Міністерство освіти і науки України
Харківський національний університет імені В. Н. Каразіна
Навчально-науковий інститут «Українська інженерно-педагогічна академія»
Кафедра автоматизації, метрології та енергоефективних технологій

КВАЛІФІКАЦІЙНА РОБОТА

магістра

на тему

«Удосконалення підходів кваліметричної оцінки ризиків енергетичних підприємств із включенням складових кібербезпеки»_____
(тема кваліфікаційної роботи)

Виконав: студент 2 курсу, групи ДІВс24мг
спеціальності: 175 Інформаційно-вимірювальні технології
_____/_Олексій КІПОРЕНКО_____
(підпис) (ім'я та прізвище)
Керівник _____/_Ганна ГРІНЧЕНКО___
(підпис) (ім'я та прізвище)
Рецензент _____/_ __
(підпис) (ім'я та прізвище)

«До захисту допущено»

Завідувач кафедри _____/_Геннадій КАНЮК_
(підпис) (ім'я та прізвище)
Нормоконтроль_____/_____
(підпис) (ім'я та прізвище)
Секретар ЕК _____/__Євгеній КЛЮЧКА_
(підпис) (ім'я та прізвище)

Харків – 2025 рік

Міністерство освіти і науки України

Харківський національний університет імені В. Н. Каразіна
Навчально-науковий інститут «Українська інженерно-педагогічна академія»
Кафедра автоматизації, метрології та енергоефективних технологій

Спеціальність 175 Інформаційно-вимірювальні технології
Освітньо-професійна програма «Якість, стандартизація та сертифікація»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____
(підпис)

д.т.н., проф. Геннадій КАНЮК__
(науковий ступінь, вчене звання, ім'я, прізвище)

«___» _____2025 р.

ЗАВДАННЯ
на кваліфікаційну роботу
другого (магістерського) рівня вищої освіти

здобувача вищої освіти _____Олексій КІПОРЕНКО_____
(ім'я, прізвище)

1. Тема Удосконалення підходів кваліметричної оцінки ризиків енергетичних підприємств із включенням складових кібербезпеки
затверджена наказом по академії №____від «___»_____ 20___р.

2. Термін здачі закінченої роботи «____»_____20___р.

3. Вихідні дані до роботи/проєкту
_____
_____

4. Зміст роботи/проєкту (перелік питань, які належить розробити):
_ Вивчити нормативну та науково-технічну базу щодо управління ризиками та кібербезпеки в енергетичному секторі. Розробити методику кваліметричної оцінки ризиків, що включає кіберкомпонент як фактор підвищеного ризику. Запропонувати інтегральну модель аналізу ризиків, що враховує як технічні, так і кібернетичні загрози. Визначити шкалу оцінювання наслідків небажаних подій та їхнього впливу на безпеку та функціонування енергетичних систем. Розробити рекомендації щодо використання отриманих результатів.

5.Перелік графічного матеріалу (презентаційний матеріал):

_____

_____

_____

6. Консультант:

Розділ	Консультант	Підпис, дата		Оцінка (бали)
		Завдання видав	Завдання прийняв	

7. Дата видачі завдання«___»_____20___р.

Керівник _____ _Ганна ГРІНЧЕНКО__
(підпис) (ім'я, прізвище)

Завдання прийняв до виконання _____ Олексій КІПОРЕНКО
(підпис) (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН-ГРАФІК
виконання кваліфікаційної роботи

№ з/п	Назва етапів роботи та питань, які мають бути розроблені відповідно до завдання	Термін виконання	Позначки керівника про виконання завдань
1.	Розробка плану кваліфікаційної роботи, ознайомлення з літературними джерелами за темою		
2.	Написання теоретичної частини кваліфікаційної роботи		
3.	Написання аналітичної частини кваліфікаційної роботи		
4.	Написання дидактичного проєкту в рамках кваліфікаційної роботи		
5.	Перевірка чернетки кваліфікаційної роботи та внесення змін до неї керівником		
6.	Перевірка якості кваліфікаційної роботи у системі «Антиплагіат»		
7.	Оформлення кваліфікаційної роботи		
8.	Проходження нормоконтролю оформлення кваліфікаційної роботи		

Здобувач вищої освіти _____ Олексій КІПОРЕНКО
(підпис) (ім'я, прізвище)

Нормоконтроль

_____ _____
(підпис) (ім'я, прізвище)

ЗМІСТ

АНОТАЦІЯ

У дослідженні проаналізовано сучасні підходи до оцінювання ризиків у функціонуванні міських енергетичних систем з метою формування ефективної стратегії управління, основаної на нормативному підході. Виконано огляд існуючих методик і визначено нормативний підхід як ключовий інструмент управління ризиками, що передбачає кваліметричну оцінку впливу внутрішніх та зовнішніх чинників, визначених нормативно-правовими документами.

Виявлено основні складнощі процесу управління ризиками, зокрема потребу комплексного аналізу, який охоплює не лише окремі елементи системи, а й їхні взаємозв'язки та перебіг процесів, що впливають як на технічний стан обладнання, так і на екологічну безпеку. Запропоновано розглядати відхилення від нормальних умов експлуатації енергообладнання як ризикові події в межах кваліметричної оцінки технічних систем, із врахуванням потенціалу їхнього відновлення та модернізації.

Як модель управління ризиками функціонування технічних систем представлено підхід, що спирається на інтенсивність відмов та імовірність відновлення працездатності енергетичної інфраструктури. Для оцінювання ризиків сформовано шкалу, яка враховує рівень безпеки, ступінь наслідків небажаних подій, а також можливості відновлення технічних елементів системи та ліквідації екологічних наслідків (з урахуванням часу їхнього усунення).

Додатково проведено оцінку впливу зовнішніх чинників на роботу технічної системи та запропоновано використовувати матриці ризику для оцінювання рівня безпеки й ефективності функціонування. Такий підхід дає змогу оцінювати ефективність упровадження, організації та подальшої експлуатації системи, а головне — забезпечує можливість оперативного управління та вдосконалення її роботи на будь-якому етапі життєвого циклу.

Для проведення оцінювання та подальшого управління ризиками здійснено аналіз науково-технічних джерел і нормативної документації, на основі якого

сформовано алгоритм-схему з урахуванням кіберскладової. Кіберкомпонент розглядається як самостійна загроза для стабільного функціонування енергетичного підприємства, а також як чинник, що може підсилювати дію інших ризиків, спричиняючи зростання сукупного рівня небезпеки.

У ході проведеного дослідження було сформовано науково обґрунтований підхід до оцінювання рівня безпеки підприємства з урахуванням впливу сучасних кіберзагроз. Запропонована методика поєднує кваліметричні інструменти з удосконаленою системою вагових коефіцієнтів, що дало змогу розробити комплексну інтегральну модель аналізу ризиків. Така модель забезпечує глибоке та багатовимірне уявлення про стан захищеності підприємства, дозволяючи своєчасно ідентифікувати критичні вразливості як на етапі стратегічного планування, так і під час оперативного управління.

У межах роботи також здійснено детальний аналіз основних загроз для атомної електростанції, що дало можливість виявити приховані ризики та конкретизувати джерела їхнього походження. Зокрема, встановлено, що відмова систем охолодження може бути спричинена не лише технічними несправностями, а й навмисним втручанням у програмне забезпечення або маніпуляцією сигналами датчиків. Усі ці фактори були враховані при формуванні підходу до оцінювання ризиків, що підвищує точність і надійність отриманих результатів.

