцінки ймовірнісних переходів станів вузлів КІ при виникненні каскаду — мережі Маркова.

Одним із шляхів для покращення розуміння особливостей функціонування КІ є побудова її онтології, яка зосереджує увагу на накопиченому досвіді. Це надає

можливість на основі наявних знань формувати більш реалістичні сценарії виникнення та розвитку каскадних збоїв у певній КІ. Також, завдяки накопиченим знанням, краще формувати управлінські рішення як у разі запобігання виникненню каскадних збоїв, так і усунення їхніх наслідків.

Більшість існуючих програмних засобів для моделювання і аналізу каскадних/доміно ефектів використовуються для конкретної (однієї) галузі критичної інфраструктури, враховуючи особливості процесів, і потребують додаткового налаштування, впровадження на об'єктах. Методи і алгоритми, які використовуються в аналізі властивостей КІ (мережі), сценаріїв розвитку каскадних ефектів (ефект доміно) мають переваги та недоліки, тому питання створення нових підходів для збільшення стійкості мережі і досі є актуальним.

Технології, алгоритми, підходи до розробки програмного забезпечення стрімко розвиваються, що робить можливим покращення існуючих рішень — створення програмного забезпечення для аналізу каскадних ефектів зі збільшеною точністю результатів, зменшенням часу на виконання обчислень, гнучким функціоналом налаштування, можливістю для розширення та інтеграції для застосування в різних секторах КІ, в процесі розгляду каскадних ефектів одночасно для декількох взаємопов'язаних критичних інфраструктур.

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

2. Rinaldi S.M., Peerenboom J.P., Kelly T.K. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*. 2001. **21**(6). P. 11–25. DOI:10.1109/37.969131.

3. Kadri F., Birregah B., Châtelet E. The Impact of Natural Disasters on Critical Infrastructures: A Domino Effect-based Study. *Journal of Homeland Security and Emergency Management, De Gruyter*. 2014. **1**1(2). P. 217–241. DOI:10.1515/jhsem-2012-0077.

4. Darbra R.M., Palacios A., Casal J. Domino effect in chemical accidents: main features and accident sequences. *Journal of Hazardous Materials*,. 2010. **83**(1–3). P. 565–573. https://doi.org/10.1016/j.jhazmat.2010.07.061.

5. Chen C., Reniers G., Khakzad N. A thorough classification and discussion of approaches for modeling and managing domino effects in the process industries. *Safety Science*. 2020. **125**. P. 1–23. https://doi.org/10.1016/j.ssci.2020.104618.

6. Закон України «Про об'єкти підвищеної небезпеки» № 2245-III від 18.01.2001. URL: https://zakon.rada.gov.ua/laws/show/2245-14#Text

7. Kinney R., Crucitti P., Albert R., Latora V. Modeling cascading failures in the North American power grid. *The European Physical Journal B-Condensed Matter and Complex Systems*. 2005. **46**(1). P. 101–107. DOI:10.1140/epjb/e2005-00237-9.

8. Koç Y., Verma T., Araujo N.A.M., Warnier M. MATCASC: A tool to analyse cascading line outages in power grids. 2013 IEEE International Workshop on Inteligent Energy Systems (IWIES). 2013. P. 143–148. https://doi.org/10.1109/IWIES.2013.6698576.

9. Magdi S. Mahmoud, Yuanqing Xia. Cascading failures in power grids. *IEEE Potentials*. 2019. **28**(5). P. 24–30. https://doi.org/10.1109/MPOT.2009.933498.

10. Xie B., Tian X., Kong L., Chen W. The Vulnerability of the Power Grid Structure: A System Analysis Based on Complex Network Theory. *Sensors.* 2021. **21**(21):7097. https://doi.org/10.3390/s21217097.

11. Panteli M., Mancarella P., Trakas D. N., Kyriakides E., Hatziargyriou N.D. Metrics and Quantification of Operational and Infrastructure Resilience. Power Systems. *IEEE Transactions on Power Systems*. 2017. **32**(6). P. 4732–4742. https://doi.org/10.1109/TPWRS.2017.2664141.

12. Nan C., Sansavini G., Kröger W., Heinimann H.R. A Quantitative Method for Assessing the Resilience of Infrastructure Systems. Proceedings of the Probabilistic Safety Assessment and Management Conference, PSAM12, 2014.

13. Poulin C., Kane M.B. Infrastructure resilience curves: Performance measures and summary metrics. *Reliability Engineering & System Safet.* December 2021. Vol. 216, 107926. https://doi.org/10.1016/j.ress.2021.107926.

