МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки

Кафедра комп'ютерних технологій та інформаційної безпеки

ЗАТВЕРДЖУЮ
Завідувач кафедри комп'ютерних технологій та інформаційної безпеки, к.т.н., доцент
_____ С.М. Нужний
«10» 12 2025 р.

КВАЛІФІКАЦІЙНА РОБОТА

ДОСЛІДЖЕННЯ ФАКТОРІВ ВРАЗЛИВОСТЕЙ НА ОБ'ЄКТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ З ВИКОРИСТАННЯМ МЕТОДІВ ЕКСПЕРТНОГО ОЦІНЮВАННЯ

Ступінь вищої освіти: магістр
Галузь знань: 14 Електрична інженерія
Спеціальність: 141 «Електроенергетика, електротехніка та електромеханіка»
Освітньо-професійна програма: Системи технічного захисту інформації, автоматизація її обробки

Виконав: студент 6 курсу групи 6366м
Бесідовський Вадим Вікторович _____

Керівник:
д.т.н., професор, професор кафедри комп'ютерних технологій та інформаційної безпеки

Передерій Віктор Іванович _____

Кваліфікаційна робота містить результати самостійного виконання навчального завдання. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Миколаїв – 2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки

ЗАТВЕРДЖУЮ
Гарант освітньої програми,
д.т.н., професор,
професор кафедри КТІБ
_____ Передерій В.І.
«14» 10 2025 р.

ЗАВДАННЯ

на кваліфікаційну роботу

Студент: Бесідовський Вадим Вікторович

Курс:6

Група: 6366м

Ступінь вищої освіти: магістр

Галузь знань: 14 Електрична інженерія

Спеціальність: 141 «Електроенергетика, електротехніка та електромеханіка»

Освітньо-професійна програма: Системи технічного захисту інформації, автоматизація її обробки

1. Тема роботи: Дослідження факторів вразливостей на об'єкті критичної інфраструктури з використанням методів експертного оцінювання.

затверджена наказом НУК від «14» 10 2025 р. № 1217-42

2. Вихідні дані до роботи: : моделі, методи і інформаційні технології оцінки та забезпечення стану захищеності ОКІ.

1.Провести аналіз методів і способів експертного оцінювання у дослідженні впливу факторів вразливостей на ОКІ.

2.Розробити математичну модель оцінювання залежності стійкості об'єкту критичної інфраструктури від впливу визначених факторів вразливостей.

3.Провести експерименти з оцінки впливу факторів вразливостей на об'єкт критичної інфраструктури.

4. Терміни виконання завдання:
термін видачі завдання:«01- 05» вересня 2025 р.

термін подання роботи: «18» грудня 2025 р.

6. План-графік виконання кваліфікаційної роботи

п/п	Заходи	Дата		Готовність
		Навч. тиждень	Контрольна дата	
1.	Наукове стажування	1 - 8	27.10.2025	Звіт з наукового стажування
2.	Організаційні збори	9	29.10.2025	Попередній варіант змісту КР
3.	Рубіжний контроль	10	05.11.2025	Попередній варіант оглядових розділів, звіт з практика
4.	Рубіжний контроль	13	27-28.11.2025	Доповідь на 13-ій Всеукраїнській науково-технічній конференції з міжнародною участю «СПІБТ–2025»
5.	Рубіжний контроль	14	3.12.2025	1. Попередній варіант повної КР 2. Попередній варіант презентації
6.	КЕ на рівень «магістра»	15	8,9.12.2025	Складання державного екзамену зі спеціальності на ступінь магістра
7.	Перевірка на плагіат	15	10.12.2025	Електронний варіант кваліфікаційної роботи, попередній захист (робота передається студентом на кафедру для внутрішньої рецензії).
8.	Оформлення КР та супутньої документації	16	15-17.12.2025	1. Оформлена КР (в форматі pdf) У разі отримання позитивної внутрішньої рецензії, КР подається на зовнішню рецензію. 2. Оформлена презентація (в форматі pdf).
9.	Подання документів на захист	16	18.12.2025	1. Подання щодо захисту КР: тема, успішність, висновок керівника та висновок кафедри про КР. 2. Зовнішня рецензія (окремо від КР). Резюме на КР. 3. Електронний варіант презентації. 4. Електронний варіант КР на диску
10.	Захист ДР	17	22,23,24 12.2025	1. Приєднання студента до засідання кваліфікаційної комісії (конференції) у встановлений час для проведення процедури дистанційного захисту 2. Процедура захисту КР.

Керівник
д.т.н., професор, професор кафедри комп'ютерних технологій
та інформаційної безпеки, _____ В.І. Передерій

Студент _____ В.В. Бесідовський

АНОТАЦІЯ

У магістерській роботі досліджувалась актуальна проблема визначення та оцінювання впливу факторів вразливостей на стійкість об’єкту критичної інфраструктури з використанням методів експертного оцінювання. В роботі проведено детальний аналіз сучасних методів і способів оцінювання впливу факторів вразливостей на стійкість об’єкту критичної інфраструктури. Досліджені проблемні питання з визначення та проведена класифікація основних факторів вразливостей що впливають на захищеність об’єктів. Для визначення та оцінки залежності стійкості об’єкта критичної інфраструктури від впливу факторів вразливостей розроблено інформаційну та інформаційно – логічну модель з використанням методів експертного оцінювання.

Для прогнозування рівня безпекового стану та залежності стійкості об’єкту критичної інфраструктури від впливу факторів визначених вразливостей використовувались системний аналіз, теорія експертних оцінок та графо-аналітичні методи Байесовської мережі довіри.

Проведено ряд експериментів з оцінювання залежності стійкості об’єкту критичної інфраструктури від впливу факторів вразливостей з використанням методів експертного оцінювання.

Ключові слова: *фактори вразливостей, стійкість об’єкту критичної інфраструктури, методів експертного оцінювання, інформаційно – логічна модель, системний аналіз, теорія експертних оцінок, графо-аналітичні методи, Байесовська мережа довіри.*

ABSTRACT

The master's thesis investigated the current problem of determining and assessing the impact of vulnerability factors on the stability of a critical infrastructure facility using expert assessment methods. The work conducted a detailed analysis of modern methods and methods for assessing the impact of vulnerability factors on the stability of a critical infrastructure facility. Problematic issues in determining and classifying the main vulnerability factors that affect the security of facilities were studied. To determine and assess the dependence of the stability of a critical infrastructure facility on the impact of vulnerability factors, an information and information-logical model was developed using expert assessment methods.

To predict the level of security status and the dependence of the stability of a critical infrastructure facility on the impact of identified vulnerability factors, system analysis, the theory of expert assessments, and graph-analytical methods of the Bayesian trust network were used.

A number of experiments were conducted to assess the dependence of the stability of a critical infrastructure facility on the impact of vulnerability factors using expert assessment methods.

Keywords: *vulnerability factors, critical infrastructure object stability, expert assessment methods, informational-logical model, system analysis, expert assessment theory, graph-analytical methods, Bayesian trust network.*

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ЕС – Експертні системи

ТЕО – теорія експертних оцінок

ІБ – Інформаційна безпека.

КБ – Кібербезпека.

ОКІ – Об’єкт критичної інфраструктури

СОКІІ – Стійкість об’єкту критичної інфраструктури

БМД – Байєсівська мережа довіри.

ПЗ – програмне забезпечення;

ОПР – Особа, що приймає рішення.

СППР – Система підтримки прийняття рішень

ЗМІСТ

ВСТУП

На сьогодні визначення та оцінка основних факторів, які визначають стійкість критичної інфраструктури, а також розробку підходів до її посилення стають для країни надзвичайно актуальною проблемою. Практично щоденно населення країни відчуває негативні наслідки обстрілів, зокрема й внаслідок руйнування об’єктів критичної інфраструктури. Загалом, згідно з міжнародними стандартами, національними нормативно-правовими актами та науковими узагальненнями дослідників, критична інфраструктура охоплює об'єкти, системи та мережі, що забезпечують функціонування економіки, безпеку суспільства та держави, що вимагає розробки нового інструментарію по забезпеченню їх захищеності.

Актуальність теми. Сучасні методи моделювання загроз та їхнього впливу на безпеку об'єктів критичної інфраструктури вимагають складних розрахунків, наявності достатньо повної статистичної інформації та тривалого часу обробки даних. Тому варто розглянути підходи, що дозволяють вирішувати задачі, що не піддаються суворій формалізації, використовуючи неповну, нечітку інформацію та суб'єктивні оцінки експертів у певній галузі, а також будуючи гнучкі, конструктивні моделі, що адекватно реагують на зміни. У цьому контексті ця галузь досліджень є критично важливою.

Виходячи з цього, в даній роботі пропонується дослідження залежності впливу основних факторів вразливостей на стійкість об’єкту критичної інфраструктури з застосуванням методів експертного оцінювання.

Мета дослідження. Мета магістерської роботи є дослідити залежність впливу основних факторів вразливостей на стійкість об’єкту критичної інфраструктури з застосуванням методів експертного оцінювання.

Завдання дослідження:

1. Провести аналіз сучасних методів та способів дослідження факторів вразливостей на об’єктах критичної інфраструктури.

2. Провести аналіз методів і способів експертного оцінювання у визначені та дослідженні впливу факторів вразливостей на об’єктах критичної інфраструктури.

3. Розробити інформаційну модель дослідження взаємовпливу основних факторів вразливостей на об’єкт критичної інфраструктури.

4. Провести оцінювання та ранжування основних факторів вразливостей на об’єкті критичної інфраструктури.

5. Розробити математичну модель оцінювання залежності стійкості об’єкту критичної інфраструктури від впливу визначених факторів вразливостей.

6. Провести експерименти з оцінки впливу факторів вразливостей на об’єкт критичної інфраструктури по результатам експертного оцінювання.

Об'єкт дослідження: моделі, методи і інформаційні технології оцінки та забезпечення стану захищеності ОКІ.

Предмет дослідження: сукупність теоретичних та практичних засад з використанням теорії експертних оцінок для оцінювання впливу факторів вразливостей на стійкість об’єкту критичної інфраструктури.

Методи дослідження: Системний аналіз, теорія експертних оцінок, Байесовської мережі довіри.

Наукова новизна одержаних результатів: Побудова математичної моделі дослідження та оцінювання залежності впливу основних факторів вразливостей на стійкість об’єкту критичної інфраструктури з використанням методів експертного оцінювання.

Очікуваний результат: Результати дослідження нададуть можливість вирішення задач з оцінювання стійкості об’єкту критичної інфраструктури в залежності від впливу факторів вразливостей які характеризуються високим ступенем невизначеності, складністю строгої формалізації та мають суб’єктивний характер.

Дипломна робота є самостійним дослідженням, та базується на актуальних наукових публікаціях, а також даних, отриманих в результаті експертних опитувань.

1. ОСНОВНІ ОСОБЛИВОСТІ ФАКТОРІВ ВРАЗЛИВОСТЕЙ НА ОБ’ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1 Основні особливості впливу факторів вразливостей на стійкість об’єкту критичної інфраструктури.

Стійкість критичної інфраструктури є комплексним та багатогранним поняттям, яке включає не тільки фізичний захист інфраструктурних об'єктів, але й адаптацію до змін, здатність відновлюватися після кризових ситуацій та забезпечення безпеки в умовах постійно змінюваних загроз. В умовах глобалізації та технологічних змін для досягнення стійкості критичної інфраструктури важливим є інтегрований підхід, що охоплює правові, технічні, економічні та соціальні аспекти, які містять в основі врахування рівня критичності відповідного об’єкту. Забезпечення стійкості критичної інфраструктури в Україні є необхідною умовою для збереження національної безпеки та розвитку економіки. Враховуючи багатоаспектні загрози – від воєнних до кібернетичних і природних – Україні необхідно розвивати комплексну стратегію для захисту важливих об'єктів інфраструктури. Це включає [1-7]:

— адміністративно-правові та інституційні заходи:

— удосконалення правового та нормативного забезпечення;

— впровадження новітніх технологій для підвищення ефективності та безпеки;

— розвиток інформаційної і кібербезпеки та підготовку кваліфікованих кадрів;

— розвиток міжнародного співробітництва для обміну досвідом та ресурсами.

На сьогодні критична інфраструктура є основою функціонування сучасного суспільства та економіки. Вона включає всі ключові об'єкти та системи, від яких залежить життєдіяльність населення, ефективність державного управління та стабільність економічної діяльності. Стійкість

таких систем визначає здатність держави підтримувати основні соціальні функції навіть в умовах надзвичайних ситуацій, таких як природні катастрофи, техногенні аварії, або кібератаки. У зв'язку з зростанням кількості глобальних катастроф та загроз, необхідність забезпечення стійкості критичних інфраструктур стає дедалі більш актуальною. Головними важливими питаннями стійкості є до технологічних, екологічних та соціальних загроз, а також готовність до швидкого відновлення після криз та катастроф. Для України, яка стикається з численними внутрішніми та зовнішніми загрозами, забезпечення стійкості критичної інфраструктури на сьогодні, набуває особливого значення. Збройні конфлікти, кіберзагрози, природні катастрофи, техногенні аварії та економічні виклики створюють серйозні ризики для безпеки та функціонування критичних об' єктів

Разом з тим, окремі питання дослідження стійкості критичної інфраструктури потребують додаткового дослідження особливо в умовах сучасних викликів в країні.

У контексті розгляду критичної інфраструктури, її стійкість характеризується кількома основними аспектами, а саме [7]:

1. Здатність до безперервності функціонування. Цей аспект передбачає, що стійка критична інфраструктура повинна забезпечувати безперервне надання основних послуг, таких як енергопостачання, водопостачання, транспорт, зв'язок, охорона здоров'я, навіть у випадку виникнення надзвичайних ситуацій або зовнішніх загроз. Наприклад, енергетична мережа повинна залишатися функціональною під час техногенних аварій, природних катастроф або навіть воєнних конфліктів.

2. Здатність до адаптації та гнучкості, яка визначає, що стійкість також передбачає здатність інфраструктури адаптуватися до змінних умов або нових загроз. Це може включати впровадження нових технологій, оновлення систем безпеки, а також зміни в управлінні чи організаційній структурі. Наприклад, у випадку зміни кліматичних умов чи збільшення кількості кіберзагроз, інфраструктура повинна бути здатною швидко адаптуватися до нових реалій.

3. Відновлювальна здатність - має важливе значення, коли інфраструктура піддається руйнуванню через надзвичайні ситуації (природні катастрофи, терористичні акти, кібератаки чи інші фактори), стійкість визначається здатністю швидко відновлюватися і повернутися до нормального функціонування. Для цього необхідно мати наявність резервних систем, швидку реакцію на надзвичайні події та чітко налагоджені процеси відновлення.

4. Захист від загроз та забезпечення безпеки, потребує здатності системи до запобігання або мінімізувати вплив зовнішніх і внутрішніх загроз. Стійкість критичної інфраструктури у цьому разі включає в себе заходи щодо кібербезпеки, захисту фізичних об'єктів, а також управління ризиками, що можуть виникнути внаслідок природних або техногенних катастроф.

5. Стійкість до зовнішніх і внутрішніх надзвичайних ситуацій, тобто здатність витримувати зовнішні виклики, такі як військові загрози, природні катастрофи, економічні кризи, а також внутрішні стреси, пов'язані з технічними неполадками чи людським фактором. Важливою складовою є також мінімізація ефектів від цих аварій, щоб не допустити великомасштабних руйнувань і порушень.

6. Інтеграція з іншими системами, що часто визначається також здатністю критичної інфраструктури інтегруватися в загальну екосистему, включаючи взаємодію з іншими інфраструктурами та державними системами управління, що сприяє ефективному реагуванню на надзвичайні ситуації на всіх рівнях – від місцевого до національного.

7. Забезпечення стійкості в умовах цифрової трансформації, на сьогодні набуває особливого значення в умовах поширення цифровізації. У сучасному світі важливим аспектом стійкості є здатність інфраструктури функціонувати в умовах цифрових технологій, до яких відносяться захист від кіберзагроз, інтеграцію нових технологій та забезпечення стійкості цифрових платформ, які підтримують економічні і соціальні процеси.

8. Стійкість екологічних і соціальних факторів. Дана критична інфраструктура також має бути стійкою до екологічних змін, таких як зміна клімату або природні катастрофи, та здатною реагувати на соціальні виклики, наприклад: міграційні процеси або соціальні хвилювання. Така критична інфраструктура повинна мати ресурси для адаптації і реагування на виклики без значного порушення функціонування. Отже, стійкість, можна трактувати як здатність системи, організації та інфраструктури ефективно функціонувати і відновлюватися після впливу різноманітних загроз або стресових факторів. Така критична інфраструктура повинна включати не лише здатність витримувати критичні навантаження, але й забезпечувати безперервність важливих функцій у довгостроковій перспективі, навіть у випадку глобальний аварій чи катастроф.

На сьогодні визначення та оцінка основних факторів, які визначають стійкість критичної інфраструктури, а також розробку підходів до її посилення стають для країни надзвичайно актуальною проблемою. Практично щоденно населення країни відчуває негативні наслідки обстрілів, зокрема й внаслідок руйнування об’єктів критичної інфраструктури. Загалом, згідно з міжнародними стандартами, національними нормативно-правовими актами та науковими узагальненнями дослідників, критична інфраструктура охоплює об'єкти, системи та мережі, що забезпечують функціонування економіки, безпеку суспільства та держави. Це важливі елементи, без яких неможливо забезпечити нормальне життя населення та підтримку базових державних функцій [7,8].

До основних складових критичної інфраструктури за законодавством України відноситься:

- енергетична інфраструктура (енергетичні мережі, енергоблоки, системи електропостачання та газопостачання, електростанції, мережі енергопостачання, газові та нафтові магістралі, які забезпечують країну енергоресурсами для промисловості, транспорту та побутових потреб);

- транспортна інфраструктура (автомобільні, залізничні, авіаційні й водні шляхи, а також логістичні хаби, які гарантують переміщення товарів і людей по території країни та за її межами);

- інформаційно-комунікаційна інфраструктура (телекомунікаційні мережі, Інтернет, бази даних, мобільний зв'язок, інформаційні платформи, сервісні мережі та інші технології передачі даних, які забезпечують цифрову взаємодію та передачу даних);

- водопостачання та каналізація (системи постачання питної води, водовідведення та очистки стічних вод)

- охорона здоров'я (лікарні, медичні заклади, системи швидкої допомоги);

- фінансова інфраструктура (банки, платіжні системи, фондові ринки, які гарантують фінансову стабільність та безперервність економічних операцій);
- захист від надзвичайних ситуацій (служби порятунку, цивільного захисту, пожежні частини та інші органи, які займаються реагуванням на надзвичайні ситуації) [8].

До основних особливостей факторів вразливостей на об’єктах критичної інфраструктури відносяться такі як їх масштабність, складність впливу, взаємозалежність та технічна застарілість, висока вартість, залежність від людського фактору та значний потенціал наслідків від ураження. Вразливості охоплюють як фізичні, так і інформаційні та операційні аспекти, що робить їх унікальними цілями для кібератак, тероризму та стихійних лих.

На об'єктах критичної інфраструктури вразливості можуть призводити до масштабних наслідків, які впливають на енергетичну, економічну, екологічну та інші сфери, а взаємодія між різними системами робить їх уразливими до каскадних збоїв.

Розглянемо основні особливості факторів вразливостей на об’єктах критичної інфраструктури:

— Масштабність - чим більший об'єкт критичної інфраструктури, тим більше в ньому вразливостей, що ускладнює процес управління вразливостями

та може призвести до накопичення технічного боргу, коли старі вразливості не виправляються вчасно через брак часу чи ресурсів.

— Складність впливу - порушення функціонування об'єктів критичної інфраструктури спричиняє надзвичайні ситуації або має негативний вплив на стан екологічної, енергетичної, економічної, фінансової та інших сфер, що є головним критерієм віднесення об'єкта до критичної інфраструктури.