Для підвищення наочності й ефективності представлення результатів запропоновано використовувати 3D-матрицю ризиків із включенням кіберкомпонента. Такий формат візуалізації дає керівництву енергетичних підприємств можливість швидко визначати найбільш критичні зони ризику, у яких кіберфактор істотно підсилює загрозу безпеці. Застосування розробленої інтегральної моделі підтвердило, що реальний рівень ризиків на атомній електростанції значно зростає за рахунок кіберчинника.

Мета дослідження: Удосконалення підходів кваліметричної оцінки ризиків енергетичних підприємств із інтеграцією компонентів кібербезпеки для

підвищення ефективності управління ризиками та забезпечення комплексної безпеки технічних систем.

Задачі дослідження:

Проаналізувати сучасні підходи до оцінки ризиків функціонування енергетичних підприємств та визначити їхні обмеження у врахуванні кіберзагроз.

1. Вивчити нормативну та науково-технічну базу щодо управління ризиками та кібербезпеки в енергетичному секторі.
2. Розробити методику кваліметричної оцінки ризиків, що включає кіберкомпонент як фактор підвищеного ризику.
3. Запропонувати інтегральну модель аналізу ризиків, що враховує як технічні, так і кібернетичні загрози.
4. Визначити шкалу оцінювання наслідків небажаних подій та їхнього впливу на безпеку та функціонування енергетичних систем.
5. Провести апробацію запропонованої методики на прикладі атомної або іншої енергетичної установки з оцінкою ефективності інтегрованого підходу.
6. Розробити рекомендації щодо використання отриманих результатів для підвищення рівня безпеки та управління ризиками на енергетичних підприємствах.

ВСТУП

У сучасних умовах швидкого технологічного розвитку та підвищення вимог до безпеки підприємств оцінювання ризиків стає ключовим інструментом ефективного управління якістю та дотримання нормативних стандартів. Ризики можуть виникати на будь-якому етапі життєвого циклу — від проєктування та виробництва до експлуатації в позапроєктні періоди, виведення з експлуатації та поводження з відпрацьованими матеріалами. Вчасне виявлення та зниження ризиків дає можливість не лише запобігати загрозам для суспільства й довкілля, а й удосконалювати виробничі процеси, скорочувати витрати та підвищувати конкурентоспроможність підприємства.

Сучасні енергетичні підприємства працюють у комплексному, динамічному середовищі, яке постійно змінюється — як з боку вихідних параметрів, так і з боку вимог до процесів. Ефективність виробництва та рівень надійності енергопостачання визначаються не лише технічним станом обладнання, а й здатністю підприємства своєчасно ідентифікувати та мінімізувати ризики. Цифровізація енергетики — впровадження автоматизованих систем управління, smart grid, IoT та Big Data — значно посилює можливості моніторингу, прогнозування та забезпечення безпеки, але водночас формує нові загрози та потенційні вразливості.

У процесі переходу до «цифрової енергетики» традиційні методи оцінювання ризиків втрачають свою достатність через збільшення спектра можливих загроз — від кіберризиків і техногенних аварій до збоїв цифрових систем управління та помилок алгоритмічної обробки даних. Це обумовлює необхідність удосконалення методології управління ризиками з урахуванням інтеграції цифрових технологій, посилення кіберзахисту та підвищення стійкості енергетичної інфраструктури до комплексних впливів.

Ризики можуть виникати на будь-якому етапі життєвого циклу підприємства — від проєктування та виготовлення обладнання до його експлуатації у понадпроєктні строки, а також під час виведення з експлуатації й утилізації матеріалів та технічних засобів. Своєчасне виявлення та мінімізація таких ризиків дозволяють не лише запобігати потенційним негативним наслідкам для довкілля та суспільства, але й оптимізувати виробничі процеси, скорочувати витрати та підвищувати конкурентоспроможність підприємства.

Сучасні енергетичні підприємства функціонують у динамічному та багатофакторному середовищі, де ефективність виробничих процесів і надійність енергопостачання визначаються не лише технічною справністю обладнання, а й здатністю своєчасно ідентифікувати, оцінювати та контролювати потенційні ризики. Інтенсивне впровадження цифрових рішень — автоматизованих систем керування, технологій smart grid, Інтернету речей та аналітики на основі Big Data — відкриває нові можливості для оптимізації управління, підвищення рівня безпеки, більш точного моніторингу та прогнозування технічного стану обладнання. Водночас така цифровізація створює додаткові загрози, зокрема пов’язані з кібербезпекою та збільшенням уразливості цифрових інфраструктур.

У контексті трансформації галузі до формату «цифрової енергетики» традиційні методи оцінювання ризиків поступово втрачають свою ефективність, оскільки спектр потенційних небезпек стає значно ширшим і складнішим — від кібератак та техногенних аварій до збоїв в алгоритмічному управлінні. Це підсилює необхідність модернізації системи управління ризиками через інтеграцію сучасних цифрових інструментів, посилення кіберзахисту та формування більш стійкої інженерної та IT-інфраструктури, здатної протистояти комплексним і взаємопов’язаним загрозам.

Таким чином, важливість дослідження полягає у створенні сучасних підходів до оцінювання ризиків енергетичних підприємств, здатних ефективно адаптуватися до умов цифрової трансформації й забезпечувати надійність, безперервність та безпеку енергетичних процесів.

РОЗДІЛ 1. АНАЛІЗ ПІДХОДІВ ОЦІНЮВАННЯ РИЗИКІВ ЕНЕРГООБ'ЄКТІВ

1.1.Науково-обгрунтовані підходи до управління ризиками енергетичних об'єктів

Управління ризиками та їх оцінювання можуть здійснюватися за допомогою різних підходів, що застосовуються як у соціальних, так і в інженерних системах. Серед таких підходів виділяють кількісний аналіз, який ґрунтується на статистичних даних і прогнозуванні ймовірності виникнення загроз, а також якісний аналіз, що використовує експертні судження та описові характеристики. Значну роль відіграє сценарний метод, який дозволяє моделювати різні варіанти розвитку подій. Крім того, поширеною є оцінка ризиків відповідно до вимог нормативних стандартів, таких як ISO 31000 чи ISO 9001 [1]. Сучасні цифрові технології істотно посилюють ефективність процесів управління ризиками шляхом автоматизації збору даних, їх обробки та підтримки прийняття рішень, що також регламентується такими стандартами, як ДСТУ EN IEC 62351, ISA/IEC 62443, ISO/IEC 27001/27019. Кожен із підходів має власні сильні сторони та обмеження, тому в практиці управління ризиками їх часто поєднують для отримання більш повної та точної оцінки.

Серед сучасних кількісних підходів до оцінювання ризиків в інженерних та технологічних системах провідну роль відіграють математико-статистичні методи, здатні відображати стохастичну природу технічних відмов і складність взаємодії численних факторів. Одним із найбільш поширених інструментів є метод Монте-Карло [2–6], який дає можливість моделювати широкий спектр випадкових сценаріїв, враховувати невизначеності параметрів, визначати ймовірність критичних подій і досліджувати поведінку системи за різних умов експлуатації. Завдяки своїй універсальності цей метод використовується для прогнозування надійності енергетичного обладнання, оцінки стійкості промислових об'єктів, оптимізації режимів роботи критичних інфраструктур.

Не менш затребуваним є метод аналізу дерева відмов (Fault Tree Analysis, FTA) [7–11], який дозволяє структурувати складні технічні ризики через побудову логічних моделей причинно-наслідкових зв'язків. Методика передбачає формування ієрархічної схеми, де базові події — первинні причини — логічно пов'язуються між собою та ведуть до виникнення верхньої події, що характеризує відмову системи. Завдяки таким побудовам інженери можуть ідентифікувати найкритичніші елементи системи, оцінювати їхній вплив на загальний рівень ризику та розробляти ефективні стратегії мінімізації небезпек.