14. The total amount of damage caused to Ukraine's infrastructure due to the war has increased to almost $138 billion. 24 January 2023. URL: https://kse.ua/about-the-school/news/the-total-amount-of-damage-caused-to-ukraine-s-infrastructure-due-to-the-war-has-increased-to-almost-138-billion/

15. Hern´andez J.M., Mieghem P.V. Classification of graph metrics. 2011. URL: https://www.nas.ewi.tudelft.nl/people/Piet/papers/TUDreport20111111_MetricList.pdf

16. Oehlers M., Fabian B. Graph Metrics for Network Robustness — A Survey. *Mathematics.* 2021. **9**(8). 895. https://doi.org/10.3390/math9080895.

17. Di Nardo A., Giudicianni C., Greco R., Herrera M., Santonastaso G.F. Applications of Graph Spectral Techniques to Water Distribution Network Management. Water. 2018. **10**(1):45. https://doi.org/10.3390/w10010045.

18. Puuska S., Kansanen K., Rummukainen L., Vankka J. Modelling and real-time analysis of critical infrastructure using discrete event systems on graphs. 2015 IEEE International Symposium on Technologies for Homeland Security (HST). DOI:10.1109/THS.2015.7225330.

19. Stergiopoulos G., Kotzanikolaou P., Theocharidouc M., Gritzalis D. Risk mitigation strategies for critical infrastructuresbased on graph centrality analysis. *International Journal of Critical Infrastructure Protection*. September 2015. **10**. P. 34–44. DOI:10.1016/j.ijcip.2015.05.003.

20. Guze S. Graph Theory Approach to the Vulnerability of Transportation Networks. *Algorithms*. 2019. **12**(12):270. https://doi.org/10.3390/a12120270.

21. Zelin Wan, Yash Mahajan, Beom Woo Kang, Terrence J. Moore, Jin-Hee Cho. A Survey on Centrality Metrics and Their Implications in Network Resilience. https://doi.org/10.1109/ACCESS. 2021.3094196.

22. Cuadra L, Salcedo-Sanz S, Del Ser J, Jiménez-Fernández S, Geem ZW. A Critical Review of Robustness in Power Grids Using Complex Networks Concepts. *Energies*. 2015. **8**(9). P. 9211–9265. https://doi.org/10.3390/en8099211.

23. Vaniš M, Lokaj Z, Šrotýř M. A Novel Algorithm for Merging Bayesian Networks. Symmetry. 2023. **15**(7):1461. https://doi.org/10.3390/sym15071461.

24. Daly R, Qiang S & Aitken S. Learning Bayesian Networks: Approaches and Issues. *Knowledge Engineering Review.* 2011. Vol. 26, No. 2. P. 99–127. https://doi.org/10.1017/S0269888910000251.

25. Srinivas S. A Generalization of the Noisy-Or Model. Proceedings of the Ninth Conference on Uncertainty in Artificial Intelligence. 1993. P. 208–215. https://doi.org/10.1016/B978-1-4832-1451-1.50030-5.

26. Kitson N.K., Constantinou A.C., Zhigao G., Liu Y., Chobtham K. A survey of Bayesian Network structure learning. *Artificial Intelligence Review.* 2023. **56**. P. 8721–8814. DOI:10.1007/s10462-022-10351-w.

27. Khakzad N. A Tutorial on Fire Domino Effect Modeling Using Bayesian Networks. *Modelling*. 2021. **2**(2). P. 240–258. https://doi.org/10.3390/modelling2020013.

28. Cerotti D., Codetta-Raiteri D., Dondossola G., Egidi L., Franceschinis G., Portinale L., Terruggia R. Evidence-Based Analysis of Cyber Attacks to Security Monitored Distributed Energy Resources. *Applied Sciences.* 2020. **10**(14):4725. https://doi.org/10.3390/app10144725.

29. Wright M, Chizari H, Viana T. A Systematic Review of Smart City Infrastructure Threat Modelling Methodologies: *A Bayesian Focused Review. Sustainability*. 2022. **14**(16):10368. https://doi.org/10.3390/su141610368.

30. Eldosouky A., Saad W., Mandayam N. Resilient Critical Infrastructure: Bayesian Network Analysis and Contract-Based Optimization. *Reliability Engineering & System Safety*. January 2021. Vol. 205, 107243. https://doi.org/10.1016/j.ress.2020.107243.

31. He X. A comprehensive survey of petri net modeling in software engineering. *International Journal of Software Engineering and Knowledge Engineering*. 2013. **23**(5). P. 589–625. DOI: 10.1142/S021819401340010X.

32. Murata T. Petri nets: properties, analysis and applications. Proceedings of the IEEE. 1989. **77**(4). P. 541–580. DOI: 10.1109/5.24143.

33. Ge M., Rossi B., Chren S., Blanco J.M. Petri Nets for Smart Grids: The Story So Far. SAC'24: Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing, 2024. P. 661–670. https://doi.org/10.1145/3605098.3635989.

34. Kamil M.Z., Taleb-Berrouane M., Khan F., Ahmed S. Dynamic domino effect risk assessment using Petri-nets. Process Safety and Environmental Protection. April 2019. Vol. 124. P. 308–316. https://doi.org/10.1016/j.psep.2019.02.019.