— Взаємозалежність – масштабні об'єкти критичної інфраструктури (такі як енергетика, транспорт, зв'язок) які тісно взаємопов'язані та означає, що збій в одній системі може спричинити каскадний ефект та призвести до порушень роботи інших систем, що робить їх особливо вразливими.

— Технічна застарілість – характеризується виникненням ризикових ситуацій, із за того, що деякі об'єкти можуть використовувати застаріле програмне та апаратне забезпечення, яке не підтримується і має відомі вразливості, що робить їх легкою мішенню для атак.

— Людський фактор - це людські помилки, недостатня кваліфікація персоналу або навмисні шкідливі дії можуть стати причиною виникнення вразливостей або призвести до ураження системи.

— Висока вартість - збитки від ураження об'єкта критичної інфраструктури, які можуть бути значними, що робить їх привабливою ціллю для ворожих дій.

— Недостатній рівень захищеності - незважаючи на наявність нормативних документів, значна кількість об'єктів критичної інфраструктури мають недостатній рівень захищеності, що може бути наслідком браку ресурсів, застарілих стандартів або низького рівня усвідомлення ризиків.

— Складна система управління - управління об'єктом критичної інфраструктури здійснюється багатьма суб'єктами, що може призвести до нечіткого розподілу відповідальності та недостатньої координації дій.

Розглянемо класифікацію факторів вразливостей.

— Фізичні вразливості: Фізичні системи, такі як електромережі, водопостачання, нафтопроводи, можуть бути уражені внаслідок фізичного впливу, стихійних лих або ненавмисних інцидентів.

— Кібервразливості: Вразливості в комп'ютерних системах, які керують об'єктом критичної інфраструктури і можуть бути використані для кібератак, що призводять до викрадення даних або порушення роботи систем.

— Операційні вразливості: Не коректні або нечіткі процедури, відсутність належного плану реагування на надзвичайні ситуації, недостатнє навчання персоналу можуть призвести до ураження системи.

— Вразливості, пов'язані з людським фактором: Недостатній рівень кваліфікації персоналу, неналежний рівень підготовки, брак мотивації або цілеспрямовані дії працівників можуть призвести до ураження системи.

Заходи для мінімізації ризиків.

— Комплексний підхід - необхідніст розробки та впровадження комплексної системи захисту, яка охоплюватиме всі аспекти роботи об'єкту критичної інфраструктури.

— Оновлення застарілих систем - необхідність регулярно оновлювати та вдосконалювати застарілі системи, що використовуються на об'єктах критичної інфраструктури, для усунення їх вразливостей.

— Навчання персоналу - необхідність регулярного проводження навчання персоналу щодо правил безпеки та процедур реагування на надзвичайні ситуації.

— Створення паспорта безпеки - розроблення та узгодення паспорту безпеки на кожному об'єкті критичної інфраструктури для визначення заходів, які мають бути вжиті у разі виникнення загроз.

— Міжнародне співробітництво - необхідність розвитку міжнародного співробітництво для обміну інформацією та досвідом у сфері захисту об'єктів критичної інфраструктури.

— Рішення зазначених цих основних завдань дослідження вразливостей критичної інфраструктури, які включають аналіз загроз, оцінку рівня

захищеності, розробку заходів безпеки та створення моніторингу систем обміну інформацією, дозволить виявляти, запобігати та ліквідувати наслідки інцидентів безпеки на всіх етапах життєвого циклу об'єкту критичної інфраструктури .

1.2 Роль і значення математичних методів та засобів в дослідженні факторів вразливостей на об’єктах критичної інфраструктури.

На сьогодні для України, як для держави, що перебуває у стані безпрецедентних викликів, таких як збройна агресія, пошкодження енергетичної інфраструктури, а також глобальні кліматичні зміни, розробка інструментів оцінки вразливості та стійкості об'єктів критичної інфраструктури є значно важливим завданням [6,7].

Оцінювання ризиків функціонування об’єктів критичної інфраструктури є ключовим елементом забезпечення національної безпеки, оскільки дозволяє ідентифікувати можливі загрози та приймати рішення щодо їхнього усунення чи мінімізації. Традиційні методи оцінювання ризиків часто виявляються недостатньо ефективними через високу невизначеність і складність даних, що надходять з існуючих систем захисту критичної інфраструктури. В умовах постійно змінюваних загроз, таких як природні катаклізми, техногенні аварії або цілеспрямовані ракетно-дронові атаки рф, особливо актуальним є використання методів та засобів інформаційної та інтелектуальної технології, які дозволяють працювати з нечіткими, неповними або непередбачуваними даними. Застосування зазначених методів, дозволяє ефективніше моделювати реалізацію загроз для об’єктів критичної інфраструктури та оцінювати ризик їх функціонуванню на основі змінних, що не мають чітких границь або однозначних значень. Сучасні виклики, зокрема пов’язані з військовими загрозами, кібератаками, природними катастрофами, потребують створення математичних моделей, здатних швидко реагувати на зміни та враховувати комплексність процесів. Особливо це актуально в умовах агресивних ракетно-дронових атак на об’єкти критичної інфраструктури, що може призвести до

каскадних деструктивних наслідків. Знищення ключових об’єктів атомної енергетики, гідросистем, водопостачання, зв’язку чи транспорту може викликати великомасштабні аварії, що впливають на економіку, екологію та населення.

Але актуальні виклики сьогодення, такі як військові загрози, вторинні деструктивні впливи та природні катаклізми, потребують створення математичних моделей, здатних швидко адаптуватися до змін і враховувати багатофакторність процесів. Це особливо актуально при захисті від ракетно-дронових атак на об'єктах критичної інфраструктури, оскільки вони можуть спровокувати ланцюгові руйнівні аварії та катастрофи, що матимуть значний вплив на економічний стан країни, стан довкілля та добробут населення. Тому одним із найбільш перспективних підходів для ідентифікації можливих загроз та оцінювання відповідних ризиків їх реалізації являються методи м’яких обчислень такі як теорія нечіткої логіки, теорія експертних систем, методи теорії ймовірності та інш., які є одними із найбільш перспективних підходів для ідентифікації можливих загроз та оцінювання відповідних ризиків їх реалізації, оскільки вони дозволяють працювати з інформацією, яка не може бути точно виміряною або яка має значну невизначеність.

Зазначені математичні методи та моделі відіграють ключову роль в дослідженні вразливостей критичної інфраструктури, оскільки дозволяють кількісно оцінити ризики, оптимізувати заходи безпеки та прогнозувати ймовірність відмов. Вони використовуються для моделювання різних загроз, аналізу залежностей між компонентами системи, виявлення критичних точок ураження та розробки ефективних стратегій захисту.

Основні задачі математичних методів та моделей.

- Кількісна оцінка ризиків - дозволяють перетворити якісні оцінки вразливостей на числові показники, такі як ймовірність відмови, вартість збитку або рівень ризику.
- Моделювання загроз - методи такі як теорія графів, ймовірність та статистика, дозволяють створювати моделі, що симулюють поведінку

нападників, природні явища або технічні збої, аби передбачити їхній вплив на систему.

- Аналіз залежностей - математичні методи які допомагають виявити критичні залежності між різними компонентами критичної інфраструктури, де аналіз залежностей може показати, що збій одного елемента може спричинити каскадний відказ у всій системі.
- Оптимізація заходів безпеки - математичні методи, оптимізаційні алгоритми, що дозволяють знайти найефективніший розподіл ресурсів для захисту інфраструктури, мінімізуючи при цьому витрати.
- Прогнозування та моніторинг - математичні моделі які використовуються для створення систем моніторингу, таі можуть вчасно виявляти відхилення від нормального стану і прогнозувати майбутні проблеми, що дозволяє уникнути аварій.
- Розробка сценаріїв - математичне моделювання що дозволяє створювати реалістичні сценарії розвитку подій, та допомагає розробляти адекватні плани реагування на надзвичайні ситуації.

Значення математичних методів та моделей в оцінювані ризиків функціонування об’єктів критичної інфраструктури.

- Зменшення невизначеності - математичні моделі дають можливість об’єктивно оцінити рівень ризиків, а не покладатися на інтуїтивні судження, що є надзвичайно важливим при роботі з критичною інфраструктурою.
- Підвищення ефективності захисту - математичне моделювання дозволяє розроблення більш ефективних та цілеспрямованих заходів безпеки, які є більш економічно доцільними.
- Підготовка до майбутніх загроз - математичні моделі що дозволяють прогнозувати нові види загроз і розробляти відповідні методи протидії до того, як вони стануть реальністю.
- Прийняття обґрунтованих рішень - математичні методи які надають об'єктивну оцінку для прийняття рішень щодо безпеки, розробки нових протоколів та інших стратегічних рішень.

- Інтеграція різних систем - математичні моделі які можуть розв’язувати складні взаємозв'язки між різними системами, що становить критичну інфраструктуру (енергетика, зв'язок, транспорт), та виявити приховані ризики.

Складність створення моделі оцінки безпеки критичної інфраструктури в цілому пов’язана з різнорідністю її складових, неповнотою знань про можливі відмови і ризики, отриманням даних про стан та функціонування об’єктів критичної інфраструктури у різних ситуаціях.

Найчастіше для оцінки ризиків для критичних систем застосовують методи детерміністського аналізу DSA (Deterministic Safety Assesment) та імовірнісного аналізу PSA (Probabilistic Safety Analysis) [8,9]. Детерміністський аналіз DSA передбачає послідовний аналіз поведінки інфраструктури на множині правдоподібних сценаріїв розвитку аварій з використанням визначених правил і гіпотез стосовно стану підсистем, їх характеристик, дій оператора і т.д. з обмеженням щодо технічної можливості настання певної аварії. Нажаль цей підхід не дозволяє врахувати всі існуючі невизначеності. Імовірнісний аналіз PSA використовується для оцінки імовірності великих аварій, зокрема на атомних електростанціях. Основою імовірнісного підходу є системний аналіз можливих сценаріїв, а також послідовне дослідження аварій, включаючи вихідні події, шляхи розвитку аварійних ситуацій з урахуванням накладення відмов систем. Спершу визначаються послідовності подій, які можуть призвести до аварії, а потім виконується оцінювання стану критичного об’єкта і можливе розповсюдження наслідків аварії.

На останньому етапі здійснюється оцінка впливу аварії на здоров’я людей. Оскільки великі аварії є досить рідкісними подіями, статистичних даних недостатньо для застосування класичного імовірнісного підходу. При застосуванні методу аналізу виду і наслідків критичних відмов FMECA (Failure Modes, Effects and Critical Analysis) систематично, шляхом послідовного розгляду інфраструктурних підсистем, визначаються всі можливі види відмов, пошкоджень, аварійних ситуацій та їх результуючий

вплив на інфраструктуру і оточуюче середовище. Суть FMECA полягає у визначенні впливу кожного потенційного дефекту (відмови) на функціональність інфраструктури як системи у цілому, і впорядкування відмов відповідно до величини очікуваного збитку. Цей метод дозволяє провести досить повний якісний аналіз причин і наслідків відмов елементів інфраструктури, але він трудомісткий і не враховує можливу деградацію ОКІ і інфраструктури, час настання і залежність відмов. Іноді для аналізу ризиків застосовують модифікації цих основних методів, частково долаючи зазначені недоліки. Та сьогодні все частіше починають залучати для аналізу методи штучного інтелекту, лінгвістичні методи, нечіткі моделі для уточнення основних видів невизначеностей, урахування залежності подій, зміни критичності відмов при наявності залежності відмов. Методи нечіткої математики, такі як нейроні мережі, нечітка логіка, генетичні алгоритми вбудовуються у технології нового покоління – «м'яких обчислень» (soft computing), які використовуються для управління складними системами з дефіцитом апріорної інформації в умовах невизначеності і дозволяють застосувати досвід експертів, їх знання для ризик-аналізу у процесі управління [8]. Складність і трудомісткість методів аналізу ризиків, складність математичних моделей критичних інфраструктур, неможливість врахування широкого спектру факторів, зокрема нових можливостей щодо дистанційного ураження об'єктів критичної інфраструктури, реалізації загроз виникнення аварій змушують шукати нові підходи.

1.3 Особливості та класифікація експертних методів.

На сьогодні найбільш ефективними методами оцінки стійкості об'єктів критичної інфраструктури являються експертні методи.

Метод експертних оцінок має широке застосування. Серед типових завдань, які вирішуються за допомогою цього методу, можна виділити [9,10]:

Створення переліку потенційних подій, що можуть відбутися в різних сферах протягом визначеного періоду.

2) визначення часових проміжків, в яких найімовірніше відбудеться низка подій.

3) Необхідно визначити цілі та завдання управління, а також ранжирувати їх за ступенем важливості.

4) виявлення різних способів вирішення завдання та оцінка їх ефективності;

5) Інший підхід до розподілу ресурсів, спрямований на вирішення завдань з урахуванням їхньої ефективності.

6) Розглянути різні варіанти вирішення даної ситуації та оцінити переваги кожного з них.

Існує велика кількість методів отримання експертної інформації. Класифікація цих методів, наведена на рис. 1 [9].

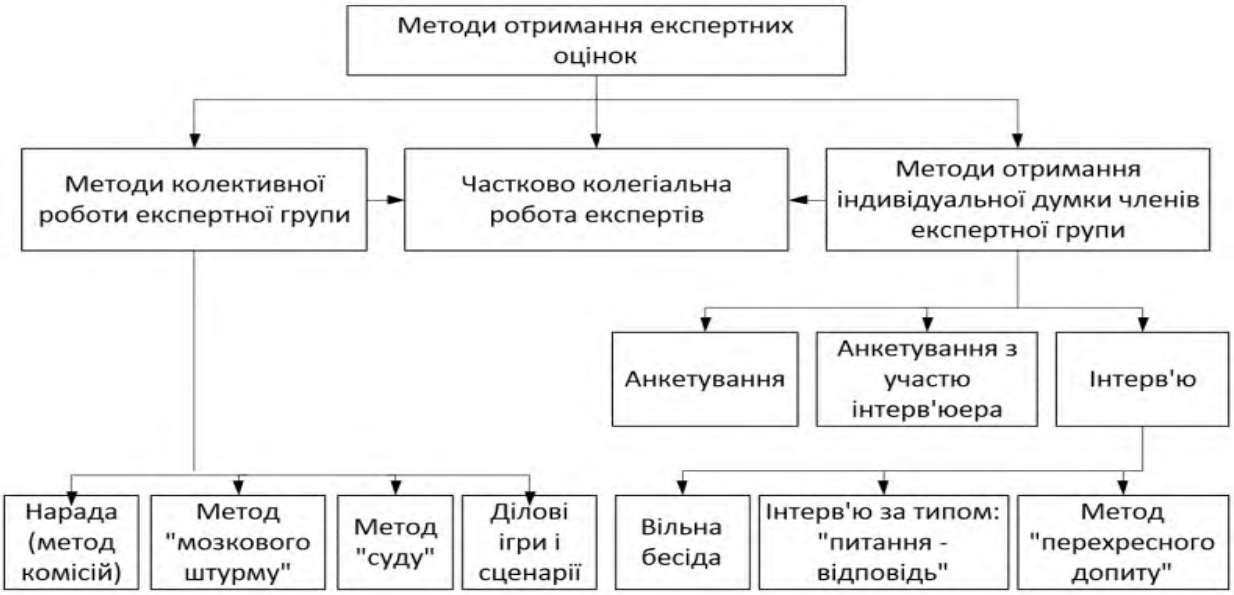

Рисунок 1.1 - Методи отримання експертних оцінок.

Різні типи завдань вирішуються за допомогою різних варіацій методу експертних оцінок. До таких варіацій належать анкетування та інтерв'ювання; мозковий штурм; дискусійні сесії; наради; оперативні ігри; сценарійні методи та інші. Кожен з цих підходів має свої сильні та слабкі сторони, що визначають сферу його оптимального використання. У численних ситуаціях найбільш

ефективним є комплексне застосування кількох видів експертизи. Кваліфіковане застосування методу експертних оцінок в значній мірі залежить від вибраного способу збору й обробки відповідей цілеспрямовано сформованої групи фахівців.

1.3.1 Особливості застосування методів колективної експертної оцінки.

Особливості застосування методів колективної експертної оцінки передбачають їх використання для розробки науково-технічних прогнозів, що базуються на статистичній обробці оцінок, наданих експертами щодо відносної важливості напрямків наукових досліджень. Цей метод включає формування прогнозу групою спеціалістів, де узагальнена думка більшості експертів стає основою для оцінки.

Для відображення групової позиції використовуються статистичні показники, які характеризують загальний рівень погодженості [10-12]. Групова відповідь може бути представлена числовим значенням, що переважає значення половини експертів і поступається іншій половині. При цьому експерти мають можливість змінити свою оцінку, якщо переконливі аргументи колег підтверджують їхню правоту, або ж залишаються при власній думці.

Основною особливістю методу є здатність досягти спільної позиції експертів щодо перспективних напрямків розвитку об'єкта прогнозування, які раніше формувалися окремими фахівцями. Метод також дозволяє оцінювати аспекти розвитку, які складно визначити іншими засобами, такими як математичні розрахунки чи експериментальні дослідження. Алгоритм методу передбачає наступні етапи:

1. Формування робочих груп для організації експертних оцінок. До їхніх завдань входять підготовка опитувань, обробка отриманих даних та аналіз результатів. Робоча група обирає експертів, які відповідають на запитання, пов'язані з перспективами розвитку галузі. Залучається від десяти до ста п’ятдесяти фахівців, залежно від складності теми.

2. Перед початком опитування визначають напрямки розвитку об'єкта і створюють матрицю, що описує цілі та способи їх досягнення. Потім формулюють питання для експертів.

3. Під час опитування забезпечується однозначність розуміння запитань та незалежність суджень кожного експерта. 4. Обробка результатів складається зі встановлення узагальненої думки експертів і визначення рівня погодженості їхніх індивідуальних оцінок. Опрацьовані дані стають основою для формування прогнозних гіпотез або варіантів розвитку галузі. Остаточна оцінка може бути представлена середнім арифметичним, середнім нормалізованим зваженим значенням або середнім судженням експертної групи.

Однак метод має низку недоліків:

1. На результати значно впливають індивідуальні когнітивні характеристики експертів, такі як схильність наполегливо відстоювати свої погляди.

2. Застосування методу потребує значних ресурсів, а отриманий результат може не відповідати очікуванням всіх учасників.

3. Існує дискусія щодо того, чи є за доцільне залучати до роботи експертів із різних спеціалізацій.