Наприклад, у роботі [8] FTA застосовано для аналізу потенційно небезпечних сценаріїв у міському транспортному комплексі із подальшим формуванням детальної структури подій. З метою підвищення точності оцінювання автори перетворили отриману логічну модель на байєсівську мережу, що дало змогу не лише посилити кількісний аналіз ризиків, а й забезпечити можливість оновлення оцінок у реальному часі за надходження нових даних. Такий підхід демонструє, як класичні методи ризик-аналізу можуть бути розширені за рахунок інтелектуальних моделей, що є особливо актуальним для сучасних інженерних систем із високим рівнем цифровізації.

Сценарний підхід удосконалюють за рахунок формування та опрацювання дерев відмов з урахуванням динамічних характеристик систем, зокрема часових змін та структурної надмірності [10, 11]. Автоматизовані методи побудови дерев відмов дають змогу оперативно визначати найбільш критичні елементи системи та порівнювати різні варіанти її проєктування чи модернізації [11, 12]. Застосування цього методу забезпечує глибоку оцінку сукупного ризику та може бути використане як інструмент аналізу надійності, стійкості й довгострокових перспектив розвитку технічних об'єктів.

Поєднання якісного та кількісного аналізу дозволяє отримати більш повне уявлення про стан інженерних систем. До якісних методів належать SWOT-аналіз, що дає змогу оцінити сильні й слабкі сторони системи, а також зовнішні можливості та загрози, і побудова матриць імовірності ризиків на основі експертних оцінок [13–19]. Хоча SWOT-аналіз традиційно застосовується у

сфері бізнесу та управління проєктами, у технічних системах він орієнтований передусім на питання безпеки та використовує кваліметричні методи [13, 17–19].

Нормативний підхід до оцінювання ризиків передбачає опору на міжнародні стандарти ISO 31000 [20], IEC 31010 [21], ISO 9001 [22], ISO 45001 [23], які формують уніфіковану методологічну базу для впровадження систем управління ризиками, інтеграції заходів безпеки та підвищення ефективності управлінських процесів. Оцінювання ризиків згідно з цими стандартами охоплює визначення критеріїв небезпеки та ризиків, аналіз потенційно критичних точок і розроблення превентивних дій щодо їх усунення або мінімізації [24–27].

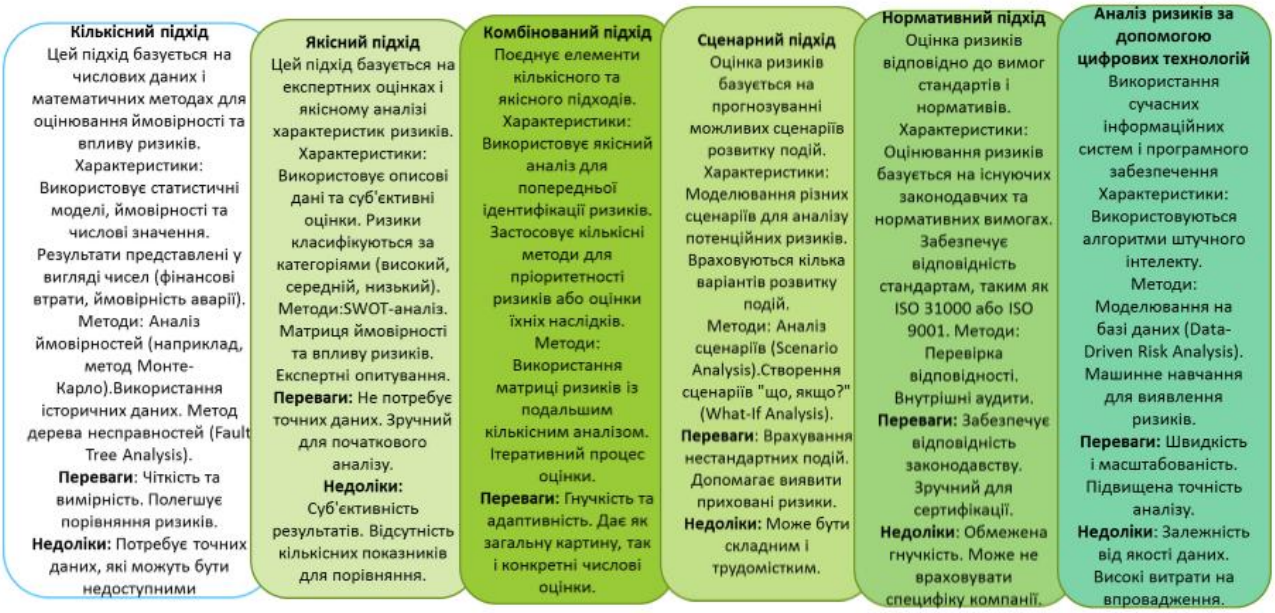


Рисунок 1.1. – Оцінювання ризиків

Кожна з представлених груп методів має свої сильні сторони та певні обмеження (Рис. 1), тому на практиці їх зазвичай поєднують для підвищення точності оцінювання та забезпечення ефективного управління ризиками. Оптимальний вибір методології повинен відповідати особливостям конкретного об’єкта, для якого здійснюється ризик-менеджмент, та специфіці його функціонування.

1.2 Аналіз підходів до оцінювання ризиків з урахуванням кіберкомпоненти

Очікуване у найближчі десятиріччя збільшення внутрішнього споживання електроенергії та зростання експортного потенціалу, обмежені ресурси органічного палива для теплових електростанцій, екологічні ризики, притаманні тепловій енергетиці, а також відсутність значних вільних гідроенергетичних потужностей та невизначені перспективи широкого впровадження нетрадиційних джерел енергії визначають атомну енергетику як стратегічно важливий і високо конкурентний напрям розвитку України.

Попри це, галузь атомної енергетики залишається об’єктом численних дискусій і суперечностей, пов’язаних із потенційними загрозами для суспільної безпеки, ризиками забруднення довкілля та складністю забезпечення технологічної надійності. Такі чинники вимагають системного аналізу та застосування науково обґрунтованих методів оцінювання ризиків і виявлення можливих загроз.

Комплексний підхід до аналізу ризиків енергетичних об’єктів дає змогу прогнозувати потенційні загрози на всіх етапах життєвого циклу атомної станції — від планування та проєктної експлуатації до роботи в умовах продовжених строків служби та з урахуванням зношування обладнання. Оцінка здатності енергетичного об’єкта як складної технічної системи адаптуватися до зовнішніх і внутрішніх викликів є ключовою складовою ефективного ризик-менеджменту. Це дозволяє підвищити точність та економічну обґрунтованість оцінок, а також сприяє формуванню стратегії управління ризиками, орієнтованої на підвищення стійкості урбанізованих енергетичних систем.

Кваліметричний підхід виступає одним із науково виважених методів кількісної оцінки складних систем та процесів. Він ґрунтується на побудові інтегральних індикаторів якості, нормуванні показників та їх зважуванні. Цей метод активно застосовується в машинобудуванні, енергетиці, харчовій промисловості, фінансах і соціальних сферах [1–5].