35. Rui Li, Bertr Decocq, Anne Barros, Yiping Fang, Zhiguo Zeng. Petri Net-Based Model for 5G and Beyond Networks Resilience Evaluation. 25th Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN). Paris, France. Mar. 2022. P. 131–135. 10.1109/ICIN53892. 2022.9758134. hal-03648310.

36. Lu W., Besanger Y., Zamai E., Radu D. Blackouts: Description, analysis and classification. Proceedings of the 6th WSEAS International Conference on Power Systems. Lisbon, Portugal, 2006, September. P. 429–434.

37. Chao Zhai. A Robust Optimization Approach for Terminating the Cascading Failure of Power Systems. https://doi.org/10.48550/arXiv.1907.13452.

38. Nakarmi U., Rahnamay-Naeini M. A Markov Chain Approach for Cascade Size Analysis in Power Grids based on Community Structures in Interaction Graphs. 2020 International Conference on Probabilistic Methods Applied to Power Systems (PMAPS). 2020. P. 1–6. DOI:10.1109/ PMAPS47429.2020.9183579.

39. Farid Kadri, Eric Chatelet. Domino Effect Analysis and Assessment of Industrial Sites: A Review of Methodologies and Software Tools. *International Journal of Computers and Distributed Systems*. 2013. **02**(III). P. 1–10. hal-01026495f

40. Scott Freitas, Diyi Yang, Srijan Kumar, Hanghang Tong, Duen Horng Chau. Evaluating Graph Vulnerability and Robustness using TIGER. https://doi.org/10.48550/arXiv.2006.05648.

41. Naeem Md Sami, Mia Naeini. Machine Learning Applications in Cascading Failure Analysis in Power Systems: A Review. Electric Power Systems Research. July 2024. Vol. 232, 110415. https://doi.org/10.1016/j.epsr.2024.110415.

42. Chadaga S., Wu X., Modiano E. Power Failure Cascade Prediction using Graph Neural Networks. 2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Glasgow, United Kingdom, 2023, P. 1–7. https://doi.org/10.1109/SmartGridComm57358.2023.10333943.

43. Varbella A., Gjorgiev B., Sansavini G. Geometric deep learning for online prediction of cascading failures in power grids. *Reliability Engineering & System Safety*. September 2023. Vol. 237, 109341. https://doi.org/10.1016/j.ress.2023.109341.

44. More than 700 critical infrastructure facilities damaged in Ukraine since the beginning of full-scale russian invasion: Yevhenii Yenin. Ministry of Internal Affairs of Ukraine, posted 28 December 2022 11:33. URL: https://www.kmu.gov.ua/en/news/v-ukraini-z-pochatku-povnomasshtabnoho-vtorhnennia-rf-urazheno-ponad-700-obiektiv-krytychnoi-infrastruktury-ievhenii-ienin

45. Коваль О.В. Методи та засоби комп'ютерного моделювання сценаріїв аналітичної діяльності: дис. … д-ра техн. наук: 01.05.02. Київ: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, 2021. 440 с.

46. Коваль О.І., Додонов О.Г., Сенченко В.Р., Путятін В.Г., Бойченко А.В. Методологічні та технологічні аспекти комп'ютерного моделювання сценаріїв прийняття рішень. *Математичні машини і системи*. 2023. № 3. С. 65–88. ISSN 1028-9763. https://doi.org/10.34121/1028-9763-2023-3-65-88.

47. Коваль О.В., Додонов О. Г., Сенченко В.Р., Бойченко А.В. Моделювання сценаріїв аналітичної діяльності на основі нотації BPMN OWL. *Реєстрація, зберігання і оброб. даних.* 2020. Т. 22, № 1. С. 31–48. https://doi.org/10.35681/1560-9189.2020.1.1.207782.

48. Thomas R. Gruber. A translation approach to portable ontology specifications. *Knowledge Acquisition, Knowledge Acquisition*. 1993. **5**(2). P. 199–220. URL: https://tomgruber.org/writing/ ontolingua-kaj-1993.pdf.

49. Natalya F. Noy, Deborah L. McGuinness. Ontology Development 101: A Guide to Creating Your First Ontology. 2001. URL: https://protege.stanford.edu/publications/ontology_development/ontology101.pdf.

50. Asunción Gómez Pérez, V. Richard Benjamins. Overview of Knowledge Sharing and Reuse Components: Ontologies and Problem-Solving Methods. Proceedings of the IJCAI-99 workshop on Ontologies and Problem-Solving Methods (KRR5) Stockholm, Sweden, August 2, 1999.

51. M. Fernández, A. Gómez-Pérez, N. Juristo. METHONTOLOGY: From Ontological Art Towards Ontological Engineering. Spring Symposium on Ontological Engineering (AAAI): Technical Report SS-97-06, 1997.

Надійшла до редакції 03.10.2024