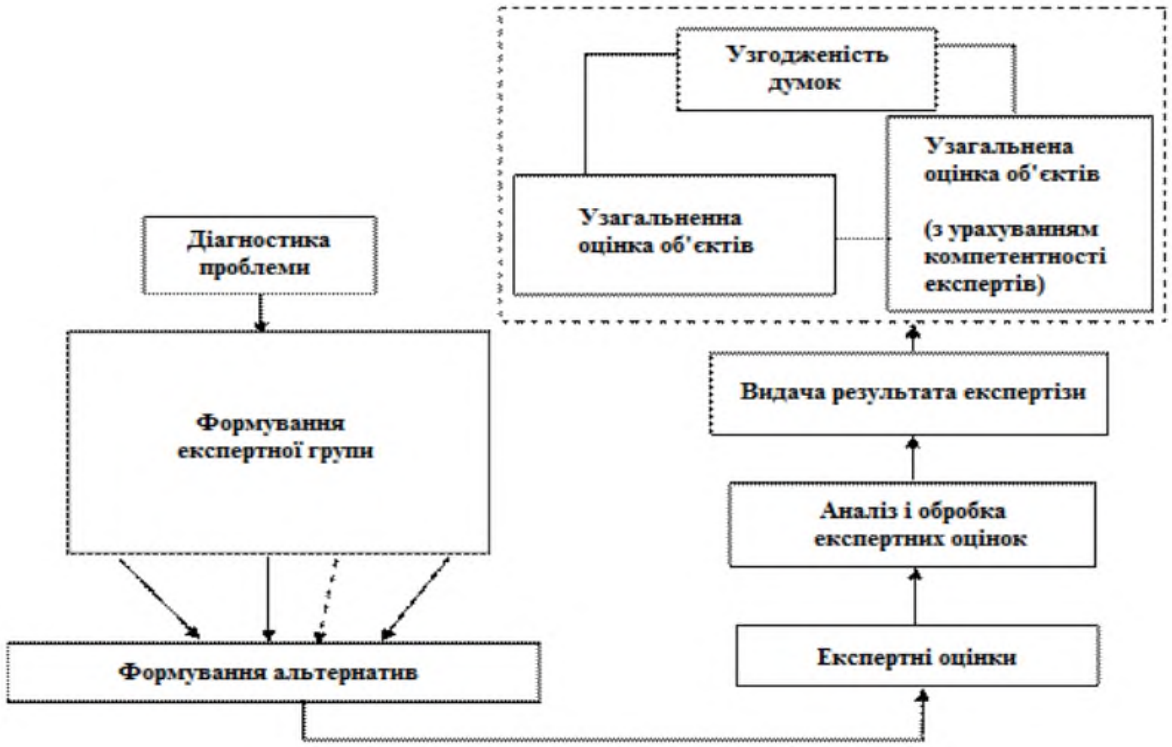

Рисунок 1.2 - Структурна схема програми проведення експертизи.

Розглянемо ключові етапи використання експертних методів для оцінки стійкості об'єкта критичної інфраструктури:

1. Формування варіантів рекомендацій. Процес вибору методології оцінки стійкості об'єкта повинен включати створення прогнозних анкет, підготовку інструкцій щодо їх заповнення, а також визначення моделей і методик, необхідних для розрахунку показників, які використовуються в експертних оцінках.

2. Розробка питань анкет. Анкети мають містити питання, які чітко відображають суть проблеми та потребують відповідей експертів. Зміст і форма запитань залежать від специфіки об'єкта дослідження. Питання слід розділити на відкриті та закриті, прямі та непрямі.

3. Визначення кількості питань. При підготовці анкет важливо суворо дотримуватися оптимальної кількості запитань. Вважається, що експертна група може якісно працювати з опитувальником до 25 питань. У деяких випадках можна збільшити їх кількість, але якщо число запитань сягає понад 50, керівник експертизи має ретельно опрацювати їх доцільність.

4. Обробка анкет. Процес опрацювання заповнених анкет передбачає обчислення ряду показників, що забезпечують можливість формулювання узагальнюючих висновків. Організатори експертизи повинні володіти необхідною методикою обробки даних.

5. Формування інформаційної бази. Для успішної організації дослідження потрібна ефективна інформаційна база, яка складається з нормативно-довідкової та змінної інформації. Нормативно-довідкова включає довідники, коди, інструкції тощо. Натомість змінна інформація базується на даних заповнених анкет.

6. Передпрогнозний аналіз. На цьому етапі досліджується стан і тенденції розвитку об’єкта прогнозування як у межах країни, так і за кордоном, аби чітко визначити завдання для експертної оцінки.

7. Використання технічних і програмних засобів. Реалізація методу експертних оцінок потребує відповідного технічного забезпечення (обчислювальні засоби, оргтехніка) і програмних продуктів, які дозволяють зберігати інформацію, друкувати звіти тощо.

8. Стимулювання експертів. Ефективність експертизи значно підвищується завдяки належній мотивації учасників. Це можуть бути як моральні стимули (визнання авторства чи пріоритету нових ідей), так і матеріальні.

9. Матеріальна зацікавленість. Оскільки розробка науково обґрунтованого прогнозу є результатом праці висококваліфікованих фахівців, вона не може бути безоплатною. Забезпечення матеріальної мотивації є необхідною умовою якісного виконання експертизи.

Застосування такого підходу гарантує системність та наукову обґрунтованість оцінки стійкості об'єктів критичної інфраструктури.

1.3.2 Класифікація методів експертних оцінок.

Процес проведення експертизи для вимірювання та порівняння досліджуваних об’єктів супроводжується їх оцінюванням. Залежно від виду оцінок, їх можна класифікувати на різні типи.

На відміну від кількісних оцінок, котрі базуються на об’єктивних показниках, у межах експертизи використовуються бальні оцінки, що відображають суб’єктивну думку. Бальна шкала являє собою обмежений набір чисел, рівновіддалених одне від одного. Залежно від виконуваних завдань виділяють два типи бальних оцінок [13] :

- Перший тип передбачає оцінювання за об’єктивним критерієм або загальновизнаним еталоном з урахуванням його градацій. Точність характеристики та оцінки відхилення від еталона є ключем до довіри до такого способу оцінювання, яке виконують із використанням бальної шкали.

- Другий тип застосовують у випадках відсутності не лише загальноприйнятих зразків, а й одного-єдиного об’єктивного критерію. У таких випадках використовуються суб’єктивні відображення у вигляді оцінок, які формуються за порядковою, або ранговою шкалою. Ці оцінки порівнюють за принципом «більше-менше».

Для отримання експертних оцінок існує декілька методів:

“Метод ранжування”:

- полягає у впорядкуванні об’єктів за зменшенням або збільшенням переваг. При цьому допускається рівноцінність об’єктів чи їхніх оцінок.

“Метод попарного порівняння”:

- передбачає просте якісне порівняння двох об’єктів, що залишає поза потребую бальної або рангової шкали. Цей метод вважається більш зручним для визначення якісної різниці між двома об’єктами.

“Метод середньої точки”:

- використовується для оцінювання на основі якісного критерію, особливо якщо потрібно визначити кращий і гірший об’єкти. Після цього послідовно знаходять об’єкти, які можна розташувати між крайніми

варіантами: спершу середній між кращим і гіршим, далі проміжні між знайденим середнім і кожним із крайніх, і так доти, доки не буде розташовано всі об’єкти. Рисунок 1.3 демонструє типові кількісні методи експертного оцінювання.

Рисунок 1.3 - Типові кількісні методи експертного оцінювання.

1.3.3 Аналіз результатів проведення експертного оцінювання.

Завершальний етап експертної оцінки передбачає аналіз отриманих результатів, які слугують основою для ухвалення управлінських рішень, а також є джерелом інформації та рекомендацій.

Предметом аналізу має бути не лише система статистичних показників, а й увесь процес проведення експертизи, включно з формуванням цілей, відбором експертів, розробкою анкет для опитування та організацією самого процесу. Кожен етап повинен бути детально вивчений, щоб виявити потенційні недоліки та уникнути їх у майбутньому.

Сама система статистичних даних, яка генерується в ході оброблення анкет — це лише сукупність числових показників, або «сировина», що потребує глибокого професійного аналізу та інтерпретації. Саме від якісного осмислення цих даних залежить успіх та практична цінність усієї експертизи.

Методика аналізу результатів експертного опитування залежить від кількох факторів, серед яких [13]:

– тип експертизи (індивідуальна чи колективна),

– напрямок проведення дослідження,

– визначення часу настання конкретної події,

– оцінка прогнозованих параметрів об'єктів у майбутньому,

– визначення відносної важливості певних факторів,

– оцінка пропорцій різновиду можливих рішень тощо.

Оскільки індивідуальні експертні оцінки мають певні обмеження, їх обов'язково слід зіставляти з уже існуючими поглядами на досліджувану проблему, а також із висновками інших фахівців на основі їхніх прогнозних оцінок.

За результатами експертного аналізу важливо здійснити якісне оцінювання діяльності кожного учасника експертної групи. При цьому слід брати до уваги не лише авторитет і популярність фахівця, а й його відповідальне ставлення до роботи. Особливу увагу приділяють таким аспектам, як точність виконання завдань, сумлінність, акуратність, креативність у підході до роботи та вміння аргументувати свої переконання. Дотримання важливого принципу є обов’язковим: жодного фахівця не слід виключати з експертної групи лише через формальні критерії (наприклад, через показники узгодженості думок) без попереднього ретельного аналізу змісту його висновків.

Історія науки й техніки неодноразово демонструвала випадки, коли незвичайні чи на перший погляд суперечливі ідеї приводили до фундаментальних відкриттів. Багато фахівців є вузькопрофільними спеціалістами у своїй галузі. Тому результати їхніх суджень доцільно

співвідносити із зовнішніми факторами, які впливають на перспективи розвитку прогнозованого об’єкта.

Важливо пам’ятати про можливість існування власних інтересів експертів, які можуть не збігатися із загальними цілями проєкту. З огляду на це висновки експертиз повинні бути ретельно перевірені, критично осмислені та творчо адаптовані перед практичним використанням.

Концепція лінійної взаємодії є скоріше абстракцією, яка спрощує задачу, роблячи її завжди вирішуваною, проте із певною похибкою, що часто вважається несуттєвою. Логіка отримання результатів за такою схемою оцінювання, не беручи до уваги синергетичні ефекти, цілком зрозуміла. Вирішення шукається для конкретної ситуації з визначеною структурою показників, яка хоч і не формулюється в завданні експерта, зазвичай відображається в його уявленнях про проблему. Однак із початком змін у структурі одразу виникають непомічені раніше ефекти взаємодії, і надійність експертних оцінок помітно знижується.

Отже, пряме оцінювання показників із передбачуваною лінійною структурою зв’язків слід замінити більш складним підходом, укоріненим у модельному представленні структури, але водночас без ускладнення самого процесу опитування експертів. При цьому модель, яка відображає взаємозв'язок між ймовірністю виникнення цікавої для нас події та набором оцінюваних показників, повинна бути, вірогідно, нелінійною та економетричною. Це зумовлено не лише інтересом до механізму взаємодії, а й необхідністю отримання кількісної оцінки її сили.

Крім того, важливо мати інструмент, який дозволить замінити повторні опитування експертів на прогнозні оцінки. Цей аспект є особливо важливим і є перевагою над попередньо розглянутими методами.

Таким чином, основна цінність цього підходу полягає в тому, щоб використовувати експертну інформацію для побудови моделі, а не обмежуватися самим отриманням оцінок. Це суттєво розширює можливості практичного застосування експертного аналізу.

Висновки до першого розділу.

В розділі розглянуті основні особливості факторів вразливостей та їх вплив на стійкість об’єкту критичної інфраструктури. Визначена роль і значення математичних методів та засобів в дослідженні факторів вразливостей на об’єктах критичної інфраструктури.

Проведено аналіз особливостей і класифікацію експертних методів та зазначені особливості застосування методів колективної експертної оцінки.

Визначено, що складність створення моделі оцінки безпеки критичної інфраструктури в цілому пов’язана з різнорідністю її складових, неповнотою знань про можливі відмови і ризики, отриманням даних про стан та функціонування об’єктів критичної інфраструктури у різних ситуаціях.

Зазначено, що основна цінність застосування експертного аналізу полягає в тому, щоб використовувати експертну інформацію для побудови моделі, а не обмежуватися самим отриманням оцінок. Це суттєво розширює можливості практичного застосування даного методу.

2. АНАЛІЗ СУЧАСНИХ МЕТОДІВ ТА СПОСОБІВ ДОСЛІДЖЕННЯ ФАКТОРІВ ВРАЗЛИВОСТЕЙ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

2.1 Особливості застосування методів експертного оцінювання.

В умовах невизначеності, складності та неоднорідності систем (критичної інфраструктури) доцільно застосовувати метод експертного оцінювання групою експертів, що мають певні знання та досвід [13]. Провідні наукові установи у сфері енергетичної безпеки також широко застосовують такий метод.

Основними перевагами методу експертного оцінювання слід зазначити: використання досвіду

- експерти можуть точніше оцінювати загрози, використовуючи свій досвід та експертизу;
- розширене оцінювання загроз – експерти здатні здійснити більш точне оцінювання складних загроз, що важко охарактеризувати за допомогою автоматизованих методів;
- придатність при обмеженні ресурсів – у випадках, коли немає достатньої кількості даних для статистичного аналізу, експертне оцінювання є доцільним і раціональним методом урахування впливу людського фактору на загрози.

Основними недоліками такого методу є:

- поява людської помилки – експерти можуть допускати певні помилки під час оцінювання загроз, що можуть вплинути на точність результатів; відсутність об'єктивності (суб'єктивність) – обмеженість знань та досвіду експертів в цій галузі,
- виникнення конфлікту інтересів; неузгодженість думок – експерти можуть мати різні точки зору та оцінки, що призводить до труднощів у досягненні консенсусу;

- незнання невідомого – експерти можуть бути непоінформованими або не мати достатньої інформації про певні аспекти загроз, що може призвести до неповної оцінки.

Використання експертного оцінювання загроз є актуальним, оскільки: наявна інформація для аналізу та обробки може бути не повною, а частина спотворена; певний обсяг інформації має якісний характер; складність поставленого завдання оцінювання загроз та обмежені можливості математичного апарату не дають змогу зібрати й узагальнити всю потрібну інформацію. Для якісного оцінювання; недостатність математичного апарату для аналізу й обробки інформації; існує декілька можливих варіантів нейтралізації загроз, що не розглядаються через ресурсні та технічні обмеження; виникають непередбачувані фактори різного походження, що не можливо спрогнозувати, але можуть мати суттєвий вплив на безпеку критичної (військової) інфраструктури.

Експертне оцінювання загроз критичній інфраструктурі полягає в їхній пріоритизації за ризиками (наслідками, сукупними деструктивними ефектами) з визначенням найнебезпечніших, і відокремленні таких, що мають незначний та допустимий деструктивний ефект.

Основною метою такої пріоритизації є оптимальне використання наявних сил і засобів для захисту об’єктів критичної інфраструктури та нейтралізації найбільш значущих і найбільш імовірних загроз. Відокремлюють загрози та сукупні деструктивні наслідки реалізації яких можуть бути незначними за високої ймовірності, або значними, проте малоймовірними.

Експертне оцінювання з використанням якісного методу передбачає встановлення рівня кожної сформульованої загрози у спосіб поєднання її наслідків і ймовірностей їх настання, визначених у термінах значущості. Для досягнення цілей такого дослідження, припускають, що всі складові частини об’єкта управління, на які може вплинути певна загроза із переліку ідентифікованих загроз.

Прикладом пріоритизації до оцінювання загроз критичній інфраструктурі є відповідний перелік, сформований методом Делфі із залученням 10 експертів. Пріоритизацію виконано за рівнем загроз [13], що визначали як добуток експертних оцінок її сукупних негативних наслідків і загальної ймовірності реалізації. Вилучення загрози з реєстру здійснювали, якщо середня арифметична експертна оцінка наслідків імовірності перевищувала 2 бали.

У результаті проведених досліджень було встановлено, що метод експертного оцінювання є ефективним інструментом для оцінювання загроз критичній інфраструктурі. Він дає змогу враховувати широкий спектр факторів, що впливають на рівень загрози, і отримати об’єктивну та достовірну оцінку.

Застосування методу експертного оцінювання для оцінювання загроз критичній (військовій) інфраструктурі дає змогу: визначити пріоритетність об’єктів критичної інфраструктури для захисту; визначити найбільш значущі та найбільш імовірні загрози; розробити ефективні заходи захисту об’єктів критичної інфраструктури.

Метод експертного оцінювання може бути ефективним інструментом для оцінювання загроз критичній інфраструктурі та використаний для пріоритизації та оптимального використання наявних сил і засобів для захисту об’єктів критичної інфраструктури та нейтралізації найбільш значущих і найбільш імовірних загроз.

Для підвищення ефективності застосування методу експертного оцінювання для оцінювання загроз критичній інфраструктурі рекомендується: використовувати експертів з відповідною кваліфікацією та досвідом; проводити експертизу в кілька етапів, що дасть змогу врахувати різні точки зору експертів; використовувати сучасні інформаційні технології для обробки експертних оцінок.

2.2 Аналіз методів і способів експертного оцінювання у визначені та дослідженні впливу факторів вразливостей на об’єктах критичної інфраструктури.

Представлення знань в системах, які базуються на знаннях, являє собою систематизований спосіб формального вираження знань про предметну область. Тому практичний досвід розв'язання практичних задач від спеціалістів – експертів, вкладений в базу знань системи, представляється сукупністю фактів, правил, процедур і евристик (емпіричних правил) з предметної області.

Найбільш поширеним методом передавання знань на сучасному етапі є методи експертного оцінювання.

Ці методи незамінні під час вирішення складних управлінських проблем, аналізу і прогнозування ситуацій з великою кількістю факторів, завжди, коли виникає необхідність застосування знання, інтуїції та досвіду висококваліфікованих фахівців-експертів.

Однак проблеми розробки комплексних експертних методик, що використовують кількісні підходи, а особливо їх адаптування до потреб залишаються малодослідженими.

Але кожен окремий метод має свої переваги і недоліки, які визначають раціональну сферу його застосування. Для розв’язання більшості типових задач необхідно застосовувати комплексний підхід з обов’язковою аргументацією вибору методик-складових.

Альтернативи, розглянуті в процесі прийняття рішень, можуть мати вигляд елементів множини Ω або точок критеріального простору, який формально описується Em. Крім того, елементи Ω можуть бути впорядковані по деяких аспектах, істотних для прийняття рішень.

На даний час відомі три основні задачі аналізу групових експертних оцінок [9-13, 15]:

1.Визначення погодженості оцінок;

2.Класифікація (кластеризація) оцінок у випадку відсутності їх погодженості;

3.Визначення узагальненої оцінки усередині погодженої групи.

Для рішення таких задач існує множина методів одержання й аналізу експертних оцінок, однак науково обґрунтованої класифікації й уніфікації таких методів і тим більше однозначних рекомендацій з їхнього застосування не існує.

Розглянемо ряд можливих підходів до побудови уніфікованих технологій аналізу групових експертних оцінок, в основі яких лежить облік видів задач, типів вимірювальних шкал і форм представлення індивідуальних експертних оцінок.

Нехай експертна група в складі n експертів ($\{ni\}$, i=1,…,n) оцінює деяку множину m об'єктів O ($\{Oj\}$, j=1,…,m), так що результати можна представити матрицею розмірності nxm виду:

$$(O_{ij}) = \begin{pmatrix} O_{11} & O_{12} & \dots & O_{1m} \\ O_{21} & O_{22} & \dots & O_{2m} \\ \dots\dots & \dots\dots & \dots & \dots\dots \\ O_{i1} & O_{i2} & \dots & O_{im} \\ \dots\dots & \dots\dots & \dots & \dots\dots \\ O_{n1} & O_{n2} & \dots & O_{nm} \end{pmatrix}, \qquad (2.1)$$

де O_{ij} – оцінка і-*м* експертом j-*го* об'єкта. У даній матриці кожний рядок містить оцінки якого-небудь експерта по всіх об'єктах, а стовпець – оцінки всієї групи експертів по одному з об'єктів.

Розглянемо процедуру побудови технологій аналізу експертних оцінок з урахуванням перерахованих факторів.

Технологія аналізу на основі абсолютної шкали експертних вимірів.