У сфері управління ризиками кваліметрія забезпечує можливість переведення експертних суджень у числову форму, що полегшує порівняння, ранжування та вибір оптимальних управлінських рішень [6, 7]. Традиційні кваліметричні моделі передбачають багаторівневе зважування критеріїв, нормування показників до єдиної шкали та подальше агрегування результатів. Для аналізу ризиків застосовують матриці оцінювання, ранжування та критеріальне оцінювання [8–10]. Новітні дослідження пропонують використовувати статистичні моделі розподілу оцінок, що дозволяє визначати ймовірнісні межі ризиків [11, 12].

В енергетичній галузі поєднання кількісних методів (QRA, Monte-Carlo) з напівкількісними та кваліметричними підходами забезпечує швидке й інформативне оцінювання широкого спектра ризиків — від технічних і організаційних до екологічних і кіберризиків. Практичні рекомендації вказують на важливість інтеграції експертних і статистичних підходів для підвищення достовірності та практичної корисності результатів, особливо в умовах обмеженості статистичних даних, що ускладнює прогнозування ризиків [13–16].

Сучасні наукові напрацювання [17–19] свідчать, що ефективна методика оцінювання ризиків для енергетичних підприємств має базуватися на багаторівневому підході. До нього зазвичай належать такі етапи:
(1) інвентаризація технологічних об’єктів і систем;
(2) виявлення загроз та потенційних вразливостей;
(3) присвоєння експертних значень показників якості або уразливості;
(4) нормалізація отриманих даних та їх агрегування в інтегральний показник ризику.

Дослідження в енергетиці, а також у нафтогазовому та відновлюваному секторах [20–22], підтверджують активну тенденцію до комбінування кваліметричних підходів із методами аналізу часових змін ризику та сценарного моделювання. Іншим перспективним напрямом є інтеграція кваліметрії з алгоритмами машинного навчання та технологіями обробки великих даних. Такий підхід дає змогу автоматизувати процес збору експертних оцінок,

об’єктивізувати вагові коефіцієнти на основі архівів відмов та інцидентів, формувати ймовірнісні розподіли ризиків та оперативно оновлювати інтегральні показники у разі зміни стану енергосистем.

Зростає також увага до включення кіберпараметрів у кваліметричні моделі — таких як рівень уразливості інформаційно-керувальних комплексів, швидкість виявлення інцидентів чи здатність до відновлення після кібератак. Це пояснюється тим, що кіберінциденти істотно впливають на доступність, цілісність і конфіденційність енергетичних сервісів [5, 13].

Кваліметричні методи мають низку суттєвих переваг: вони працюють із багатопараметричними системами, забезпечують швидке ранжування ризиків, є прозорими для ухвалення рішень та легко адаптуються до впровадження нових показників у процесі модернізації енергетичних об’єктів [23, 24]. Водночас їх застосування пов’язане з певними обмеженнями, серед яких — висока залежність від кваліфікації експертів, можливість появи суб’єктивних упереджень, недостатня статистична перевірка результатів за обмежених даних та потреба поєднувати кваліметрію з кількісними інженерними моделями для оцінки масштабних технічних ризиків.

Огляд сучасних досліджень [25–28] свідчить про низку актуальних викликів для українського енергетичного сектору. Серед них — відсутність єдиної системи стандартизованих кіберіндикаторів, необхідність удосконалення методів визначення експертних ваг (зокрема із застосуванням машинного навчання), потреба в інтеграції кваліметричної оцінки з моніторингом у реальному часі та сценарним аналізом стійкості, а також удосконалення методів валідації моделей на основі історичних кейсів і симуляційних даних.

Методологічною основою для комплексної оцінки ризиків у енергетиці слугують міжнародні стандарти ISO 31000 «Risk Management – Guidelines» [29] та ISO/IEC 27001 «Information Security Management Systems» [30], які поєднують системний підхід до ризик-менеджменту та управління інформаційною безпекою. Крім того, рекомендації NIST SP 800-82 [31–34] надають детальні вимоги щодо захисту промислових систем управління (SCADA, DCS), що є критично

важливим елементом інтеграції кіберризиків у комплексну кваліметричну модель оцінювання ризиків енергетичних підприємств.

Кваліметричні підходи залишаються одним із найбільш дієвих інструментів для системного та оперативного оцінювання ризиків в енергетичній сфері, особливо в умовах стрімкої цифровізації та зростання кількості різнорідних загроз. Вони дозволяють структурувати комплексний ризиковий простір, швидко ранжувати загрози за пріоритетністю та враховувати не лише техніко-технологічні, а й якісні чинники — зокрема, рівень кіберзахищеності, організаційні особливості, людський фактор. Водночас, класичні методи кваліметрії мають певні обмеження, пов'язані з суб'єктивністю експертних оцінок і недостатньою гнучкістю щодо динамічних змін у стані системи.

Щоб підвищити точність, стійкість та адаптивність оцінювання, доцільно поєднувати кваліметричні методи з кількісними підходами та сучасними цифровими технологіями — такими як аналіз великих масивів даних, машинне навчання й інтелектуальні системи підтримки рішень. Така інтеграція дозволяє істотно зменшити вплив суб'єктивних факторів, автоматично оновлювати вагові коефіцієнти, враховувати нові дані про вразливості та формувати прогнозні моделі поведінки енергетичних об'єктів у різних сценаріях.

Особливої актуальності набуває застосування методичних рекомендацій NIST у поєднанні з міжнародними стандартами ISO 31000 (ризик-менеджмент) та ISO/IEC 27001 (інформаційна безпека). Разом вони формують цілісну рамкову систему для побудови інтегрованого управління ризиками, де поєднуються кількісні та якісні методи аналізу, враховуються технічні, організаційні та кібернетичні компоненти безпеки. Такий підхід створює надійну методологічну основу для вдосконалення кваліметричних моделей, забезпечує узгодженість між різними рівнями управління та сприяє підвищенню загального рівня безпечності й стійкості енергетичних підприємств (табл. 1).

Таблиця 1 - **Порівняння міжнародних нормативних документів з управління ризиками та кібербезпеки в енергетиці**

Нормативний документ	Основна сфера застосування	Ключові положення	Релевантність для енергопідприємств
ISO 31000 "Risk Management – Guidelines"	Управління ризиками (усі сфери діяльності)	- Принципи, структура та процес управління ризиками - Інтеграція в систему корпоративного управління - Баланс якісних та кількісних методів	Забезпечує методологічну основу для оцінювання ризиків технічних процесів, управління інфраструктурою та прийняття рішень у сфері енергетики
ISO/IEC 27001 "Information Security Management Systems"	Управління інформаційною безпекою	- Побудова системи управління інформаційною безпекою (СУІБ) - Ідентифікація, аналіз та мінімізація кіберризиків - Контроль доступу, моніторинг та інцидент-	Дозволяє захистити дані, мережеву інфраструктуру та SCADA-системи енергопідприємств від кіберзагроз

		менеджмент	
NIST SP 800-82 "Guide to ICS Security"	Кібербезпека промислових систем управління (ICS, SCADA, DCS)	- Практичні заходи кіберзахисту - Моделі загроз для ICS - Інструменти моніторингу та реагування	Орієнтований на специфіку промислових систем, критично важливих для енергетики; дає практичні рекомендації з технічного захисту
NIST «Roadmap for Improving Critical Infrastructure Cybersecurity»	Розвиток кібербезпеки для критичної інфраструктури	- Автентифікація та аналіз даних - Автоматизований обмін індикаторами загроз - Оцінка відповідності - Підготовка кадрів - Управління ланцюгами постачання - Розробка стандартів у сфері конфіденційності	Орієнтований на забезпечення кіберзахисту в промислових та енергетичних системах

У межах Європейського Союзу питання кібербезпеки та захисту критично важливої інфраструктури розглядаються як один із ключових пріоритетів стратегічного розвитку. На рівні Європейської комісії (ЄК) постійно формуються нормативні та програмні документи, спрямовані на підвищення стійкості держав-членів до сучасних кібер- та фізичних загроз. Однією з таких ініціатив стала комплексна програма зміцнення безпеки критичної інфраструктури (CIP), у якій систематизовано принципи управління ризиками та

визначено механізми взаємодії між країнами ЄС. Документ містить рекомендації щодо ідентифікації критично важливих об’єктів, запровадження узгоджених підходів до оцінювання загроз, використання інструментів моніторингу та розроблення превентивних заходів для мінімізації потенційних наслідків.