Абсолютна шкала застосовується, наприклад, для виміру кількості об'єктів (предметів, подій, і т.п.). Експертні оцінки, отримані в такій шкалі являють собою звичайні натуральні числа x, наприклад, в інтервалі [0; 100], тобто $x \in [0;100]$. Тоді схему аналізу можна представити в наступному виді:

$$(x_{ij}) = \begin{pmatrix} x_{11} & x_{12} & \dots & x_{1m} \\ x_{21} & x_{22} & \dots & x_{2m} \\ \dots\dots & \dots\dots & \dots & \dots\dots \\ x_{i1} & x_{i2} & \dots & x_{im} \\ \dots\dots & \dots\dots & \dots & \dots\dots \\ x_{n1} & x_{n2} & \dots & x_{nm} \end{pmatrix} \Rightarrow \begin{pmatrix} \overline{X}_1 \\ \overline{X}_2 \\ \dots\dots \\ \overline{X}_j \\ \dots\dots \\ \overline{X}_m \end{pmatrix} \Rightarrow X_{об.} \qquad (2.2)$$

,

де $\overline{X}_j$ – оцінка типу «середнє», отримана по j-*му* стовпцю (об'єкту) усіма експертами їх погодженість, що й $X_{об.}$ характеризує; – узагальнена експертна оцінка усередині погодженої групи. Якщо j –й стовпець матриці (2.2) представлений однорідними й нормально розподіленими значеннями, то в якості оцінки $\overline{X}_j$ може бути використане звичайне середнє арифметичне. Однак, як було сказано вище, така ситуація можлива далеко не завжди. Тому в цьому випадку доцільно використовувати адаптивні оцінки робастного статистичного оцінювання. Основна ідея такого оцінювання полягає в тому, що зі сформованого набору оцінок типу «середнє» вибирається та, яка відповідає певним значенням статистик, що характеризують, наприклад, так звані «хвости» розподілів. Розглянемо одну з таких процедур, представлену на 2.3:

$$\overline{X}_j = \begin{cases} x^o(0.25), & Q < 2; \\ x(0), & 2 \le Q \le 2.6; \\ x(0.1875), & 2.6 < Q \le 3.2; \\ x(0.375), & Q > 3.2. \end{cases} \qquad Q = \frac{U(0.05) - L(0.05)}{U(0.5) - L(0.5)} \qquad (2.3)$$

,

Тут: Q – статистика, що характеризує вагу «хвостів» розподілу; $U(\cdot)$ – середнє $[0.05 \cdot n]$ і $[0.5 \cdot n]$ старших членів варіаційного ряду; $L(\cdot)$ – середнє $[0.05 \cdot n]$ й $[0.5 \cdot n]$ молодших членів варіаційного ряду; $x^o(0.25)$ – середнє, побудоване по $\alpha_1 n$, α_1=0.25 старшим і $\alpha_1 n$ молодшим значенням варіаційного ряду; $x(0)$ – арифметичне середнє; $x(0.1875)$ і $x(0.375)$ – усічені середні, отримані

по усіченому варіаційному ряду з рівнями усікання $k_1=\alpha_2 n$, $\alpha_2=0.1875$ і $k_2=\alpha_3 n$, $\alpha_3=0.375$; n – об'єм варіаційного ряду.

Отримане значенні Q ($2\le Q\le 2.6$) дає можливість використовувати оцінку $x(0)$, що і буде означати погодженість експертних оцінок. Інші оцінки $x^{o}(0.25)$, $x(0.1875)$ і $x(0.375)$ говорять про те, що усереднення можна одержати тільки по окремих сукупностях значень варіаційного ряду, отриманого за експертними оцінками. Інакше кажучи, характеризують їхня непогодженість, що й приводить до задачі класифікації, яка може бути представлена процедурою розбивки варіаційного ряду на однорідні сукупності наступного виду:

$$X_{(j)}=\begin{cases}(x_{(1)},x_{(2)},\ldots,x_{(\alpha_1 n)}),\ (x_{(\alpha_1 n+1)},x_{(\alpha_1 n+2)},\ldots,x_{(3\alpha_1 n)}),\\ (x_{(3\alpha_1 n+1)},x_{(3\alpha_1 n+2)},\ldots,x_{(n)}), & Q<2,\\ (x_{(1)},x_{(2)},\ldots,x_{(\alpha_2 n)}),(x_{(\alpha_2 n+1)},x_{(\alpha_2 n+2)},\ldots,x_{(n-3\alpha_2 n)}),\\ (x_{(n-3\alpha_2 n+1)},x_{(n-3\alpha_2 n+2)},\ldots,x_{(n)}), & 2{,}6<Q\le 3{,}2,\\ (x_{(1)},x_{(2)},\ldots,x_{(\alpha_3 n)}),\ (x_{(\alpha_3 n+1)},x_{(\alpha_3 n+2)},\ldots,x_{(n-\alpha_3 n)}),\\ (x_{(n-\alpha_3 n+1)},x_{(n-\alpha_3 n+2)},\ldots,x_{(n)}), & Q>3{,}2.\end{cases} \qquad (2.4)$$

,

Узагальнену оцінку усередині погодженої експертної групи можна одержати, використовуючи одну з бутстреп-процедур, наприклад, процедуру «розмноження» вибірок (*resampling*). Вона складається з наступних ітерацій:

$$\begin{aligned}&X_j=\{x_{1j},x_{2j},\ldots,x_{ij},\ldots,x_{nj},\}\Rightarrow \bar{x}_0=\frac{1}{n}\sum_{i=1}^{n}x_{ij},\\ &X_j^1=\{x_{2j},x_{3j},\ldots,x_{ij},\ldots,x_{nj},\}\Rightarrow \bar{x}_1=\frac{1}{n-1}\sum_{i=1}^{n-1}x_{ij},\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ &X_j^n=\{x_{1j},x_{2j},\ldots,x_{ij},\ldots,x_{(n-1)j},\}\Rightarrow \bar{x}_n=\frac{1}{n-1}\sum_{i=1}^{n-1}x_{ij},\end{aligned} \qquad (2.5)$$

,

Для одержання найбільш ефективної оцінки аналізуються залишкові різниці по наступних формулах:

$$F_0=\sum_{i=1}^{n}(x_{ij}-\bar{x}_0)^2,\quad F_1=\sum_{i=1}^{n}(x_{ij}-\bar{x}_1)^2,\ldots,\quad F_n=\sum_{i=1}^{n}(x_{ij}-\bar{x}_n)^2, \qquad (2.6)$$

і вибирається $F_i \Rightarrow \min$. Цій величині і буде відповідати одна з оцінок $\bar{x}$ (2.6), яка і приймається в якості узагальненої оцінки.

Технологія аналізу на основі порядкової шкали експертних вимірів.

Дана шкала застосовується для виміру впорядкування (ранжирування) об'єктів по одному або сукупності ознак. Числа в порядковій шкалі використовуються для встановлення порядку між об'єктами за допомогою двох видів відносин: еквівалентності (~) і переваги ($\succ$ *или* $\prec$). У практиці експертного ранжирування найчастіше застосовується числова перевага виді натуральних чисел:

$$r_1 = f(O_1) = 1, \quad r_2 = f(O_2) = 2, \quad \ldots, \quad r_n = f(O_n) = n ,$$

Числа r_1, r_2,…, rn – називаються рангами. Найбільш кращому об'єкту привласнюється перший ранг, другому – другий і т.д.

При груповій експертизі кожний *i*–й експерт привласнює кожному об'єкту j-*й* ранг *rij*. У результаті експертного оцінювання виходить матриця рангів (*rij*), яка трансформується за наступною схемою:

$$(r_{ij}) = \begin{pmatrix} r_{11} & r_{12} & \ldots & r_{1m} \\ r_{21} & r_{22} & \ldots & r_{2m} \\ \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots \\ r_{i1} & r_{i2} & \ldots & r_{im} \\ \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots \\ r_{n1} & r_{n2} & \ldots & r_{nm} \end{pmatrix} \Rightarrow \begin{pmatrix} \bar{R}_1 \\ \bar{R}_2 \\ \ldots\ldots \\ \bar{R}_j \\ \ldots\ldots \\ \bar{R}_m \end{pmatrix} \Rightarrow R_{об.} \qquad (2.7)$$

,

Тут $\bar{R}_j$ – оцінка типу «середнє», отримана по рангах j-*го* стовпця (об'єкта) усіма експертами близькість, що характеризує (подібність*)* рангів $R_{об.}$ rij; – узагальнена ранжировка елементів матриці (2.7). Оцінки $\bar{R}_j$, (*j*=1,..,*m*), згідно з рекомендаціями роботи, можуть бути отримано двома способами: методом середніх арифметичних рангів і методом медіан рангів.

У першому випадку $\bar{R}_j$ має вигляд:

$$\overline{R}_j = \frac{1}{n}\sum_{i=1}^{n} r_i \quad . \qquad (2.8)$$

У другому випадку:

$$\overline{R}_j(med) = \begin{cases} r_{(n+1)/2}, \ \textit{если } n - \textit{нечетное}, \\ [r_{(n/2)} + r_{(1+n/2)}]/2, \ \textit{если } n - \textit{четное}. \end{cases} \qquad (2.9)$$

Попередньо ранги, що становлять елементи матриці (2.9) ранжуються (упорядковуються) по стовпцях у вигляді:

$$r_{1j} \geq r_{2j} \geq \ldots \geq r_{ij} \geq \ldots \geq r_{nj} \quad . \qquad (2.10)$$

В остаточному підсумку $R_{об.}$ може бути представлено двома видами ранжировок:

- *строгій* $R_{об.}: \ r_{1j} \succ r_{2j} \succ \ldots \succ r_{ij} \succ \ldots \succ r_{nj}$;
- *нестрогій* $R_{об.}: \ r_{1j} \succ r_{2j} \succ r_{3j} \sim r_{4j} \sim r_{5j} \succ \ldots \succ r_{ij} \succ \ldots \succ r_{nj}$ (2.11)

Поява в ранжировках (2.11) знака говорить про наявність у них кластерів, наприклад, ($r_{3j} \sim r_{4j}$) . Тоді друга ранжировка з (2.11) може бути представлена так:

$$R_{об.}: \ r_{1j} \succ r_{2j} \succ (r_{3j}, r_{4j}, r_{5j}) \succ \ldots \succ r_{ij} \succ \ldots \succ r_{nj} \quad . \qquad (2.12)$$

При наявності, наприклад *k*, ранжировок виду (2.12) для побудови їх узагальненої усередненої оцінки може бути використана медіана Кемені.

Нехай є $R_{об.1}, R_{об.2}, R_{об.3}, \ldots, R_{об.k}$, тоді вираження для визначення медіани Кемені має вигляд:

$$Arg \min_{R_{об.}} \sum_{i=1}^{k} D(R_{об.i}, R_{об.}) \qquad (2.13)$$

де *Arg* min – значення $R_{об.}$, при яких досягає мінімуму зазначена сума відстаней (заходів близькості) *D* Кемені від ранжировок $R_{об.i}$ до поточної ранжировки $R_{об.}$, по якій і проводиться мінімізація. У такий спосіб:

$$\sum_{i=1}^{k} D(R_{об.i}, R_{об.}) = D(R_{об.1}, R_{об.}) + D(R_{об.2}, R_{об.}) + D(R_{об.3}, R_{об.}) + \ldots D(R_{об.k}, R_{об.}) \qquad (2.14)$$

Слід зазначити, що в обчислювальнім відношенні медіана Кемени є досить складною процедурою. У той час вона дозволяє одержувати єдине коректне результуюче ранжирування.

Технологія аналізу експертних вимірів на основі шкали відносин.

У даній шкалі відбиваються відносини властивостей об'єктів, тобто в скільки раз властивість одного об'єкта перевершує цю ж властивість іншого об'єкта. Відносини, які задаються на шкалі мають вигляд: переваги ($\succ$ *или* $\prec$) і еквівалентність (~).

При виконанні експертних вимірів у шкалі відносин широке поширення одержала процедура попарного порівняння об'єктів.

Якщо, наприклад, є два об'єкти *O1* і *O2*, то при їхньому парнім порівнянні можливі тільки три варіанти результату: *O1* краще *O2* ($O_1 \succ O_2$), *O1* гірше *O2* ($O_1 \prec O_2$), *O1* і *O2* рівноцінні ($O_1 \sim O_2$). Порівнюючи попарно всі об'єкти деякої вихідної множини, наприклад $\{O_1, O_2, O_3, O_4\}$, можна одержати як строгу ($O_1 \succ O_2,\ O_2 \succ O_3, O_3 \succ O_4$), так і нестрогу ($O_1 \succ O_2,\ O_2 \succ O_3, O_3 \sim O_4$) ранжировки. У результаті виконання парних порівнянь формується матриця *Aij* із властивостями зворотної симетричності наступного виду:

$$(A_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \dots\dots & \dots\dots & \dots & \dots\dots \\ a_{i1} & a_{i2} & \dots & a_{im} \\ \dots\dots & \dots\dots & \dots & \dots\dots \\ a_{m1} & a_{m2} & \dots & a_{mm} \end{pmatrix}, \qquad (2.15)$$

де $a_{ij} = 1/a_{ji}$, i=1,…,m і j=1,…,m ставляться відповідно до рядка й стовпцю, а m – число порівнюваних елементів (об'єктів); a_{ij} – деякі позитивні числа.

В основі аналізу матриці (2.’15) лежать процедури знаходження власних векторів, які у свою чергу, використовуються для визначення значень векторів пріоритетів (ранжировок). Зазначені процедури можуть бути реалізовані по наступних схемах:

$$1) \quad (A_{ij}) = \begin{pmatrix} a_{11} + a_{12} + \dots + a_{1m} = A_1 \\ a_{21} + a_{22} + \dots + a_{2m} = A_2 \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ a_{m1} + a_{m2} + \dots + a_{mm} = A_m \end{pmatrix} \Rightarrow \{A = A_1 + A_2 + \dots + A_m\} \Rightarrow$$

$$\Rightarrow \left\{ \frac{A_1}{A} = \omega_1; \frac{A_2}{A} = \omega_2; \dots; \frac{A_m}{A} = \omega_m \right\} \Rightarrow (\omega_1, \omega_2, \dots, \omega_m) \qquad (2.16)$$

де $(\omega_1, \omega_2, \dots, \omega_m)$ – вектор пріоритетів (ω – вагарні коефіцієнти).

$$2) \quad (A_{ij}) = \begin{pmatrix} a_{11} + a_{12} + \dots + a_{1m} = B_1 \\ a_{21} + a_{22} + \dots + a_{2m} = B_2 \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ a_{m1} + a_{m2} + \dots + a_{mm} = B_m \end{pmatrix} \Rightarrow \{B^{-1} = B_1^{-1} + B_2^{-1} + \dots + B_m^{-1}\} \Rightarrow$$

$$\Rightarrow \left\{ \frac{B_1^{-1}}{B^{-1}} = \omega_1; \frac{B_2^{-1}}{B^{-1}} = \omega_2; \dots; \frac{B_m^{-1}}{B^{-1}} = \omega_m \right\} \Rightarrow (\omega_1, \omega_2, \dots, \omega_m) \qquad (2.17)$$

$$3)\qquad (A_{ij}) = \begin{pmatrix} \sqrt[m]{a_{11}\cdot a_{12}\cdot \ldots \cdot a_{1m}} = d_1 \\ \sqrt[m]{a_{21}\cdot a_{22}\cdot \ldots \cdot a_{2m}} = d_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \sqrt[m]{a_{m1}\cdot a_{m2}\cdot \ldots \cdot a_{mm}} = d_m \end{pmatrix} \Rightarrow \{D = d_1 + d_2 + \ldots + d_m\} \Rightarrow \tag{2.18}$$

$$\Rightarrow \left\{ \frac{d_1}{D} = \omega_1; \frac{d_2}{D} = \omega_2; \ldots; \frac{d_m}{D} = \omega_m \right\} \Rightarrow (\omega_1, \omega_2, \ldots, \omega_m)$$

Із трьох наведених схем (2.16 - 2.18) доцільно використовувати третю, тому що в її основі лежить операція визначення геометричного середнього найбільш характерна для шкали відносин.

Для визначення погодженості елементів вектора пріоритетів підраховується індекс погодженості (ІП):

$$ІП = \frac{(\lambda_{max}}{(m-1)} \tag{2.19}$$

де $\lambda_{\max} = \left(\sum_{j=1}^{m1} a_j\right)\cdot \omega_1 + \left(\sum_{j=1}^{m2} a_j\right)\cdot \omega_2 + \ldots + \left(\sum_{j=1}^{mm} a_j\right)\cdot \omega_m -$ максимальне власне число матриці. Крім цього може бути виконана перевірка на наявність транзитивності: якщо $\omega_1 \succ \omega_2$, $\omega_2 \succ \omega_i$, $\omega_i \succ \omega_m$ те $\omega_1 \succ \omega_m$; якщо $\omega_1 \sim \omega_2$, $\omega_2 \sim \omega_i$, $\omega_i \sim \omega_m$ те $\omega_1 \sim \omega_m$; якщо $\omega_1 \succ \omega_2$, $\omega_2 \sim \omega_i$, $\omega_i \succ \omega_m$ те $\omega_1 \succ \omega_m$. Для одержання узагальненої оцінки погодженої множини векторів пріоритетів, як і в попередньому випадку доцільно використовувати медіану Кемені.

На даний час найбільш популярним методом для експертних вимірів у шкалі відносин, є метод аналізу ієрархій і його модифікації (мультиплікативний метод аналізу ієрархій, метод аналізу ієрархій з використанням теорії Демпстера-Шейфера й ін.).

2.2.1 Сфера застосування теорії експертних оцінок.

Існує цілий ряд прикладних завдань, розв'язання яких за допомогою систем, заснованих на знаннях, є ефективнішим, ніж використання інших

підходів. Однак перед застосуванням таких систем важливо врахувати декілька ключових критеріїв:

1. Дані та знання повинні бути достовірними й залишатися незмінними з часом.

2. Обсяг можливих рішень має бути відносно невеликим.

3. Розв’язання задач повинно здійснюватися через формальні логічні міркування.

Варто зазначити, що системи на основі знань ще не здатні ефективно працювати із завданнями, які потребують аналогій чи високого рівня абстрагування — у цьому аспекті людський мозок значно переважає.

У той же час традиційні комп'ютерні програми ефективніші для виконання завдань, пов'язаних із процедурним аналізом. Найкраще області застосування таких систем — завдання, які потребують саме формальних міркувань.

4. Повинен бути принаймні один експерт, здатний чітко сформулювати свої знання та методи їх застосування для вирішення конкретних завдань.

У таблиці 2.1 представлені порівняльні характеристики прикладних завдань, для яких використання експертних систем є доцільним. Загалом не рекомендується застосовувати експертні системи для таких типів завдань: - математичних, які можна розв’язати традиційними формальними перетвореннями чи процедурним аналізом;

- задач розпізнавання, оскільки вони зазвичай вирішуються чисельними методами;

- завдань, де відсутні знання про методи їх розв’язання; через це неможливо створити базу знань.

Таблиця 2.1 - Критерії застосування теорії експертних оцінок.

Застосовні	Непридатні
Не існує суворих алгоритмів чи процедур; рішення базуються на евристичних методах.	Існують ефективні алгоритмічні методи
Завдання вирішуються фахівцями з відповідною кваліфікацією	Бракує фахівців або знання є недостатніми
Завдання переважно стосуються діагностики, інтерпретації чи прогнозування	Завдання є виключно обчислювальними
Доступні дані можуть бути неточними чи "зашумленими".	Використовується точна інформація та чіткі процедури
Рішення ґрунтуються на формальних міркуваннях	Методи вирішення включають аналоги, процедури або інтуїцію.
Знання залишаються статичними (незмінними).	Знання динамічні, адаптуються із часом

Критерії застосування розділяють завдання на дві основні категорії: ті, що можна вирішити за допомогою експертних систем, і ті, де ці системи непридатні. Завдяки евристичним підходам, експертні системи вирішують завдання без потреби точних алгоритмічних методик, тоді як непридатні операції базуються на твердо заданих алгоритмах. Евристичний тип задач залежить від компетентності фахівців, що їх виконують, тоді як у випадку непридатних задач зазвичай відсутня доступна експертиза або необхідні ресурси.

Задачі з першої категорії часто залучаються у контексті аналізу "зашумлених" даних та працюють з невизначеністю. Непридатні ж завдання спираються на точні факти та обчислення. Типова риса застосовності ЕС — це статичність використовуваних знань, що лишаються постійними впродовж тривалого періоду, на відміну від динамічних задач, які регулярно адаптуються до нових умов. Галузі застосування систем на основі знань можна згрупувати у декілька основних категорій: медична діагностика, контроль і управління,

виявлення несправностей у механічних та електронних пристроях, а також навчання. Деякі ключові напрямки використання експертних систем:

Медична діагностика.

Діагностичні системи слугують для визначення зв'язків між порушеннями функціонування організму та їх можливими причинами. Однією з найвідоміших діагностичних систем є MYCIN, розроблена для діагностики та моніторингу стану пацієнтів із менінгітом та бактеріальними інфекціями. Її перша версія з'явилася у Стенфордському університеті в середині 1970-х років. Система ставить діагноз на рівні лікаря-фахівця і має обширну базу знань, що дозволяє використовувати її в інших галузях медицини.

Прогнозування.

Системи прогнозування дозволяють передбачати можливі результати або події, базуючись на поточній інформації про об’єкт. Наприклад, програма "Завоювання Уолл-стріта" аналізує ринкову кон'юнктуру, використовуючи статистичні алгоритми, аби створити план інвестицій. Хоча наразі подібні системи ще не спроможні безпосередньо примножувати капітал через роботу на фінансових ринках як ЕС, вони вже демонструють ефективність у прогнозуванні погоди, врожайності чи пасажиропотоку.

Планування.

Цей напрямок стосується досягнення конкретних цілей за умов великої кількості змінних. Наприклад, компанія Informat запровадила консультаційні робочі станції для клієнтів, які допомагають обрати комп'ютер залежно від бюджету та вимог. Boeing використовує ЕС для проектування космічних станцій і технічного обслуговування авіадвигунів. Система XCON компанії DEC спеціалізується на налаштуванні конфігурації комп’ютерної техніки VAX відповідно до потреб клієнтів. Інтерактивна система XSEL розширює ці можливості та допомагає обрати конфігурацію обчислювальних систем безпосередньо разом із користувачем.

Інтерпретація.

Інтерпретуючі системи володіють здатністю робити висновки на основі отриманих даних спостережень. Однією з найвідоміших інтерпретуючих систем є PROSPECTOR, яка об'єднує знання дев'яти експертів. Ця система, використовуючи комбінацію дев'яти методів експертизи, змогла виявити поклади руди вартістю мільйон доларів, навіть попри те, що жоден із залучених фахівців не передбачав їх існування. Ще однією подібною системою є HASP/SIAP, яка визначає місцезнаходження та типи суден у Тихому океані за допомогою даних акустичних систем стеження.

Контроль і управління.

Знання-орієнтовані системи використовуються як ефективні інтелектуальні засоби для контролю та прийняття рішень, аналізуючи інформацію з різних джерел. Їх уже застосовують на атомних електростанціях, у повітряному русі або для здійснення медичного моніторингу. Такі системи знаходять застосування і в регулюванні фінансової діяльності підприємств, а також допомагають ухвалювати рішення в критичних ситуаціях.

Діагностика несправностей.

У механічних та електричних пристроях системи на основі знань показують свою незамінність як під час проведення ремонтних робіт (наприклад, автомобілів або дизельних локомотивів), так і при усуненні несправностей програмного чи апаратного забезпечення комп’ютерів.

Навчання.

Знання-орієнтовані системи також інтегруються до комп’ютерних навчальних платформ. Вони здатні аналізувати інформацію стосовно діяльності об'єкта (наприклад, студента), адаптуючи свою базу знань та методики відповідно до його поведінки. Як приклад, можна назвати комп’ютерні ігри, складність яких автоматично зростає зі збільшенням рівня майстерності гравця. Особливий інтерес викликає система EURISCO, розроблена Дугласом Ленатом, яка використовує базові евристики. Її успішно тестували у військово-тренувальній грі Тревевелера, яка моделює бойові дії. Завдання гри полягало в

тому, щоб скласти флотилію для ефективної атаки в умовах незмінності набору правил. EURISCO включала до складу флотилії невеликі швидкісні кораблі та одне маневрене судно і протягом трьох років постійно вигравала, навіть незважаючи на щорічну зміну правил гри.

Більшість експертних систем (ЕС) включають набір знань, які можуть належати відразу до кількох типів інформації. Наприклад, навчальна система може мати функціонал для діагностики і планування: вона аналізує здібності студента в межах курсу та формує індивідуальний навчальний план із врахуванням його успіхів. Крім того, керуючі системи можуть бути застосовані для завдань контролю, діагностики, прогнозування та планування. Наприклад, система охорони житла може відстежувати навколишнє середовище, ідентифікувати події (наприклад, відкриття вікна), прогнозувати загрози (проникнення злодія) і розробляти план дій (виклик поліції).

Таким чином, основними сферами застосування експертних систем є медицина, електроніка, комп'ютерна техніка, геологія, математика, космос, сільське господарство, управління безпекою систем критичного призначення, тощо.

2.3 Аналіз стану питання та постановка завдання.

Зосередження загроз життєво важливій інфраструктурі держави є важливим завданням у сфері її безпеки та оборони. Така критична інфраструктура, як енергетика, транспорт, телекомунікації та інші об’єкти, забезпечує нормальне функціонування суспільства і є цілями для можливих загроз. Адекватне оцінювання таких загроз допомагає виявити потенційні ризики для об’єктів критичної інфраструктури та розробити ефективні стратегії їх захисту.

Підходи до оцінювання використовуються залежно від конкретних потреб і характеристик критичної інфраструктури. Один із загальних підходів – це якісне оцінювання, де фахівці використовують свої знання і досвід для надання оцінки загрози на основі категорій, таких як імовірність загроз,

вразливість об’єктів критичної інфраструктури, вплив на неї і можливі наслідки.

Цей підхід може бути корисним для оцінювання загроз на початкових етапах аналізу. Інший підхід – кількісне оцінювання, під час якого фахівці використовують статистичні методи та моделі для оцінювання загроз. Такий підхід використовує конкретні дані та показники для розрахунку ймовірності та впливу загрози. Він може би корисним для більш точного оцінювання загроз у випадках, коли наявні статистичні дані.

Також існує підхід, що комбінує як якісні, так і кількісні оцінювання. Фахівці використовують як свої власні знання та досвід, так і конкретні дані для оцінювання загрози. Цей підхід може бути корисним для більш комплексного аналізу загроз та їхніх наслідків.

Один з методів, що доцільно використовувати для визначення загроз критичній інфраструктурі є метод експертного оцінювання. Цей підхід залучає фахівців з різних областей знань для оцінювання ймовірності та впливу загроз. Фахівці використовують свій професійний досвід і знання, для оцінювання потенційних ризиків.

Доцільність застосування методів експертного оцінювання нададуть можливість вирішення задачі з оцінювання стійкості об’єкту критичної інфраструктури в залежності від впливу факторів вразливостей, які характеризуються високим ступенем невизначеності, складністю строгої формалізації та мають суб’єктивний характер.

Оцінювання загроз критичній інфраструктурі методом експертного оцінювання слід проводити за такою послідовністю [13]:

- формування експертної групи;
- визначення загроз;
- встановлення критеріїв оцінювання;
- проведення збору даних та їх аналіз;
- інтерпретація результатів

Таким чином має бути чітке формулювання завдання, що залежить від виду виникнення проблеми.

Виходячи з даного аналізу, для вирішення задачі дослідження та оцінки залежності впливу факторів вразливостей на стійкість об’єкту критичної інфраструктури, пропонується вирішення наступних завдань:

Завдання дослідження:

1. Провести аналіз сучасних методів та способів дослідження факторів вразливостей на об’єктах критичної інфраструктури.

2. Провести аналіз методів і способів експертного оцінювання у визначені та дослідженні впливу факторів вразливостей на об’єктах критичної інфраструктури.

3. Розробити інформаційну модель дослідження взаємовпливу основних факторів вразливостей на об’єкт критичної інфраструктури.

4. Провести оцінювання та ранжування основних факторів вразливостей на об’єкті критичної інфраструктури.

5. Розробити математичну модель оцінювання залежності стійкості об’єкту критичної інфраструктури від впливу визначених факторів вразливостей.

6. Провести експерименти з оцінки впливу факторів вразливостей на об’єкт критичної інфраструктури по результатам експертного оцінювання.

Висновки до другого розділу.

Проведено аналіз сучасних методів та способів дослідження факторів вразливостей на об’єктах критичної інфраструктури. Визначені особливості застосування методів експертного оцінювання та сфера застосування експертних систем. Зазначена доцільність застосування методів експертного оцінювання що нададуть можливість вирішення задачі з оцінювання стійкості об’єкту критичної інфраструктури в залежності від впливу факторів вразливостей, які характеризуються високим ступенем невизначеності, складністю строгої формалізації та мають суб’єктивний характер.

3. ЗАСТОСУВАННЯ МЕТОДІВ ЕКСПЕРТНОГО ОЦІНЮВАННЯ У ДОСЛІДЖЕННІ ВПЛИВУ ОСНОВНИХ ФАКТОРІВ ВРАЗЛИВОСТЕЙ НА ОБ'ЄКТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

3.1 Розробка інформаційної моделі визначення основних факторів вразливостей на об'єкті критичної інфраструктури.

Основна ціль розробки інформаційної моделі, полягає в використанні її як архітектурного плану завдання отримання та оцінки результатів дослідження.

У контексті визначення та дослідженні факторів вразливостей критичної інфраструктури, відповідно до нормативно-правових вимог і норм, інформаційна модель слугує фундаментом, на якому описуються та попередньо будуються усі функціональні можливості. Модель визначає спосіб обробки даних, підхід до взаємодії з процесами захищеності об'єктів критичної інфраструктури.

Побудова цієї інформаційної моделі передбачає розробку схеми складної мережі інформаційних потоків, зберігання, обробки та використання даних, які лежать в основі поставленої задачі.

Дослідження вразливостей критичної інфраструктури за допомогою експертних методів включає визначення типу інфраструктури, ідентифікацію потенційних загроз, проведення експертної оцінки вразливостей за допомогою структурованих методів (наприклад, узагальненої матриці ризиків) та розробку заходів для зменшення ризиків. Цей процес дозволяє отримати кількісну або якісну оцінку вразливостей та розробити обґрунтовані заходи безпеки.

Етапи дослідження:

1. Визначення об'єкта дослідження:

- Чітко визначити, який об'єкт критичної інфраструктури буде досліджуватися (наприклад, енергетична система, водопостачання, транспортна мережа).
- Визначити критичні елементи та компоненти цього об'єкта.

2. Виявлення потенційних загроз:

- Зібрати інформацію про всі потенційні загрози, як природні (наприклад, стихійні лиха), так і штучні (наприклад, кібератаки, терористичні акти, аварії).

3. Ідентифікація та оцінка вразливостей:

- Використовувати експертні методи для оцінки ступеня вразливості об'єкта до виявлених загроз.
- Методи експертного оцінювання:
  - Узагальнена матриця ризиків: Експерти оцінюють ймовірність настання події та її потенційні наслідки. Результати наносяться на матрицю для візуалізації рівня ризику.

У даному розділі в якості об'єкту критичної інфраструктури буде досліджуватися електромережа.

Аналіз вразливостей в електромережах — це систематичний процес виявлення слабких місць та недоліків у функціонуванні, безпеці та стабільності електромережі, які можуть призвести до збоїв, відмов або бути використані для несанкціонованого доступу чи саботажу. Він включає оцінку ризиків, аналіз уразливостей фізичної та кібербезпеки, а також планування заходів для їх усунення та мінімізації наслідків.

Основні аспекти аналізу вразливостей електромереж:

- Фізична безпека:
  - Оцінка захищеності підстанцій, ліній електропередач та іншого обладнання від фізичних загроз, таких як крадіжки, вандалізм або стихійні лиха.
- Кібербезпека:
  - Виявлення слабкостей у мережевих протоколах, системах управління, комунікаційних каналах та програмному забезпеченні, які використовуються для керування електромережею.
  - Аналіз можливості впровадження шкідливого програмного забезпечення, (Supervisory Control and Data Acquisition) та інших кіберзагроз.
- Операційна стабільність:

- Аналіз уразливостей, пов'язаних з перевантаженнями, старінням обладнання, недостатнім резервуванням та іншими факторами, що можуть спричинити збої у роботі мережі.

- Людський фактор:

- Оцінка ймовірності помилок персоналу, недостатнього рівня підготовки або зловмисних дій з боку співробітників.

- Реагування на надзвичайні ситуації:

- Перевірка ефективності планів реагування на аварії, планових та позапланових відключень, а також здатності швидко відновити роботу мережі після інциденту.

У даній роботі було проведено дослідження Нормативних та регламентуючих документів з експлуатації електромереж які включають [14-20] :

- Правила технічної експлуатації електроустановок споживачів (ПТЕЕС),

- Правила безпечної експлуатації електроустановок (НПАОП40.11.1-97),

- Правила охорони праці при виконанні робіт у діючих електромережах.

А також галузеві нормативні акти такі як ГКД 34.20.507-2003 «Технічна експлуатація електричних станцій і мереж. Правила». Важливу роль також відіграють Кодекси електричної енергії та інші нормативні документи, що регулюють ринок електроенергії.

Основні нормативні документи.

- Правила технічної експлуатації електроустановок споживачів (ПТЕЕС): затверджені наказом Міністерства палива та енергетики України від 25.07.2006 № 258.

- Правила безпечної експлуатації електроустановок (НПАОП 40.1-1.01-97): затверджені наказом від 06.10.1997 р. № 257.

- ГКД 34.20.507-2003 «Технічна експлуатація електричних станцій і мереж. Правила»: редакція наказу від 21.06.2019 № 271.

- Правила охорони праці при виконанні робіт у діючих електроустановках: цей тип документації регулює безпеку при роботі з електричними пристроями, які знаходяться під напругою.

У результаті досліджень були визначені найбільш важливі фактори вразливостей які найчастіше призводять до аварійних ситуацій електромереж.

Результати дослідження наведені в таблиці 3.1.

Для вагомості наведених факторів вразливостей було проведено їх оцінку за допомогою методу експертної теорії – методу кваліметрії (табл. 3.1).

Для визначення взаємовпливу зазначених факторів вразливостей та їх вплив на загальну стійкість об’єкту критичної інфраструктури, яким є **е**лектромережа, застосовувалась теорія експертних оцінок.

Для цього диспетчерам-експертам було запропоновано заповнювати он – лайн модель-анкету по кожному напрямку управління електромережею.

На підставі модель-анкет вивчалась і узагальнювалась отримана інформація типу:

$$Z_k(t_i);\ П_j(t_j);\dots A_e(t_i).$$

$$I_q = \sum_{q=1}^{n1} Z_q(t_i)\,; I_j = \sum_{j=1}^{n2} П_j(t_j);\dots I_e = \sum_{e=1}^{nm} A_e(t_i) \qquad (3.1)$$

Найбільш загальними і важливими для всіх ділянок і служб електромережі експертами було визначено 6 груп основних причин та вразливостей які найчастіше призводять до аварійних режимів роботи, та 24 фактори що обумовлюють виникнення цих причин (табл.3.1).

На підставі результатів дослідження побудована інформаційна модель взаємовпливу зазначених в таблиці 3.1 факторів вразливостей та їх вплив на загальну стійкість об’єкту критичної інфраструктури, яким є електромережа.

Схема інформаційної моделі наведена на рисунку 3.1.

Таблиця 3.1 - Вразливості які найчастіше призводять до аварійних ситуацій електромереж.

Вразливості аварій в електромережі		Вагомість
(LD) - ВИМУШЕНОГО ВІДХИЛЕННЯ ВІД ГРАФІКІВ НАВАНТАЖЕННЯ		
a1	відхилення частоти або перевищення величин граничних перетоків потужності в перетинах по окремих лініях електропостачання.	0,1
a2	несправності пристроїв РЗА, або вимкнення ліній електропередавання, що призводять до обмеження видачі потужності електростанції	0,2
a3	перевищення встановлених контрактних величин перетоків потужності на міждержавних електричних зв'язках	0,2
a4	аварійний вихід з роботи енергоблоків, який може призвести до виникнення значних дефіцитів потужності.	0,5
(EF) - ВИХІД З ЛАДУ ЕЛЕКТРОМЕРЕЖЕВОГО ОБЛАДНАННЯ		
в1	виникнення пожежі	0,5
в2	порушення режимів роботи Перемикань	0,15
в3	відмови автоматичних пристроїв	0,25
в4	порушення допустимих режимів роботи електричних підстанцій	0,1
(OE) - ПЕРЕВАНТАЖЕННЯ ЕЛЕКТРОМЕРЕЖІ		
c1	не дотримання нормальних режимів устаткування, систем, пристроїв	0,3
c2	не своєчасне виявлення загрози виникнення технологічного порушення	0,1

c3	не швидке відновлення енергопостачання споживачів і нормальних параметрів енергії, що відпускається споживачам	0,45
c4	не з'ясовування стану устаткування, що вимкнулося внаслідок технологічних порушень, та можливості, увімкнення його в роботу	0,15
(TV) - ТЕХНОЛОГІЧНИХ ПОРУШЕНЬ (ВІДМОВИ, АВАРІЇ),		
f1	порушена організаційна взаємодія оперативно-диспетчерського персоналу.	0,6
f2	зниження напруги в контрольних вузлах	0,1
f3	зниження частоти	0,1
f4	порушення режиму допустимих перетоків і перевантаження мережних елементів,	0,2
(HF) - ЛЮДСЬКИЙ ФАКТОР		
e1	Психо-функціональний стан ОПР	0,25
e2	Когнітивна складова ОПР	0,2
e3	Психо-емоційний стан ОПР	0,25
c	Професійний рівень ОПР.	0,3
(SF) - ЗБІЙ В РОБОТІ КТЗ ПІДСТАНЦІЙ		
d1	Використання не «сухих» контактів пристроїв релейного захисту і автоматики, блок-контактів коммутаційного приладя.	0,2
d2	Використання промышленных перетворювачів серії Е з уніфікованим виходом 5 мА і швидкодією не менше 0,5 с.	0,15
d3	Наявність встроєної системи автодіагностики, забезпечующої постійний контроль роботоздібності компонент електромеханічного комплексу і ліній звязку.	0,3
d4	Наявність системи автоматичного перезапуска (рестарт) КТС	0,35

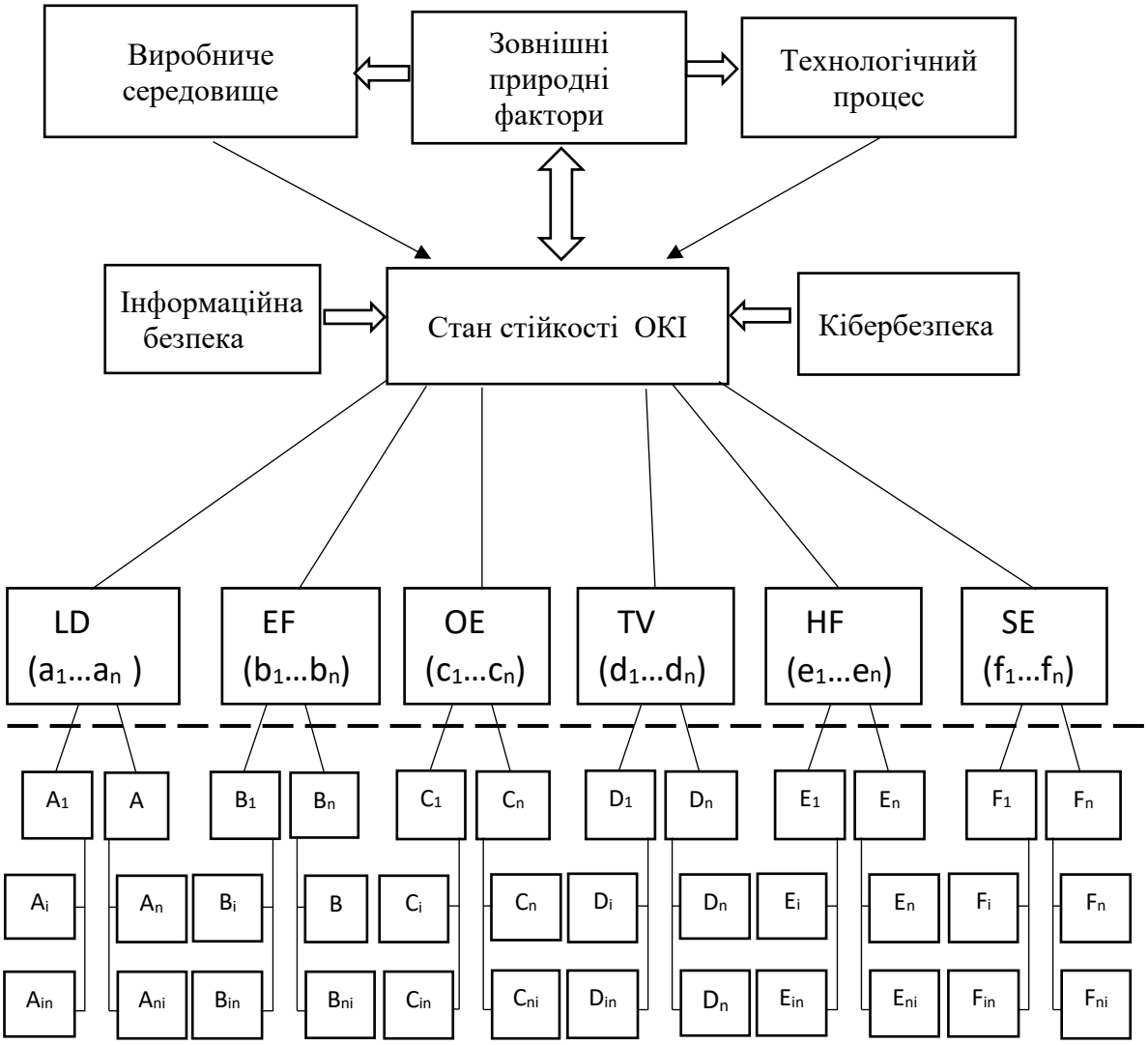

Рисунок 3.1 – Інформаційна модель дослідження факторів вразливостей в електромережі.