Подальший розвиток безпекових підходів отримав відображення у представленій ЄК у 2015 році концепції «Енергетичного союзу». Її головна мета — зміцнення енергетичної незалежності ЄС, модернізація інфраструктури, розширення застосування відновлюваних джерел енергії та створення більш інтегрованого внутрішнього енергетичного ринку. Значну увагу в концепції приділено цифровій трансформації енергетичного сектору, оскільки цифровізація створює не лише нові можливості керування енергосистемами, а й нові кіберзагрози. У цьому контексті підсилення кіберзахисту стає одним із визначальних елементів енергетичної безпеки ЄС.

Аналіз відповідних європейських та міжнародних документів свідчить про послідовність і взаємопов’язаність глобальних підходів до управління ризиками. Стандарти ISO формують загальні методологічні засади, спрямовані на побудову системного ризик-менеджменту, тоді як рекомендації NIST деталізують технічні та організаційні інструменти забезпечення кібербезпеки. Європейська комісія, у свою чергу, зосереджується на гармонізації цих підходів у межах ЄС, створюючи умови для інтегрованої політики безпеки.

Незмінною залишається спільна тенденція: розвиток системного управління ризиками, підвищення кіберстійкості та поглиблення міжнародної співпраці. Усе це формує комплексну рамку, необхідну для забезпечення стабільності енергетичних систем, захисту інфраструктурних об’єктів та зміцнення загальної безпеки у цифровизованому середовищі.

РОЗДІЛ 2. РОЗВИТОК НОРМАТИВНОГО ПІДХОДУ ДО ОЦІНЮВАННЯ РИЗИКІВ НА ОСНОВІ КВАЛІМЕТРИЧНИХ МЕТОДІВ

2.1. Наукова методологія управління ризиками енергообладнання

Аналіз потенційних наслідків реалізації загроз та їхнього впливу на безперебійне забезпечення населення, бізнесу, державних інституцій і суспільства енергоресурсами є визначальним чинником формування енергетичної безпеки. Не менш важливо оцінювати здатність учасників енергетичної системи оперативно реагувати на ризики, локалізувати їх та запобігати розвитку критичних ситуацій. Такий підхід дає змогу не лише зменшити імовірність збоїв у постачанні енергоресурсів, але й забезпечити довгострокову стійкість паливно-енергетичного комплексу, що є основою стабільної роботи економіки та соціальної інфраструктури.

Комплексне управління ризиками сьогодні розглядається як універсальний інструмент, що передбачає систематичне планування, розроблення та впровадження заходів безпеки, інтегрованих у державну політику та галузеве управління. Його головною метою є запобігання появі нових загроз і мінімізація вже наявних шляхом застосування узгоджених превентивних дій на рівні окремих об’єктів, секторів економіки та держави загалом. Практика країн Європейського Союзу підтверджує результативність таких підходів: у 2017 році були впроваджені спеціалізовані методики оцінки ризиків для критичної інфраструктури [29], засновані на всебічному аналізі загроз, можливих сценаріїв їх розвитку та масштабів потенційних наслідків.

Ризик є природною та невід’ємною характеристикою будь-якої соціально-економічної діяльності, оскільки виникає всюди, де присутня невизначеність, обмеженість ресурсів та багатоваріантність управлінських рішень. Він не може трактуватися виключно як негативне явище чи як перевага — ризик відображає баланс між потенційними втратами та можливостями, що відкриваються перед системою внаслідок прийняття рішень. Відповідно, мета управління ризиками не

полягає у повному їх усуненні (що на практиці неможливо), а у своєчасному виявленні, кількісному та якісному аналізі й забезпеченні належного контролю, що дозволяє мінімізувати можливі збитки та водночас використати наявні можливості для розвитку. Сучасна парадигма ризик-менеджменту ґрунтується на концепції «прийнятного ризику», відповідно до якої рівень сукупного ризику повинен підтримуватися в межах, допустимих стратегічними цілями розвитку соціально-економічної системи та її здатністю до відновлення [1].

Процес оцінювання ризиків включає низку ключових взаємопов'язаних етапів: ідентифікацію потенційних загроз; аналіз частоти або ймовірності їхнього виникнення; оцінювання вразливості системи до кожного виду загроз; визначення інтегрального рівня ризику як функції від ймовірності та очікуваних наслідків; а також аналіз можливих сценаріїв розвитку ситуації, включаючи найгірший варіант. Такий підхід дозволяє сформувати цілісне бачення ризикового профілю об'єкта та визначити пріоритетні напрями реагування. Концепція ризик-менеджменту виходить за рамки традиційної оцінки загроз: вона охоплює формування системи превентивних, компенсуючих та адаптивних заходів, інтегрованих у практичну діяльність підприємства чи галузі, а також забезпечує підтримку прийняття рішень з урахуванням потенційних соціальних, економічних та технологічних наслідків [20–23].

Для формування ефективної моделі управління ризиками енергетичного підприємства, що функціонує в умовах складної соціально-екологічної та техногенно-інформаційної взаємодії, необхідно чітко визначити послідовність етапів виявлення, оцінювання та контролю ризиків. Ці етапи мають ґрунтуватися на міжнародно визнаних нормативних підходах, зокрема рекомендаціях ISO 31000, ISO/IEC 27005, NIST та інших регуляторних документах, що формують системний, інтегрований та адаптивний підхід до управління ризиками. Інтеграція таких стандартів дає змогу побудувати гнучку модель ризик-менеджменту, орієнтовану на підтримання безперервності функціонування енергетичного підприємства, з урахуванням технічних, інформаційних, екологічних та організаційних факторів (рис. 2).