У відповідності до інформаційної моделі, вершини LD, EF, OE, TV, HF, SF є причини аварійного стану, а $a_1, a_2, \dots a_n,\ b_1, b_2, \dots b_n,\ c_1, c_2, \dots c_n,\ d_1, d_2, \dots d_n\ , f_1, f_2, \dots f_n$ - відповідні фактори цих причин, які є вершинами типу ″decision″ характеризують ступінь стійкості по відповідним до однойменних факторів $a_1, a_2, \dots, f_n$ і можуть приймати два стани: ″sufficient″ - достатня і ″insufficient″ - недостатня.

На схемі інформаційної моделі складові кожного відповідного фактору під номером i позначаються як $j(a_{ij}, b_{ij}, c_{ij}, d_{ij}, f_{ij})$.

Наприклад, символ a_{11} позначає першу складову фактору під номером 1. Тоді, приймаючи що складові будь-якого фактору рівнозначні, можемо оцінити ступінь стійкості електромережі по фактору a_i:

$$Q_{a_i} = m_{a_i} / n_{a_i}, \tag{3.2}$$

де: m_{a_i} - кількість достатнього рівня складових фактору a_i, n_{a_i} - загальна кількість складових фактору a_i $(i = \overline{1,n})$, при тому, що $0 \le Q_{a_i} \le 1$ для будь-якого значення $i = \overline{1,n}$. Тоді, чим більше значення величини Q_{a_i}, тим вище ступінь стійкості електромережі по фактору a_i. Оцінка ступеня стійкості електромережі по усім факторам b_i , c_i , d_i , f_i $(i = \overline{1,n})$ проводиться аналогічно.

3.2 Оцінка та ранжування основних факторів вразливостей на об'єкті критичної інфраструктури.

У даному розділі для ранжування основних факторів вразливостей електромережі використаний сучасний математичний апарат теорії експертних оцінок [21-34], де експертам-фахівцям пропонувалось провести оцінювання за ступенем важливості кожного представленого у таблиці 3.1 фактору.

Виходячи з умови завдання, де експертизу проводять більше двох експертів, що мають відповідну кваліфікацію і досвід роботи, та необхідно визначити тільки ранги факторів вразливості, то погодженість їх думок доцільно оцінити за допомогою множинного коефіцієнта конкордації K_0 запропонованого М. Кендаллом і Б. Смітом [13].

У якості експертів були фахівці диспетчерського та технічного персоналу електромережі. Де експертам (m) пропонувалося привласнити ранг

(n) інформації перерахованих в анкеті. На підставі отриманих результатів складено матрицю розмірністю (*m**n*)* (табл. 3.2).

Погодженість думок експертів перевіряється за допомогою *F*- критерія Фішера. Де через (*Xij*) позначено ранг j -го виду інформації ($j = \overline{1,n}$) у ранжировці i -го експерта ($i = \overline{1,n}$). Для оцінки підготовленості експертів дотримуємось умови:

$$\sum_{j=1}^{n} X_{ij} = 0{,}5n(n+1) \tag{3.3}$$

де $\sum_{j=1}^{n} X_{ij}$- сума рангів у ранжировці j -го експерта.

Погодженість експертів при ранжировці груп інформації оцінювалася коефіцієнтом конкордації (згоди):

$$K_0 = \frac{12S}{m^2(n^2-n)-m\sum_{i-1}^{m} T_i} \tag{3.4}$$

де $S = \sum_{j-1}^{n} di^2$ - сума квадратів відхилень сум рангів, отриманих усіма групами інформації, від середньо – арифметичного сум рангів

$$d_j = X_j - 0{,}5m(n+1) \tag{3.5}$$

де X_j- відхилення суми рангів j-*го* виду від середнього значення сум рангів по всим видам;

$$T_j = \sum_{\mu=1}^{n}({t_{\mu i}}^3 - t_{\mu i}) \tag{3.6}$$

де $T_{\mu i}$-число повторень μ -го рангу в ранжировці і-*го* експерта.

При $K_0 = 1$ думка експертів вважається узгодженою повністю. При К*о* <*1*, згідно з рекомендаціями для перевірки значимості погодженості визначаються значення статистики X^1 і X^2:

$$X_{\text{набл}}^{(1)} = K_0 m(n-1) \tag{3.7}$$

$$X_{набл}^{(2)} = \frac{(m-1)X^{(1)}}{m(n-1)-X^{(1)}} \tag{3.8}$$

Після чого визначаються числа ступенів свободи (υ1) і (υ2) розподілу, для чого обчислюються значення величин;

$$\upsilon_1 = n-1 \;\; \upsilon_2 = \frac{L^2}{(m-1)\sum_{j=1}^{n} V_j^2} - (m-1) \tag{3.9}$$

де $L = (m-1)\sum_{j=1}^{n} V_j$

$$V_j = \frac{1}{(m-1)\sum_{i=1}^{m}(X_{ij}-X_j^2)} \tag{3.10}$$

$$X_j = \frac{1}{m}\sum_{i=1}^{m} X_{ij} \qquad j = \overline{1,n}$$

По таблиці F – розподілу Фішера порівнюємо критичне значення $F_{кр.}$ при рівні значимості α =0.05 і числах ступеню свободи υ1 і υ2. Порівнюючи отримане значення $X_{\text{набл}}$ зі значеням $F_{кр.}$ робимо висновок, що думки експертів можна вважати погодженими.

У відповідності до результатів оцінювання експертами факторів вразливостей електромережі (таблиця 3.2), можна обчислити коефіцієнт конкордонації за наступною формулою:

$$W = \frac{12 * S}{m^2(n^3-n)} = \quad = \frac{12 * 537}{10^2(10^3-10)} = 0.658, \tag{3.11}$$

де S – сума квадратів середньої суми;

n – кількість факторів;

m – кількість експертів.

Оскільки значення коефіцієнта W ≈ 0.658 є близьким до 1, це вказує що думки експертів узгоджені.

Таблиця 3.2 – Результати оцінювання експертами факторів вразливостей ОКІ.

Експерти *m*	**Вразливості *n***	**Експертні оцінки**									
		LD	**EF**	**OE**	**TV**	**HF**	**SF**	**EN**	**PE**	**IS**	**CS**
E1	Відхилення від графіків навантаження (LD)	5	6	8	7	7	6	8	9	4	7
E2	Збій електромережевого обладнання (EF)	8	9	9	10	7	9	8	10	6	8
E3	Перевантаження електромережі (OE)	8	7	8	8	6	7	6	9	5	8
E4	Технологічні порушеня (TV)	4	6	5	5	8	9	10	2	9	7
E5	Людський фактор (HF)	8	7	9	9	6	8	7	10	6	5
E6	Збій в роботі КТЗ підстанцій (SF)	9	8	9	6	5	7	8	9	8	10
E7	Зовнішні природні фактори (EN)	4	5	7	3	7	6	9	8	2	6
E8	Стан Виробничого середовища (PE)	6	8	7	6	6	7	8	9	6	10
E9	Стан Інформаційної безпеки (IS)	3	8	1	5	9	4	8	9	7	6
E10	Стан Кібербезпеки (CS)	4	8	10	9	7	8	9	8	6	5
$\sum xij$	*Сума*	*59*	*72*	*73*	*69*	*69*	*71*	*81*	*83*	*59*	*72*

Для візуального представлення узгодженості експертних оцінок побудовано гістограму (рис. 3.3), яка демонструє ступінь розбіжності у оцінках експертів.

По результатам проведеного експертного оцінювання, установлена відповідність, між інтервалом значень факторів вразливості електромережі і імовірнісних станів (″sufficient″ або ″insufficient″) відповідного фактору. (табл.3.3).

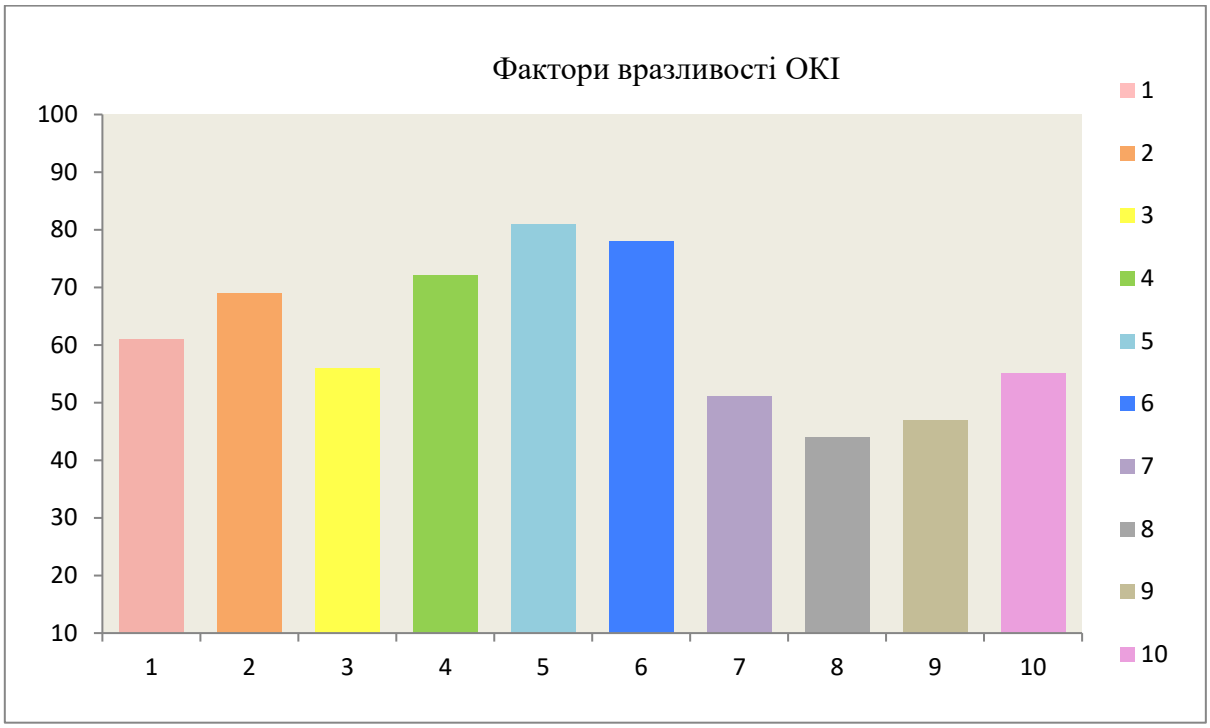

Рисунок 3.2 – Рангова діаграма значимості факторів вразливості електромережі.

Таблиця 3.3 - Результати експертного оцінювання значимості імовірнісних станів факторів вразливості електромережі.

LD			**EF**			**OE**		
	insufficient	sufficient		insufficient	sufficient		insufficient	sufficient
a1	0 – 0,5	0,5 – 1	в1	0 – 0,35	0,35 – 1	c1	0 – 0,4	0,4 – 1
a2	0 – 0,45	0,45 – 1	в2	0 – 0,55	0,55 – 1	c2	0 – 0,55	0,55 – 1
a3	0 – 0,7	0,7 – 1	в3	0 – 0,6	0,6 – 1	c3	0 – 0,6	0,6 – 1
a4	0 – 0,45	0,45 – 1	в4	0 – 0,5	0,5 – 1	c4	0 – 0, 5	0,5 – 1
SF			**TV**					
	insufficient	sufficient		insufficient	sufficient			
d1	0 – 0,4	0,4 – 1	f1	0 – 0,6	0,6 – 1			
d2	0 – 0,4	0,4 – 1	f2	0 – 0,7	0,7 – 1			
d3	0 – 0,4	0,4 – 1	f3	0 – 0,5	0,5 – 1			
d4	0 – 0, 4	0,4 – 1	f4	0 – 0, 55	0,55 – 1			

У відповідності до схеми інформаційної моделі (рис.3.1), можна проаналізувати, що на комплексну стійкість електромережі впливають також складові чинники такі як:

- Зовнішні природні фактори.
- Стан виробничого середовища.
- Стан технологічного процесу.
- Стан інформаційної безпеки .
- Стан кібербезпеки

Результати експертного оцінювання імовірнісного стану зазначених складових чинників що впливають на стійкість електромережі представлені у таблиці 3.4.

Таблиця 3.4 - Результати експертного оцінювання імовірнісного стану складових чинників що впливають на стійкість електромережі.

Фактори впливу на стійкість електромережі	**Стани роботи**		
	Нормальний	**Працездатний**	**Критичний**
Зовнішні природні фактори	0 – 0,45	0,45 – 0,6	0,6 – 1
Стан Виробничого середовища	0 – 0,6	0,6 – 0,75	0,75 – 1
Стан Технологічного процесу	0 – 0,35	0,35 – 0,6	0,6 – 1
Стан Інформаційної безпеки	0 – 0,5	0,5 – 0,75	0,75 – 1
Стан Кібербезпеки	0 – 0,5	0,5 – 0,65	0,65 – 1

3.3 Розробка математичної моделі оцінки впливу основних факторів вразливостей на стійкість об’єкту критичної інфраструктури.

На сьогодні одним з найбільш доцільних математичних інструментів, призначених для роботи з неповною, неточною та суперечливою інформацією, являє собою Байєсовська мережа довіри (БМД), що ґрунтується на

імовірнісному методі й спроможна у найбільшій мірі оперувати відомостями, які надходять з обраних джерел для досягнення найвищого ефекту [35-38].

Байєсівська мережа довіри є статистичним інструментом, який використовується для моделювання зв'язків між різними змінними і робить висновки про ймовірність подій на основі цих зв'язків. Така мережа базується на теорії ймовірностей і використовує в своїй основі правило Байєса для оновлення ймовірностей у разі отримання нової розрахункової інформації.

БМД являють собою графічні моделі подій і процесів на основі об'єднання деяких виводів теорії ймовірностей і теорії графів. Байєсівська мережа (БМ) представляє собою пару <*G*, *B*>, де G – це спрямований ациклічний граф, який записується як набір залежностей і відповідає випадковим змінним, а B – представляє собою множину параметрів, які визначають мережу. Компонента B містить у собі параметри $\Theta_{X^{(i)}|pa(X^i)} = P(X^{(i)}|pa(X^i))$ для кожного можливого значення $x^{(i)} \in X^{(i)}$ та $pa(X^{(i)}) \in Pa(X^{(i)})$, де $Pa(X^{(i)})$ позначає набір батьків змінної $X^{(i)} \in G$, а кожна змінна $X^{(i)} \in G$ подається у вигляді вершини.

Визначення повної спільної ймовірності БМ розраховується за формулою:

$$P_B(X^{(1)}, X^{(2)}, \dots, X^{(N)}) = \prod_{i=1}^{n} P_B(X^{(i)}|P_A(X^{(i)})), \qquad (3.12)$$

де A – множина станів середовища;

$N = (x_1, x_2, \dots, x_N)$ – вектор параметрів їх розподілів.

Розрахунок умовної ймовірності відбувається за наступним співвідношенням:

$$p(E|H_k) = \frac{p(E \cap H_k)}{p(H_k)}, \qquad (3.13)$$

де E та H_k – співзв’язанні змінні мережі.

Умовна ймовірність визначає вірогідність настання події E , за умови того, що конкретна подія H_k відбулась. Вичерпна множина формується подіями що взаємовиключають одна одну за умови настання рівності:

$$\bigcup_{i=1}^{n} E_i = \Omega, \tag{3.14}$$

Якщо змінні між собою не мають однакових значень – вони не перетинаються. Теорія побудови БМ основується на припущені, що події не перетинаються і є вичерпними, у такому випадку ймовірність події E визначаєтья за формулою (3.6) умовних ймовірностей:

$$p(E) = \sum_{i=1}^{n} p(E \cap H_i) \rightarrow \sum_{i=1}^{n} p(E|H_i) * p(H_i), \tag{3.15}$$

Саму ж формулу імовірності перетину двох подій *E* та *H* можна виразити, у наступному вигляді:

$$p(E \cap H_k) = p(E|H_k) * p(H_k) = p(H_k|E) * p(E), \tag{3.16}$$

Дана формула (3.7) може бути трансформована наступним чином:

$$p(H_k|E) = \frac{p(E|H_{k)} * p(H_k)}{p(E)}, \tag{3.17}$$

Беручи до уваги формули (3.15) та (3.17), процес обчислення події E можна представити у наступному вигляді:

$$p(H_k|E) = \frac{p(E|H_{k)} * p(H_k)}{\sum_{i=1}^{n} p(E|H_i) * p(H_i)}, \tag{3.18}$$

Мережа Байеса, зформована на підставі формули (3.18), являє собою спрямований ациклічний граф, де кожний вузол являє собою змінну, а кожна

дуга – імовірнісну залежність, обумовлену кількісно використанням умовного розподілу ймовірностей для кожного вузла.

До складу мережі Байеса входять наступні компоненти:

– множина вузлів, що визначають компоненти системи;

– множина спрямованих зв'язків між компонентами системи.

Загальний план зв’язків змінних та визначення зовнішніх та системних факторів впливу представлено у вигляді моделі Байєсовської мережі довіри на рисунку 3.3.