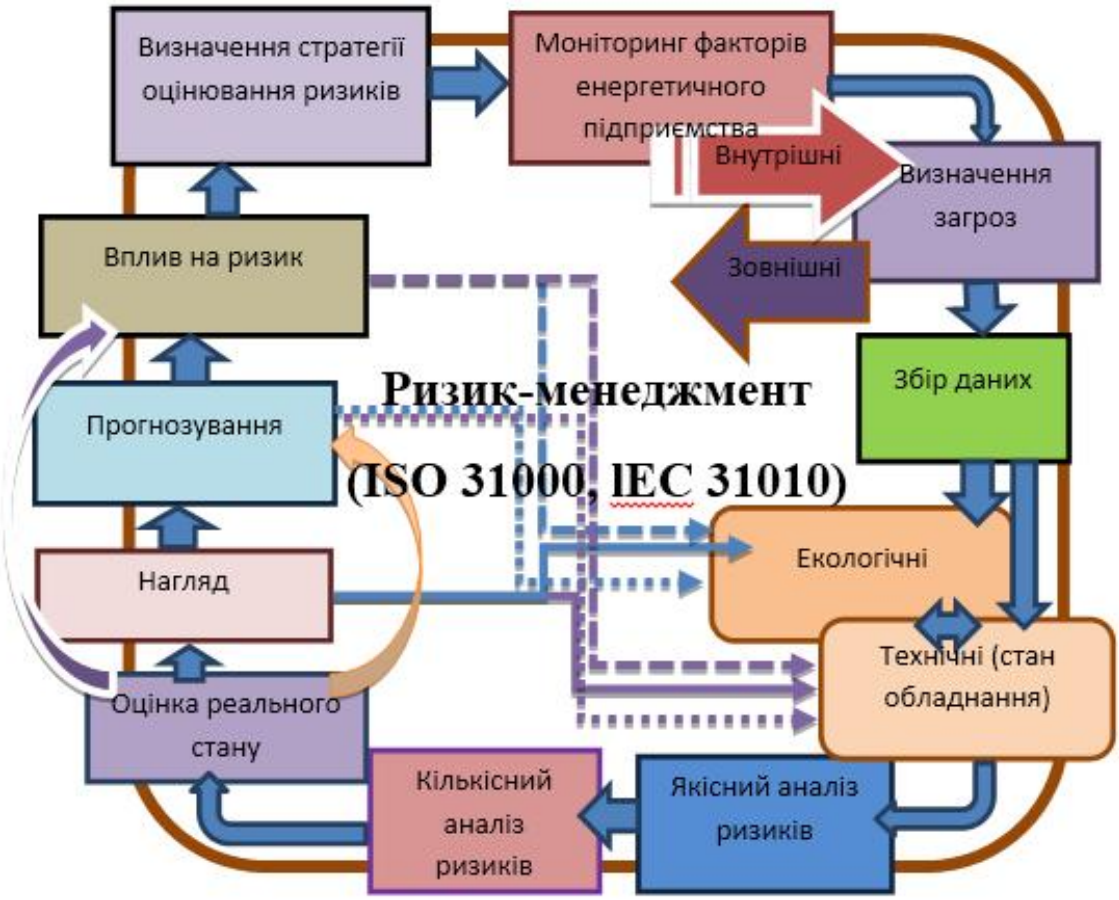


Рис.2 Модель оцінки і управління ризиками

Управління ризиками може та повинно впроваджуватися на всіх етапах життєвого циклу енергетичної системи — від стратегічного планування та проєктування до експлуатації, модернізації та виведення з експлуатації окремих об’єктів. Його результативність значною мірою залежить від рівня залучення всіх структурних підрозділів та управлінських рівнів підприємства. Вирішальна роль у цьому процесі належить керівництву вищої ланки, яке формує загальну стратегію ризик-менеджменту, визначає пріоритети безпеки, затверджує допустимі межі сукупного ризику та забезпечує ресурсне підґрунтя для реалізації відповідних заходів. Такий підхід сприяє створенню єдиної корпоративної культури управління ризиками, що підтримує проактивну поведінку персоналу і забезпечує цілісність процесу на всіх рівнях.

Система управління ризиками характеризується комплексністю та масштабністю, оскільки передбачає участь усіх підрозділів підприємства —

виробничих, технічних, адміністративних, метрологічних, інформаційно-аналітичних, а також підрозділів, що відповідають за кібербезпеку та екологічний контроль. Така інтеграція забезпечує багатовимірний аналіз потенційних загроз, дозволяє враховувати технічні, організаційні, інформаційні, екологічні та соціальні фактори та формувати збалансовану систему реагування на ризики.

Першим етапом формування дієвої системи управління ризиками є розроблення стратегії розвитку енергетичного підприємства, яка має бути тісно пов’язана з Політикою якості системи управління процесами. Політика якості визначає стратегічні напрями діяльності, встановлює чіткі, вимірювані та досяжні цілі, регламентує порядок їх впровадження та розподіл відповідальності між учасниками процесу. Цілі мають передбачати як кваліметричну, так і кількісну оцінку результативності, що забезпечує прозорість, контрольованість та можливість оперативного коригування діяльності.

Політика якості повинна мати офіційний статус, бути доступною, зрозумілою та прийнятою на всіх рівнях управління. Вона повинна відображати не лише стратегічні пріоритети підприємства, а й принципи сталого розвитку, підвищення енергоефективності, надійності технологічних процесів та безпечності об’єктів енергетичної інфраструктури. Важливо посилювати інформованість персоналу щодо їхньої ролі в реалізації цих цілей, забезпечувати належну підготовку та підтримувати компетентність працівників.

Кожен співробітник має усвідомлювати, що його повсякденні дії прямо впливають на рівень технічної безпеки, якість надання послуг, енергетичну стійкість підприємства та загальну ефективність виробничих процесів. Формування відповідального ставлення, залучення до процесів постійного вдосконалення, розвиток культури прогнозування та попередження ризиків створює передумови для зростання інноваційного потенціалу підприємства й забезпечення його конкурентоспроможності у довгостроковій перспективі.

Наступним етапом моделі ризик-менеджменту є інформаційно-аналітичний процес, що ґрунтується на безперервному моніторингу факторів,

здатних спричинити ризики. При цьому враховуються як внутрішні чинники підприємства — технічний стан обладнання, зміни у його роботі, організація технічних процесів, дії персоналу (мотивація, рівень кваліфікації, усвідомлення відповідальності), резервування систем, періодичність контролю та організація соціально-технічних систем безпеки, — так і зовнішні фактори, зокрема екологічні загрози (землетруси, повені, стихійні лиха), кіберзагрози, терористичні акти та військові конфлікти.

На цьому етапі здійснюється збір, обробка, передача та аналіз інформації, що дозволяє оцінити спектр ризиків, які можуть виникнути на підприємстві. Якість і повнота зібраних даних визначають точність наступного етапу — встановлення контексту ризику. Чим детальніше проаналізована інформація, тим точніше можливо ідентифікувати потенційні загрози та оцінити ризики, пов’язані з їх реалізацією.

Визначення ризиків базується на ідентифікації подій, що можуть впливати на досягнення стратегічних цілей підприємства, як позитивно, так і негативно. У системі управління якістю ключовою метою є забезпечення стабільного, безпечного та передбачуваного функціонування енергетичного підприємства в умовах змінного техногенного та природного середовища. Контекст ризику охоплює широкий спектр чинників, що впливають на надійність і безпеку об’єкта, зокрема відхилення від нормальних режимів роботи, виникнення аварійних або потенційно небезпечних ситуацій, перевищення проєктних параметрів, а також зовнішні впливи природного чи техногенного характеру. Важливо враховувати не лише технічні ризики, але й екологічні — наслідки надмірного антропогенного навантаження на довкілля, яке здатне спричинити довготривалі зміни в екосистемах, зменшити їхню стійкість і тим самим підвищити вразливість енергетичної інфраструктури. Ефективне управління ризиками передбачає системний облік цих взаємозалежностей для забезпечення гармонійного функціонування підприємства у межах соціо-екологічної системи.

Наступний етап полягає у зборі релевантних даних відповідно до визначеного контексту ризику. Цей процес здійснюється спеціалістами профільних підрозділів під час їхньої поточної діяльності, виконання регламентних операцій, технічних оглядів, діагностики обладнання або лабораторних досліджень — наприклад, моніторингу стану атмосферного повітря, ґрунтів, водних ресурсів. Для енергетичного підприємства важливо враховувати не лише традиційні статистичні показники надійності та відмов обладнання, але й дані в реальному часі про їх технічний стан, поведінку систем в умовах пікових навантажень, нестандартних режимів роботи чи зовнішніх впливів. Крім того, значущими є сценарії розвитку потенційних загроз, розроблені з урахуванням досвіду аналогічних підприємств або міжнародної практики, що дозволяє більш повно оцінювати можливі небажані події.

Для визначення потенційного впливу на довкілля необхідно зібрати комплексну інформацію про антропогенне навантаження на територію підприємства: показники радіаційної безпеки, теплового забруднення, обсягів і складу викидів у повітря, воду чи ґрунт, рівень шумового впливу, утворення промислових відходів тощо. Важливо враховувати взаємодію природних факторів (наприклад, зміни кліматичних умов, геологічні чи гідрологічні ризики) з технічним станом обладнання, оскільки такі взаємовпливи можуть істотно підвищувати імовірність аварій або поглиблювати їх екологічні наслідки.

Також необхідно оцінити, яким чином технічні несправності — відхилення в роботі, аварії, пошкодження, прогресуюче зношення обладнання — здатні посилювати негативний вплив на природні системи. Комплексний облік цих факторів сприяє більш точному визначенню рівня ризику та формуванню ефективних заходів його мінімізації. Доцільним є застосування методів аналізу зворотного зв’язку, які враховують, як зміни в екосистемах можуть впливати на функціональну готовність енергетичного об’єкта, зокрема на його запас міцності, надійність систем резервування, стійкість до зовнішніх загроз і здатність швидко відновлювати працездатність після інцидентів. Такий підхід підсилює

адаптивність системи управління ризиками та забезпечує стійкість енергетичної інфраструктури в умовах сучасних викликів.

Наступним етапом управління ризиками є проведення якісного аналізу, який спрямований на системну ідентифікацію факторів, здатних спричинити ризики, а також на оцінку потенційних наслідків їх реалізації для безперервного функціонування підприємства та досягнення стратегічних цілей. На цьому кроці особлива увага приділяється всебічному вивченню обставин, які можуть впливати на ризики, і використанню сучасних інструментів якісного аналізу з урахуванням специфіки технологічних процесів, організаційної структури та характеру діяльності підприємства.

Для забезпечення більш точного та обґрунтованого кількісного аналізу ризиків слід враховувати не лише ймовірність настання небажаної події, а й потенційні наслідки її реалізації, включно з можливим рівнем економічних, технічних та екологічних втрат. Інтеграція якісних та кількісних оцінок дозволяє створити більш повну картину ризиків, підвищити обґрунтованість прийняття рішень і своєчасно визначати пріоритетні напрями для заходів з мінімізації негативного впливу на діяльність підприємства.

Рекомендується класифікувати загрози за трьома категоріями:

1. **Невідворотні загрози** — події, що призводять до незворотних пошкоджень технічних або екологічних компонентів системи, наприклад, руйнування екосистеми або обладнання, яке неможливо відновити.
2. **Частково відновлювані загрози** — ситуації, що порушують нормальні умови роботи систем, але допускають відновлення без критичних втрат. Це можуть бути перевищення нормативів забруднення або порушення режимів експлуатації обладнання, що впливає на ефективність, але не призводить до повного руйнування системи.
3. **Повністю відновлювані загрози** — події, що тимчасово порушують нормальну роботу системи, проте після усунення інциденту вона повертається до номінального стану. Прикладом можуть бути

перевищення екологічних показників або тимчасові збої обладнання, які легко ліквідуються завдяки резервним ресурсам і модернізації.

Для кожної категорії загроз визначаються їх властивості, якісні та кількісні характеристики, а також потенційні негативні впливи на безпеку та функціонування підприємства. Це дозволяє встановити граничні значення небезпечних факторів і створити систематизований перелік відомих та потенційних загроз із класифікацією за впливом на різні аспекти діяльності підприємства. Така структура сприяє пріоритизації управління ризиками, розробці заходів щодо мінімізації наслідків і підвищенню стійкості підприємства до непередбачуваних подій.

Для кожної загрози проводиться оцінка можливих наслідків, аналіз причин і механізмів виникнення, а також розробляються заходи для запобігання чи зменшення ризику. Усі результати фіксуються в протоколі. На основі зібраної інформації обчислюється індекс ризику, який визначається як функція двох параметрів: ступеня тяжкості наслідків (Т) та ймовірності їх настання (Р), враховуючи ймовірність відмови системи та її здатність до відновлення.

Ймовірність настання збитку оцінюється за п’ятибальною шкалою, розробленою експертами для кожної визначеної небезпеки. Рівні ймовірності характеризують шанси виникнення збитків з урахуванням факторів небезпеки, причин їх появи, механізмів та наявних заходів щодо зменшення ризику. Хоча ранжування ймовірності носить умовний характер, його точність підвищується зі зростанням практичного досвіду та накопиченням статистичних даних.

Для визначення ймовірності застосовуються різні підходи: аналіз історичних даних, прогнозування за допомогою аналітичних та симуляційних моделей, а також експертні оцінки. Якщо ймовірність можливо визначити кількісно, її порівнюють із п’ятибальною шкалою методики шляхом встановлення діапазонів значень для кожного рівня. Процес оцінювання здійснюється за участю експертів із відповідним досвідом у галузі енергетики та включає статистичну перевірку даних і точні розрахунки ймовірностей.

Ступінь тяжкості можливих наслідків (Т) оцінюється також за п’ятибальною шкалою, що поділяє наслідки на п’ять категорій. Рівні тяжкості визначаються та детально описуються експертами до початку оцінювання потенційних збитків і фіксуються у таблиці Плану управління ризиками. Кожен рівень дозволяє чітко віднести можливий збиток до відповідної категорії на основі його характеристик. При наявності кількох сценаріїв наслідків ступінь тяжкості визначається за найсерйознішим варіантом.

Аналіз тяжкості та ймовірності збитку організовується так, щоб полегшити ухвалення рішень щодо зниження ризику шляхом мінімізації ймовірності або масштабу наслідків (табл. 2.1). На основі п’ятибальної оцінки ймовірності та тяжкості збитків формується матриця ризику, яка відображає діапазони ризику для кожного рівня і включається до Плану управління ризиками енергетичного підприємства (табл. 2.2).

Таблиця 2.1 – **Шкала ймовірності настання небажаної події (загроз) на енергетичному підприємстві**

Оцінка	**Ймовірність**	**Діапазон ймовірності**	**Визначення**
Р1	Малоймовірна	$<1x10^{-9}$	Високий рівень забезпечення безпеки технічної складової, малоймовірні загрози
Р2	Дуже низька	$1x10^{-9}$–$1x10^{-8}$	Достаній рівень забезпечення безпеки, низька ймовірність загроз
Р3	Середня	$1x10^{-8}$–$1x10^{-7}$	Ймовірні поодинокі події (загрози), недостаній рівень забезпечення безпеки
Р4	Висока	$1x10^{-7}$–$1x10^{-4}$	Небезпека висока, повторюваність загроз високо ймовірна
Р5	Надзвичайно висока	$>/=1x10^{-4}$	Високий рівень небезпеки та ймовірність настання подій (загроз)

Слід зауважити, що представлена матриця ризиків не є традиційною моделлю та була спеціально адаптована з урахуванням підвищених вимог до енергетичних підприємств, які належать до категорії об’єктів підвищеної небезпеки. Вона враховує специфіку технологічних процесів, потенційні аварійні ситуації та наслідки, що можуть виникнути при порушенні нормальної роботи систем.

На основі оцінки кожного ризику приймається одне з двох рішень:

- У разі, якщо ризик кваліфікується як незначний — тобто його індекс потрапляє в діапазон прийнятних значень — він може не враховуватися у пріоритетних заходах управління. У такому випадку розробка спеціальних заходів щодо його зниження не є обов’язковою, проте рекомендується вести періодичний моніторинг для контролю можливих змін у його характеристиках.