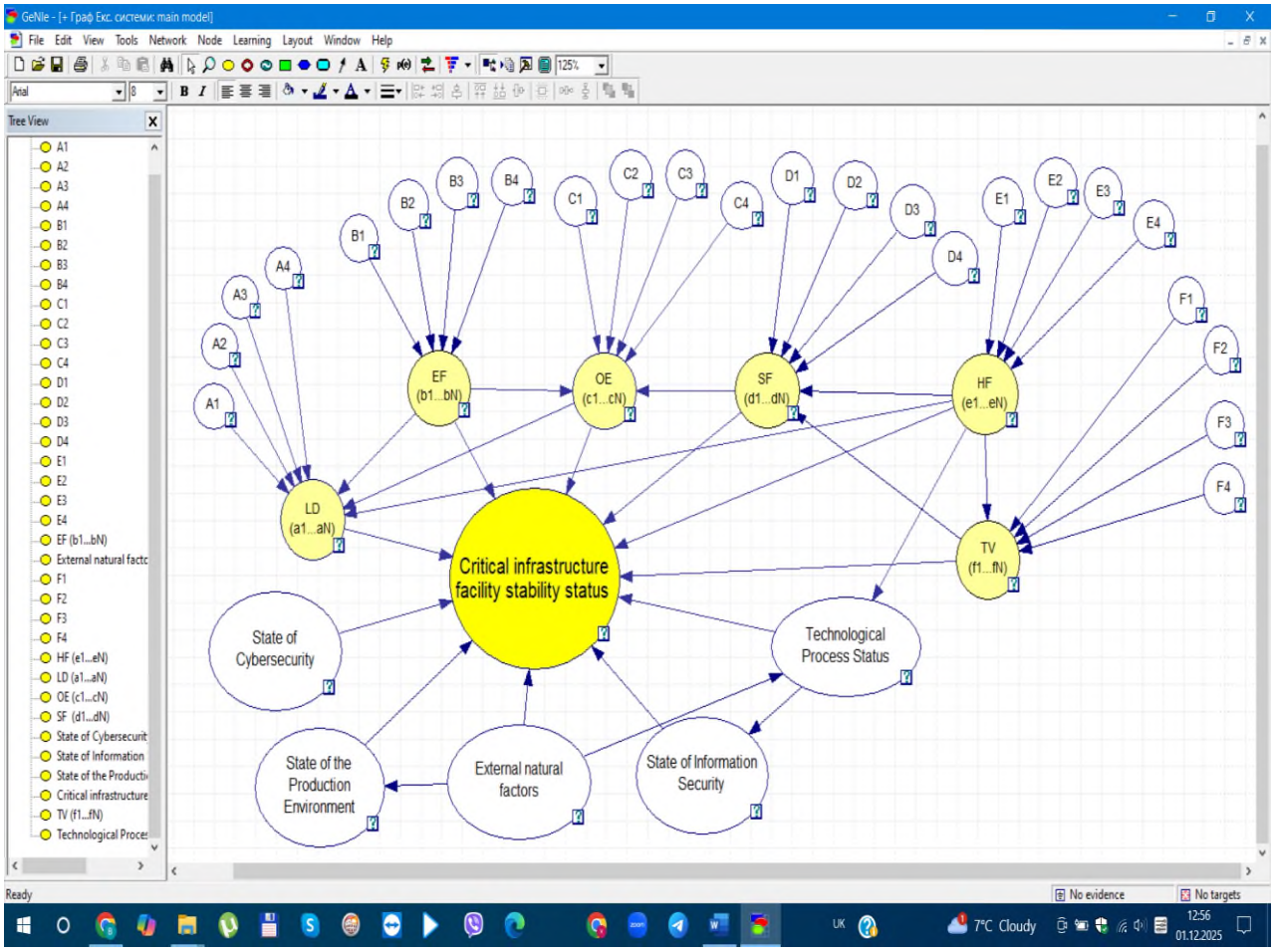

Рисунок 3.3 - Граф БМД оцінки впливу основних факторів вразливостей на стійкість об’єкту критичної інфраструктури.

Таким чином, за формулою (3.18) стан стійкості електромережі у відповідності до імовірнісного стану будь-якого із факторів вразливості,

наведених в таблиці 3.1, можна визначити значення вершини ″Critical infrastructure facility stability status″ Байєсовської мережі [39-41].

Для оцінки імовірнісної стійкості електромережі у БМД вводяться вершини складових чинників. такі як:

- “External natural factors”;
- “State of the Production Environment”;
- “Technological Process Status”;
- “State of Information Security”;
- “State of Cybersecurity”.

Дані вершини є вершинами типу ″decision″ і можуть приймати три стани: ″normal″, ″workable″ і ″critical″. Для оцінки стану вершин складових чинників у складі електромережі також був використаний сучасний математичний апарат теорії експертних оцінок.

Вершини LD, EF, OE, TV, HF, SF відповідають зазначеним вище факторам вразливості, які являються причинами виникнення збоїв і аварій в електромережі. Вони бінарні і приймають значення ″occurs″, якщо відповідна причина виникнення збоїв і аварій в електромережі існує, і ″ not occurs ″ якщо ні.

Вершина ″Critical infrastructure facility stability status″ характеризує стан стійкості і приймає тільки два значення: ″workable″, якщо стан стійкості припустимий, і ″critical″, у випадку якщо стан стійкості неприпустимий.

Зазначемо, що розглянуті вершини мають тип Noisy MAX, що дасть можливість експертам значно простіше оцінювати значення безумовної ймовірності, чим умовної.

Для опису зашумленних вершин LD, EF, OE, TV, HF, SF, ″Critical infrastructure facility stability status″ експертами-фахівцями було проведено оцінювання умовних ймовірностей можливих станів зазначених вершин. Результати оцінювання представлені в таблицях 3.5 – 3.11.

Таблиця 3.5 – Опис вузла LD

Батько	a_1		a_2		a_3		a_4	
Стан	**insuffi-cient**	**suffi-cient**	**insuffi-cient**	**suffi-cient**	insuffi-cient	**suffi-cient**	**insuffi-cient**	**suffi-ient**
occurs	0,25	0	0,3	0	0,25	0	0,25	0
not occurs	0,75	1	0,7	1	0,75	1	0,75	1

Батько	EF		OE		HF	
Стан	**occurs**	**not occurs**	**occurs**	**not occurs**	**occurs**	**not occurs**
occurs	0,1	0	0,15	0	0,1	0
not occurs	0,9	1	0,85	1	0,9	1

Таблиця 3.6 – Опис вузла EF

Батько			b_2		b_3		b_4	
Стан	**insuffi-cient**	**suffi-cient**	**insuffi-cient**	**suffi-cient**	**insuffi-cient**	**suffi-cient**	**insuffi-cient**	**suffi-cient**
occurs	0,3	0	0,3	0	0,4	0	0,25	0
not occurs	0,7	1	0,7	1	0,6	1	0,75	1

Таблиця 3.7 - Опис вузла OE

Батько			c_2		c_3		c_4	
Стан	**insuffi-cient**	**suffi-cient**	**insuffi-cient**	**suffi-cient**	**insuffi-cient**	**suffi-cient**	**insuffi-cient**	**suffi-cient**
occurs	0,3	0	0,25	0	0,2	0	0,25	0
not occurs	0,7	1	0,75	1	0, 8	1	0,75	1

Батько	EF		SF	
Стан	**occurs**	**not occurs**	**occurs**	**not occurs**
occurs	0,1	0	0,1	0
not occurs	0,9	1	0,9	1

Таблиця 3.8 - Опис вузла SF

Батько	d_1		d_2		d_3		d_4	
Стан	**insuffi-cient**	**suffi-cient**	**insuffi-cient**	**suffi-cient**	**insuffi-cient**	**suffi-cient**	**insuffi-cient**	**suffi-cient**
occurs	0,2	0	0,35	0	0,25	0	0, 2	0
not occurs	0,8	1	0,65	1	0,75	1	0,8	1

Батько	TV	
Стан	**occurs**	**not occurs**
occurs	0,1	0
not occurs	0,9	1

Таблиця 3.9 - Опис вузла HF

Батько	Psycho-functional state of the OPR		Cognitive component of OPR		Psycho-emotional state of the OPR	
Стан	**insuffi-cient**	**suffi-cient**	**insuffi-cient**	**suffi-cient**	**insuffi-cient**	**suffi-cient**
occurs	0,3	0	0,2	0	0,15	0
not occurs	0,7	1	0,8	1	0,85	1

Таблиця 3.10 - Опис вузла TV

Батько	f_1		f_2		f_3		f_4	
Стан	**insuffi-cient**	**suffi-cient**	**insuffi-cient**	**suffi-cient**	**insuffi-cient**	**suffi-cient**	**insuffi-cient**	**suffi-cient**
occurs	0,1	0	0,05	0	0,2	0	0,15	0
not occurs	0,9	1	0,95	1	0,8	1	0,85	1

Батько	HF	
Стан	**occurs**	**not occurs**
occurs	0,1	0
not occurs	0,9	1

Таблиця 3.11 - Опис вузла ″Critical infrastructure facility stability status″

Батько	LD		EF		OE		SF	
Стан	**occurs**	**not occurs**	**occurs**	**not occurs**	**occurs**	**not occurs**	**occurs**	**not occurs**
critical	0,3	0	0,35	0	0,25	0	0,2	0
workable	0,7	1	0,65	1	0,75	1	0,8	1

Батько	HF		TV		External natural factors		
Стан	**occurs**	**not occurs**	**occurs**	**not occurs**	**critical**	**workable**	**normal**
critical	0,2	0	0,2	0	0,05	0,01	0
workable	0,8	1	0,8	1	0,95	0,99	1

Батько	State of the Production Environment			Technological Process Status		
Стан	**critical**	**workable**	**normal**	**critical**	**workable**	**normal**
critical	0,05	0,01	0	0,05	0,01	0
workable	0,95	0,99	1	0,95	0,99	1

Батько	State of Information Security			State of Cybersecurity		
Стан	**critical**	**workable**	**normal**	**critical**	**workable**	**normal**
critical	0,05	0,01	0	0,05	0,01	0
workable	0,95	0,99	1	0,95	0,99	1

3.4 Практична реалізація оцінки впливу факторів вразливостей на об’єкт критичної інфраструктури по результатам експертного оцінювання.

Для практичної реалізація оцінки впливу факторів вразливостей на об’єкт критичної інфраструктури по результатам експертного оцінювання, використано графічний мережевий інтерфейс GeNIe 2.0, який представляє собою програмне середовище, створене в Університеті Піттсбурга для Microsoft Windows і пропонується безкоштовно у Genie. Даний інтерфейс є корисним для оцінки

рішень та для візуального зображення поєднання імовірностей та мережевих процесів. Зокрема, Genie можна застосовувати для дослідження Байєсівських мереж, або спрямованих ациклічних графів (тобто події у павутинні взаємозв'язків є умовно незалежними одна від одної). Байєсівські мережі або динамічні Байєсівські мережі (DBN) мають застосування у виробничому контролі, оскільки моделювання процесу з використанням DBN дає змогу враховувати зашумлені дані та міри невизначеності; вони можуть бути успішно застосовані для передбачення вірогідностей пов'язаних результатів у системі. У Байєсівських мережах додавання більшої кількості зв'язків та міркувань суттєво підвищує заплутаність задіяних обчислень, і Genie дає змогу вивчати ці заплутані системи. До того ж, графічний інтерфейс спрощує наочне розуміння мережі.

Байєсівська мережа відображається у графічному середовищі Genie. й структурує мережу вузлів та міркувань у конфігурації, яка легко сприймається візуально і є корисною як для простих, так і для надзвичайно заплутаних систем.

Виходячи з зазначеного, для оцінки стану режимів роботи електромережі, у відповідності до факторів вразливостей, використано запропонований спосіб на базі математичного апарату БМД, та теорії нечітких множин. Даний спосіб докладніше наведено в (р. 3.3). При цьому, результати експертного оцінювання, наведених у (табл. 3.5–3.11), отримані шляхом практичного дослідження, що дає можливість отримати результати наступних експериментів.

На начальному етапі експертами – фахівцями проводилось оцінювання факторів вразливостей і причин які призводять до аварійності роботи електромережі. Гістограми результатів ранжованого розподілу причин і факторів, згідно (табл.3.1 р.3.1), наведені на рисунку 3.4.

Для визначення критеріїв оцінки стану стійкості електромережі були сформульовані критерії, які визначали експерти у відповідності до ПРАВИЛ експлуатації електротехнічного обладнання, де технічний стан електромережі характеризується наступними режимами роботи:

- Нормальний, що дозволяє подальше використання обладнання;

- Працездатний, при якому дозволяється наявність дефектів, які не впливають на виконання обладнанням своїх функцій, але потребуючих прийняття заходів для усунення дефектів;

- Критичний, що потребує негайного виводу обладнання з роботи та прийняття заходів для діагностичного обстеження задля виявлення та усунення дефектів чи прийняття рішення про заміну обладнання.

При цьому за еталонний абсолютний показник критерію вибрано одиницю.

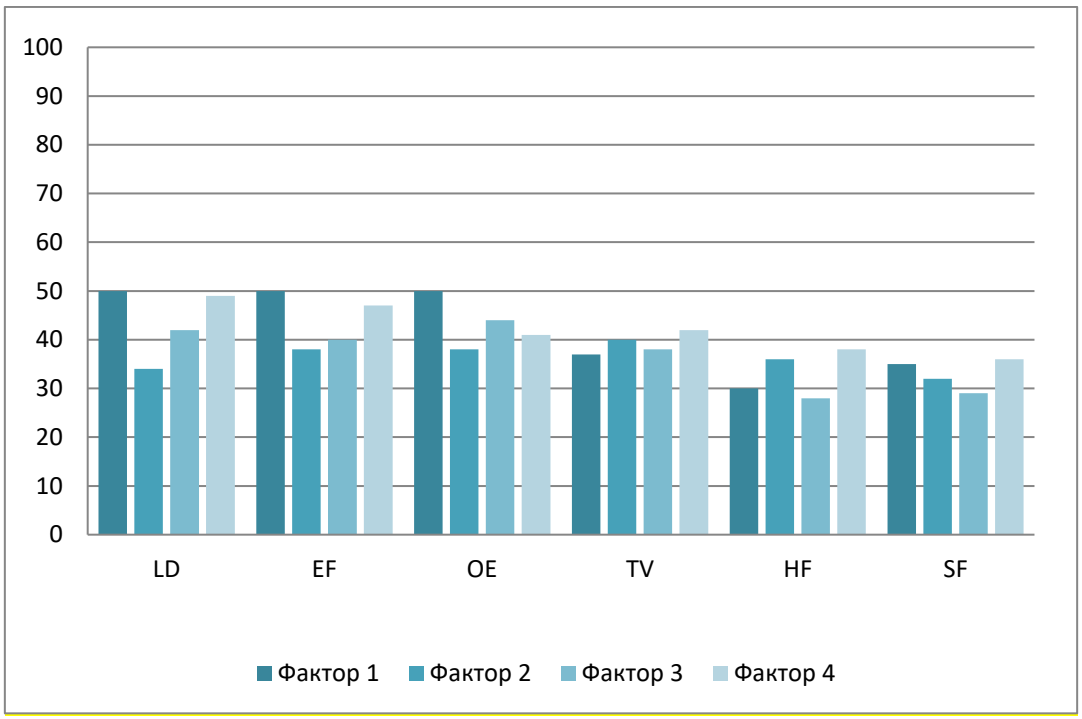

Рисунок 3.4 - Вагомість впливу факторів вразливостей на причини аварій в електромережі.

Експеримент 1.

У деякий час аварійного стану результат сканування електромережі показав, що вершини факторів a2, a4, b2, b4, c1, c4, d1, d4, e2, e4, f1,f4 – приймають стан ″sufficient″, а решта вершин факторів знаходяться у стані ″insufficient″.

Показники вразливостей LD, EF, OE, TV, HF, SF, та складових чинників мережі “Technological Process Status”, “State of Information Security”, “State of

Cybersecurity", "State of the Production Environment" - перебувають у критичному стані. При цьому стан стійкості електромережі, вершина ″Critical infrastructure facility stability status″ має всього 5%. (рис. 3.5).

Звернемо увагу на те, що причини LD, EF, OE, TV, HF, SF виникненя збоїв і аварій в електромережі мають ймовірності 17%, 43%, 22 %, 50%, 37% відповідно, то найбільший вплив на стан стійкості електромережі має та вразливість, яка має найбільшу вагомість (табл.3.2).

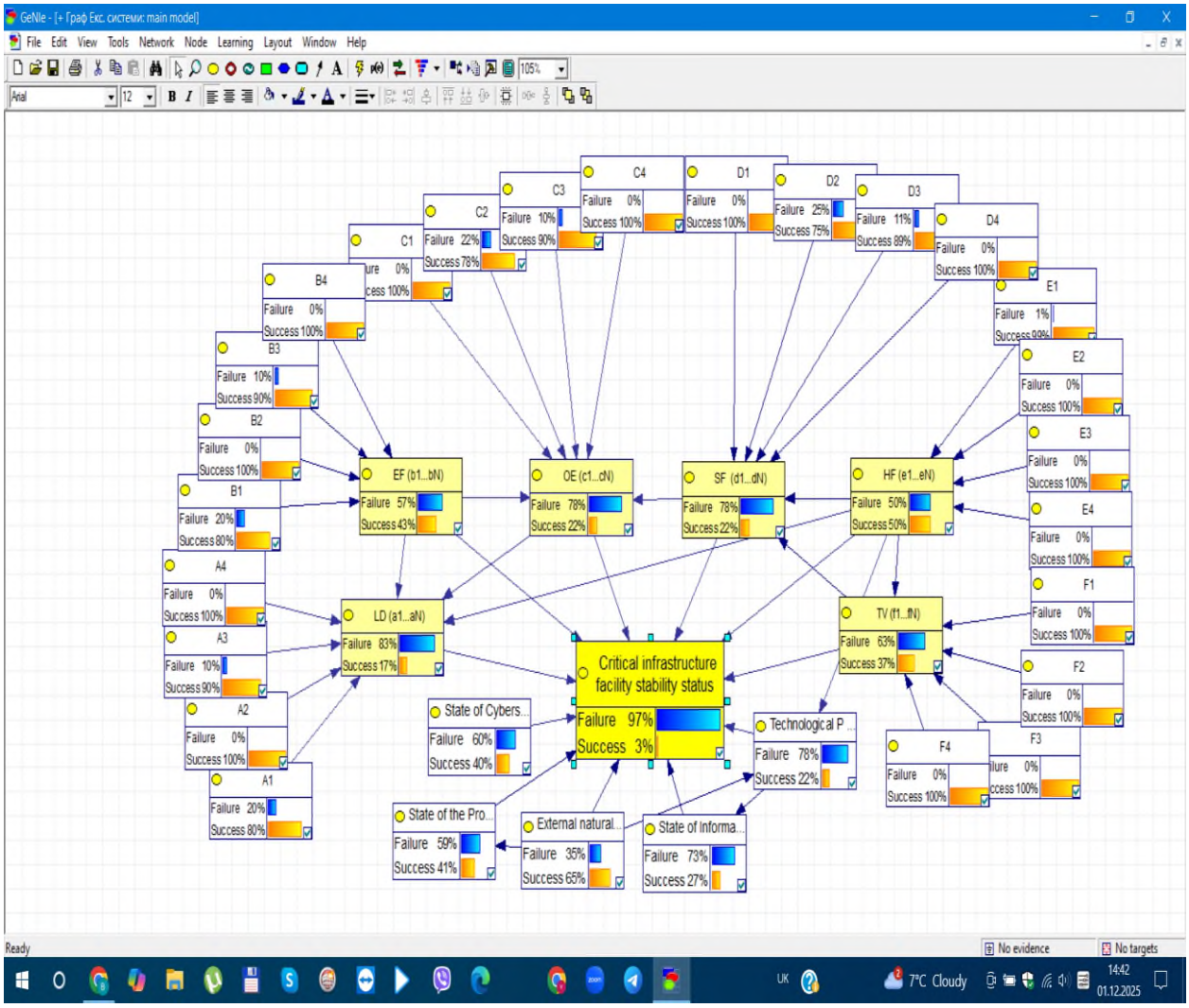

Рисунок 3.5 - Результати оцінки стану стійкості електромережі визначених по БМД (експеримент 1).

Експеримент 2.

Після проведення необхідних заходів з локалізації аварійного стану електромережі результат сканування показав, що усі вершини факторів мають

стан - ″sufficient″. Показники вразливостей LD, EF, OE, TV, HF, SF мають нормальний стан – “normal” 83%, 85%, 83%, 85%, 79% відповідно.

Складові чинники мережі “Technological Process Status”, “State of Information Security”, “State of Cybersecurity”, “State of the Production Environment” - перебувають у працездатному стані – “working condition” 51%, 50%, 60%, 55%, відповідно.

При цьому стан стійкості електромережі, вершина ″Critical infrastructure facility stability status″ становить 95%. (рис. 3.6).

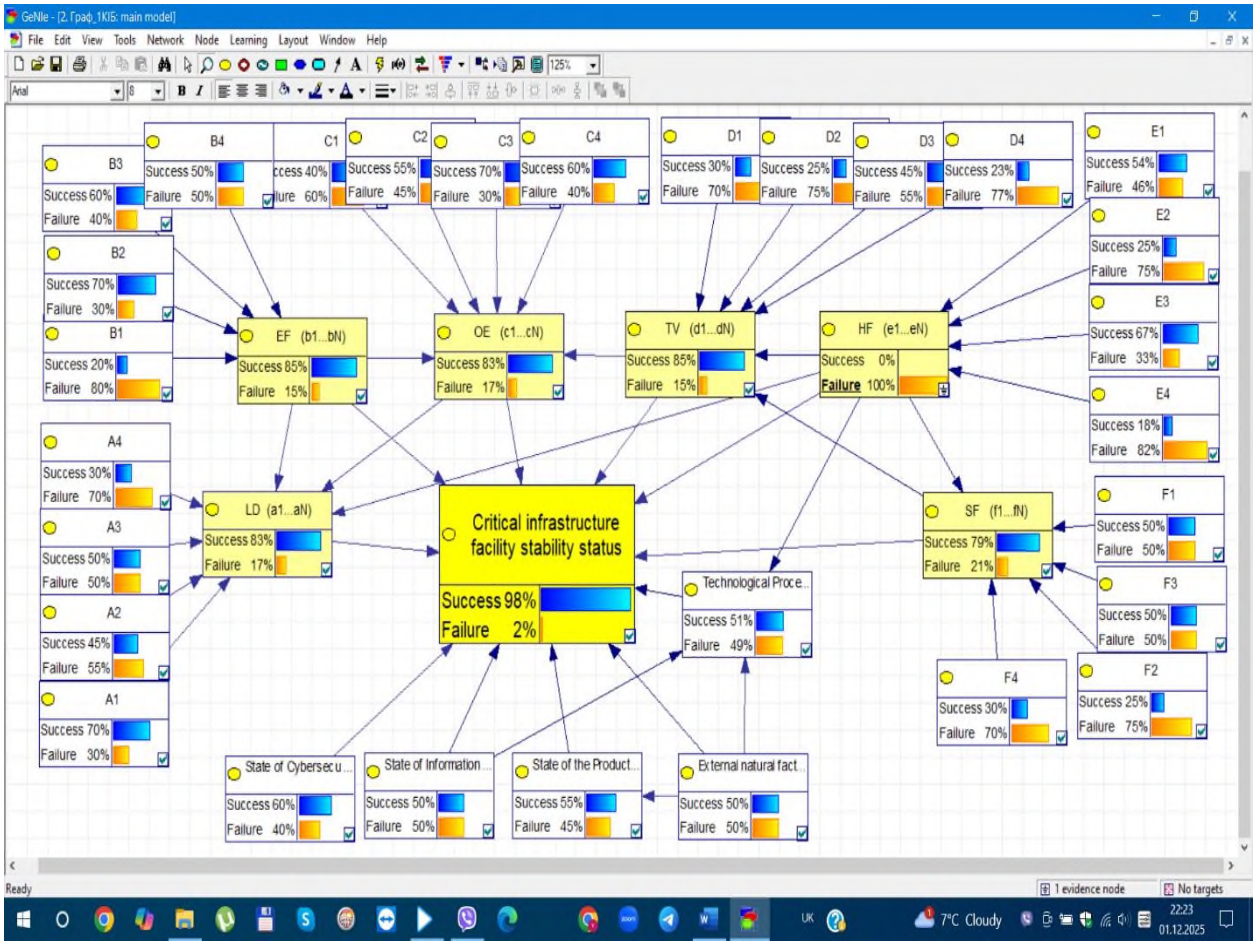

Рисунок 3.6 - Результати оцінки стану режимів роботи електромережі визначених по БМД після корекції (експеримент 2)

Експеримент 3.

Після проведення повних регламентних заходів по захищеності та стійкості електромережі результат сканування показав, що усі вершини

факторів – a, b, c, d, e, f мають стан - ″sufficient″. Показники вразливостей LD, EF, OE, TV, HF, SF мають стан “normal” - 100%, 90%, 100%, 100%, 90%, 94% відповідно. Складові чинники мережі “Technological Process Status”, “State of Information Security”, “State of Cybersecurity”, “State of the Production Environment” - перебувають у стані “normal” - 100%, 100%, 90%, 90%, 94% відповідно.

При цьому стан стійкості електромережі, вершина ″Critical infrastructure facility stability status″ становить 100%. (рис. 3.7).

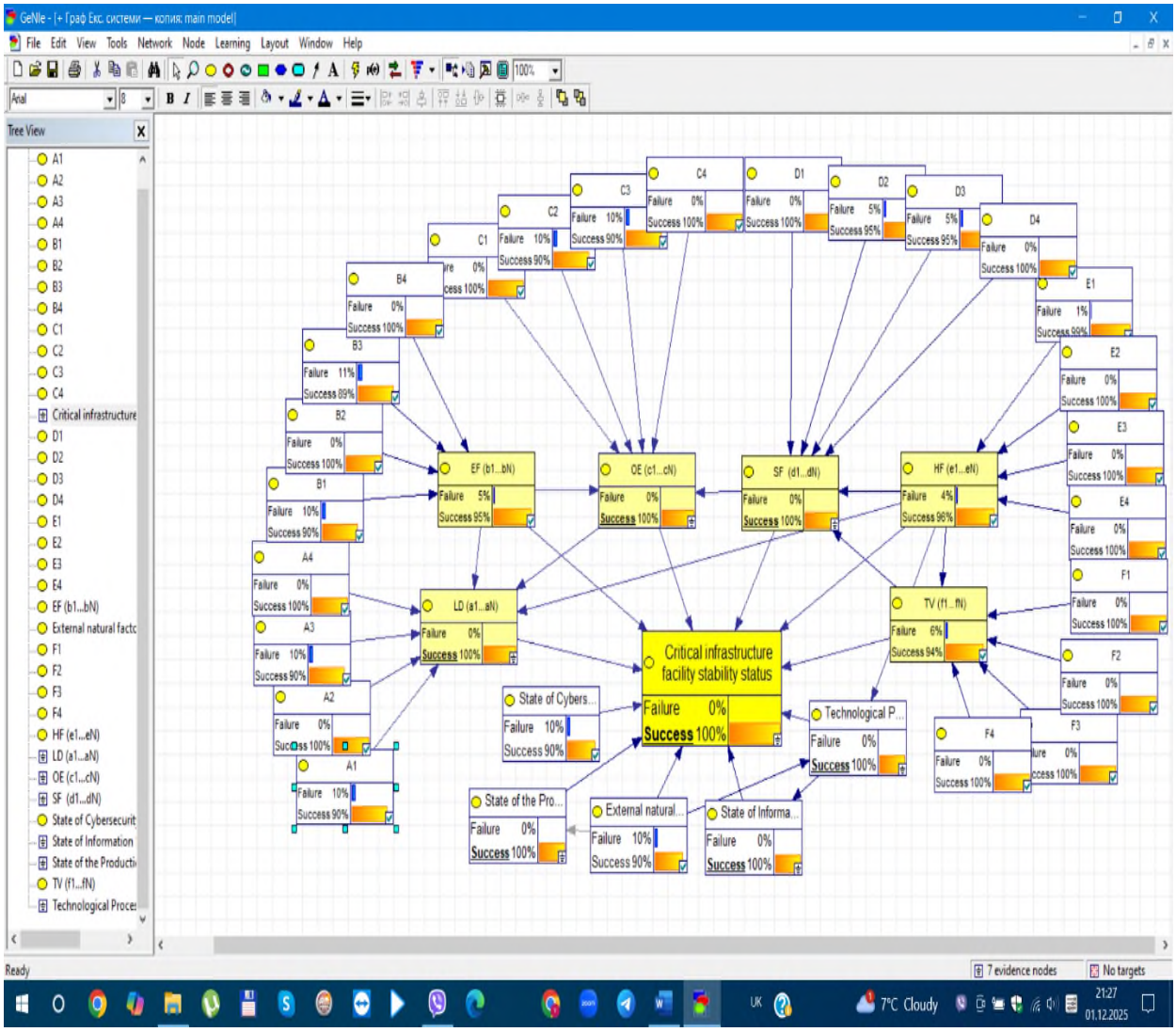

Рисунок 3.7 - Результати оцінки стану режимів роботи електромережі визначених по БМД після регламентних заходів (експеримент 3).

Висновки по третьому розділу.

У третьому розділі досліджувалась проблема визначення та оцінювання впливу факторів вразливостей на стійкість об’єкту критичної інфраструктури з використанням методів експертного оцінювання.

Досліджені питання з визначення та проведена класифікація основних факторів вразливостей що впливають на захищеність електромережі. Для визначення та оцінки залежності стійкості об’єкта критичної інфраструктури від впливу факторів вразливостей розроблено інформаційну та інформаційно – логічну модель з використанням методів експертного оцінювання.

Для прогнозування рівня безпекового стану та залежності стійкості об’єкту критичної інфраструктури від впливу факторів визначених вразливостей використовувались теорія експертних оцінок та графо-аналітичні методи Байесовської мережі довіри.

Проведено ряд експериментів з оцінювання залежності стійкості об’єкту критичної інфраструктури від впливу факторів вразливостей з використанням методів експертного оцінювання.

ВИСНОВКИ

Магістерська робота присвячена дослідженню актуальної проблеми визначення кількісної оцінки впливу факторів вразливостей на стійкість об'єктів критичної інфраструктури. У ході роботи проведено глибокий аналіз існуючих методів оцінювання вразливостей, а також ідентифіковано та класифіковано основних факторів, що знижують захищеність таких об'єктів.

Досліджені питання та проведена класифікація основних факторів вразливостей що впливають на захищеність електромережі. Для визначення та оцінки залежності стійкості об’єкта критичної інфраструктури від впливу факторів вразливостей розроблено інформаційну та математичну модель з використанням методів експертного оцінювання.

Для прогнозування рівня безпекового стану та залежності стійкості об’єкту критичної інфраструктури від впливу факторів визначених вразливостей використовувались теорія експертних оцінок та графо-аналітичні методи Байесовської мережі довіри.

Проведено ряд експериментів які підтвердили ефективність оцінювання залежності стійкості об’єкту критичної інфраструктури від впливу факторів вразливостей з використанням методів експертного оцінювання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон «Про критичну інфраструктуру» від 16.11.2021 Форма доступу - https://zakon.rada.gov.ua/laws/show/1882-20

2. Закон України Про національну безпеку України Форма доступу - https://zakon.rada.gov.ua/laws/show/2469-VIII

3. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" Указ Президента України; Стратегія від 26.08.2021 Форма доступу - https://www.president.gov.ua/documents/4472021-40013

4. Закон України "Про основи національної безпеки України" 19 червня 2003 року № 964-IV. URL: https://zakon.rada.gov.ua/laws/show/964-15#Text

5. Закон України "Про основні засади забезпечення кібербезпеки України" 5 жовтня 2017 року № 2163- VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

6. Указ Президента України. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року "Про Стратегію забезпечення державної безпеки". 16 лютого 2022 року № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text

7. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про запровадження національної системи стійкості»: Указ Президента України від 27.09.2021 № 479/2021. URL:https://www.president.gov.ua/documents/4792021-40181 (дата звернення: 29.09.2021).

8. Суходоля О. М. Стійкість критичної енергетичної інфраструктури та життєдіяльності громад. Нац. ін-т стратег. дослідж., 2024. – с.132-135URL: https://doi.org/10.53679/niss-analytrep.2024.04

9. Кількісні методи експертного оцінювання : наук.-метод. розробка / уклад. : В.П. Новосад, Р.Г. Селіверстов, І.І. Артим. Київ : НАДУ, 2009. 36 с

10. Олексієнко, Р., & Донець, А. (2021). Місце експертної оцінки у прийнятті управлінських рішень. Економіка та суспільство, (26). https://doi.org/10.32782/2524-0072/2021-26-59

11. Fisun M. T., Kandyba I. O., Borovlyova S. Y., Falenkova M.V. Development of software platforms for scenario generation using DSL and Neo4j graph database. Systemy zarządzania i społecznogospodarcze: naukowe i praktyczne aspekty zrównoważonego rozwoju administrative and socio-economic systems:scientific and practical aspects of sustainable development: Monograph, Opole: The Academy of Management and Administration in Opole, 2021, 145-155 pp

12. Galanis P. The Delphi method. Archives of Hellenic Medicine. 2018. 4. І. О. Кандиба, М. Т. Фісун, Г. В. Горбань, К. О. Антіпова. Генерація сценаріїв вступної кампанії закладу вищої освіти на основі когнітивної карти та предметно-орієнтованої мови програмування. Вчені записки Таврійського національного університету імені В. І. Вернадського, 2021. №3 т.32(71) – С. 96- 104.

13. Коваленко І. І., Швед А. В., Антіпова К. О. Моделі подання та виведення знань у системах ситуаційного управління. Миколаїв: Іліон, 2018. 92 С

14. Суходоля О. М. Проблеми визначення сфери регулювання енергетичної безпеки. Стратегічні пріоритети. 2019. № 1. С. 5–17.

15. Суходоля О. М. Системний підхід в оцінюванні стану та цілепокладанні у сфері енергетичної безпеки. Стратегічна панорама. 2019. № 1-2. С. 58–72.

16. Про національну безпеку : Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 24.09.2021).

17. Енергетична безпека України: методологія системного аналізу та стратегічного планування : аналіт. доп. ; за заг. ред. О. М. Суходолі. Київ : НІСД, 2020. 178 с.

18. ISO 31000. Risk management / ISO. URL: https://www.iso.org/iso-31000-riskmanagement.html (дата звернення: 24.09.2021).

19. Risk assessment methodologies for critical infrastructure protection. Part II: A new approach. URL: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC96623/lbna27332enn.pdf (дата звернення: 24.09.2021).

20. Суходоля О. М., Харазішвілі Ю. М., Бобро Д. Г. Методологічні засади ідентифікації та стратегування рівня енергетичної безпеки України. Економіка України. 2020. № 6(703). С. 20–42. URL: https://doi.org/10.15407/economyukr.2020.06.020 (дата звернення: 24.09.2021).

21. Харазішвілі Ю. М. Системна безпека сталого розвитку: інструментарій оцінки, резерви та стратегічні сценарії реалізації : монографія ; НАН України, Ін-т економіки промисловості. Київ, 2019. 304 с.

22. Kharazishvili Yu., Kwilinski A., Sukhodolia O., et. al. The Systemic Approach for Estimating and Strategizing Energy Security: The Case of Ukraine. Energies. 2021. Vol. 14.2126. URL: https://doi.org/10.3390/en14082126 (дата звернення: 24.09.2021).

23. Про схвалення Стратегії енергетичної безпеки : Розпорядження Кабінету Міністрів України від 04.08.2021 № 907-р. URL: https://www.kmu.gov.ua/npas/proshvalennya-strategiyi-energetichn-a907r (дата звернення: 24.09.2021).

24. Визначення рівня енергетичної безпеки України : аналіт. доп. / [Суходоля О. М., Харазішвілі Ю. М., Бобро Д. Г., Рябцев Г. Л., Завгородня С. П.] ; за заг. ред. О. М. Суходолі. Київ : НІСД, 2021. 71 с.

25. References 1. Li, Z., Du, P., Li, T. (2025). Comprehensive Risk Assessment of Smart Energy Information Security- An Enhanced MCDMBased Approach. Sustainability, 17(8), 3417.

26. Alhakami, W. (2023). Computational Study of Security Risk Evaluation in Energy Management and Control Systems Based on a Fuzzy MCDM Method. Processes, 11(5), 1366.

27. Janta, P., Leeraphun, N., Thapmanee, K., et al. (2024). Energy resilience assessment- Incorporating consideration of recoverability and adaptability in risk assessment of energy infrastructure. Energy for Sustainable Development, 81, 101506.

28. Zheng, Y., Xue, X., Xi, S., Xin, W. (2024). Balancing possibilist–probabilistic risk assessment for smart energy hubsEnabling secure peer-to-peer energy sharing with CCUS technology and cyber-security. Energy, 304, 132102.

29. Goodell, J.W., Corbet, S. (2023). Commodity market exposure to energy-firm distress- Evidence from the Colonial Pipeline ransomware attack. Finance Research Letters, 51, 103329.

30. Fan, J., Yang, W., Liu, Z., et al. (2023). Understanding Security in Smart City Domains from the ANT-Centric Perspective. IEEE Internet of Things Journal, 10(12), 11199–11223.

31. Wang, X., Li, S., Rahman, M.A. (2024). A Comprehensive Survey on Enabling Techniques in Secure and Resilient Smart Grids. Electronics, 13(2177).

32. Hu, J.-L., Chen, Y.-C., Yang, Y.-P. (2022). The Development and Issues of Energy-ICT- A Review of Literature with Economic and Managerial Viewpoints. Energies, 15(2), 594.

33. Bouramdane, A., Lin, J., Yahyaoui, A., et al. (2023). Cyberattacks in Smart Grids- Challenges and Solving the Multi-Criteria Decision-Making for Cybersecurity Options (Including Ones That Incorporate Artificial Intelligence) Using an Analytical Hierarchy Process. Journal of Cybersecurity and Privacy, 3(4), 31.

34. Abouzar, O., Gasmi, A., Derdouri, M. (2020). Identity and Access Management for IoT in Smart Grid. In- Computational Science and Its Applications – ICCSA 2020, LNCS vol.12254, Springer.

35. Kundur, P., et al. (2023). Cyber–physical security of smart grid infrastructures: Challenges and solutions. IEEE Transactions on Smart Grid, 14(1), 45–59.

36. Srivastava, A. K., & Zobaa, A. F. (2022). Review of risk assessment frameworks for power systems. Electric Power Systems Research, 203, 107678.

37. Patel, N., et al. (2024). Multi-criteria decision making in cyber-physical systems: A survey. Computers & Security, 120, 102854.

38. Murphy K. A brief introduction to graphical models and Bayesian networks / Technical report 2001-5-10, departament of computer science, University of British Columbia, Canada, May 2001. - 19 p.

39. Perederyi V., Borchik Eu., Ohnieva O. Information Technology for Decision Making Support and Monitoring in Man-Machine Systems for Managing Complex

Technical Objects of Critical Application, Advances in Intelligent Systems and Computing, 2021, Vol. 1246, pp. 448–466. DOI: 10.1007/978-3/

40. Perederyi V., Borchik Eu., Lytvynenko V., Ohnieva O. Information Technology for Performance Assessment of Complex Multilevel Systems in Managing Technogenic Objects.CEUR Workshop Proceedings, 2020, Vol. 2805, pp. 175-188.

41. Perederyi V., Borchik, Eu., Wójcik W., Ohnieva O. Assessment and Information Security Provision of the Decision Support Process in Technogenic Object Management Systems. CEUR Workshop Proceedings, 2021, Vol. 3101, pp. 322–334.

42. Evaluation of the influence of environmental factors and cognitive parameters on the decision-making process in human-machine systems of critical application / [V. I. Perederyi, E. Y. Borchik, V. V. Zosimov, O. S. Bulgakova,] // Radio Electronics, Computer Science, Control. - 2024. - № 1 – P. 77-84. DOI 10.15588/1607-3274-2024-1-7.