Такий підхід дозволяє оптимізувати ресурси підприємства, зосереджуючи увагу на критично важливих ризиках, одночасно забезпечуючи системний контроль та оперативну готовність до потенційних загроз. Крім того, адаптована матриця може слугувати основою для інтеграції кількісних та якісних методів оцінки ризиків, що підвищує точність прогнозування та ефективність заходів з мінімізації негативного впливу на діяльність підприємства.

Якщо ризик виявляється суттєвим, необхідно визначити та впровадити заходи для його контролю.

У разі потреби зниження рівня ризику розробляються заходи, спрямовані на зменшення ризику до прийнятного або практично низького рівня. Визначення та реалізація таких заходів здійснюються фахівцями експертної та робочої групи, починаючи з оцінки можливості зниження ризику за допомогою всіх доступних ресурсів і засобів. Якщо досягти прийнятного рівня ризику неможливо, заходи спрямовуються на його зменшення до практично низького рівня. Після їх впровадження проводиться оцінка залишкових ризиків з урахуванням вжитих заходів.

Таблиця 2.2 – Наслідки що є компонентами матриці ризику

Оцінка	Наслідки	Визначення
T1	Незначні	Вплив на екосистему мінімальний, не спричиняє значних наслідків для персоналу та населення, технічні пошкодження не становлять загрози безпеці працівників, існують попереджувальні заходи, а також резервування для процесів/обладнання.
T2	Низькі	Малозначні пошкодження без ускладнень, незначний вплив на екосистему, системи відновлюються швидко, без загрози для безпеки персоналу та здоров'я, технічний стан енергообладнання швидко відновлюється, висока ймовірність ремонту чи заміни, спричинення мінімальної моральної або матеріальної шкоди.
T3	Помірні	Вплив на екосистему помітний, але система може відновитися протягом певного часу або часткове відновлення наближається до початкового стану. Загрози, що виникають, були враховані під час проєктування або модернізації енергетичного підприємства. Є можливість повного відновлення системи до номінальних параметрів, технічне обладнання підлягає ремонту, можливе заміщення окремих компонентів за умови певних економічних витрат (враховуючи час простою, матеріальні витрати тощо).
T4	Значні	Вплив на екосистему є суттєвим, але можливе часткове відновлення. Існує загроза для безпеки та здоров'я персоналу енергетичного об'єкта. Повне відновлення систем, процесів чи обладнання після події неможливе. Енергетичне обладнання має низьку ймовірність ремонту, і подальша експлуатація в стандартних режимах неможлива. Це призводить до значних економічних збитків через пошкодження, тривалі перерви в роботі, необхідність заміни та модернізації обладнання. Усунення наслідків у короткі терміни є неможливим.
T5	Критичні	У разі настання загрози відновлення системи стає неможливим. Екосистема зазнає незворотних змін, що можуть мати довгострокові наслідки. Існує високий рівень небезпеки для безпеки та здоров'я як населення, так і персоналу. Технічне обладнання не підлягає ремонту або заміні, що призведе до серйозних матеріальних збитків. Окрім того, можуть виникнути інші суттєві негативні наслідки, що стосуються соціальної та економічної стабільності, що потребуватимуть значних зусиль для їх усунення..

Впровадження заходів зі зниження ризиків може супроводжуватися змінами в технологіях, технічному оснащенні, процесах функціонування підприємства або системах контролю, що потенційно створює нові чинники небезпеки та відповідні ризики. Наприклад, модернізація енергетичного обладнання може призвести до виникнення нових загроз, вплинути на рівень безпеки або змінити економічні та енергоефективні показники системи. Тому після реалізації заходів необхідно провести повторну оцінку ризиків для виявлення можливих нових небезпек.

Після впровадження заходів із запобігання та зниження ризиків робоча група проводить оцінку залишкового ризику. Для цього експерти створюють шкалу прийнятності ризиків для кожного конкретного фактора загрози. Верхня межа шкали визначається як сумарний індекс ризику всіх зафіксованих небезпек, що

дозволяє встановити максимальний потенційний рівень загроз для підприємства. Далі шкала поділяється на кілька діапазонів: **прийнятні ризики**, які не потребують додаткових заходів; **практично прийнятні ризики**, які потребують періодичного моніторингу та часткової реалізації профілактичних заходів; та **неприйнятні ризики**, для яких обов'язково розробляються комплексні заходи з мінімізації або усунення загрози.

Такий підхід дозволяє не лише систематизувати оцінку ризиків, а й забезпечує прозорість прийняття рішень для керівництва та відповідальних структур. Крім того, інтеграція шкали прийнятності з кількісними показниками, наприклад імовірністю настання події та потенційними втратами, підвищує точність ранжування ризиків і дозволяє формувати ефективні стратегії реагування на загрози. Система також передбачає можливість адаптації шкали у разі зміни зовнішніх умов, технологічних процесів або нових факторів загроз, що підвищує гнучкість та стійкість управлінських рішень.

Таблиця 2. 3 – **Матриця оцінки ризику для енергетичного підприємства**

Імовірність загроз / наслідків	Т1	Т2	Т3	Т4	Т5
Р1	РП	РПП	РПП	РН	РН
Р2	РПП	РПП	РН	РН	РН
Р3	РПП	РН	РН	РН	РН
Р4	РН	РН	РН	РН	РН
Р5	РН	РН	РН	РН	РН

Індекс ризику:
Ризик неприпустимий (РН)
Ризик практично прийнятний, але потребує постійного моніторингу та контролю (РПП)
Ризик прийнятний (РП)

Однією з ключових умов ефективного управління ризиками є належна організація системи реалізації, контролю та оцінки процесів, забезпечення необхідними ресурсами, включно з кваліфікованим персоналом, а також регулярний контроль діяльності. Відповідальність за це покладається на вищий керівний склад енергетичного підприємства.

2.2. Кваліметричні підходи до оцінювання ризиків енергопідприємств з урахуванням аспектів кібербезпеки

Кваліметрія, як наука, що займається кількісною оцінкою якості, базується на принципі об’єктивного відображення властивостей об’єкта через систему вимірюваних показників. У сфері управління ризиками цей підхід дозволяє перейти від суб’єктивних оцінок до числових значень, що підвищує точність і обґрунтованість управлінських рішень.

Основні принципи кваліметрії включають:

- **Системність** — врахування всіх аспектів ризику та взаємозв’язків між ними;
- **Комплексність** — охоплення технічних, організаційних, інформаційних і соціальних факторів;
- **Порівнюваність** — можливість порівнювати результати оцінки для різних об’єктів або процесів;
- **Адекватність** — відповідність отриманих оцінок реальним умовам функціонування системи.

Ефективність кваліметричного аналізу значною мірою залежить від правильного вибору показників, які відображають суть ризиків і відповідають критеріям **повноти, вимірюваності, незалежності та значущості**. Для оцінки ризиків у виробничих і технічних системах застосовуються:

- **Кількісні показники**: ймовірність відмов, інтенсивність відмов, очікувані фінансові втрати;
- **Якісні характеристики**: рівень підготовки персоналу, відповідність нормативним вимогам, культура безпеки.

Використання багаторівневих ієрархій критеріїв дозволяє структурувати ризики за напрямами: технічні, організаційні, інформаційні, екологічні та інші. Одним із ключових завдань є визначення **відносної ваги кожного показника** у загальному ризиковому профілі, що здійснюється через:

- методи експертних оцінок (зокрема, метод парних порівнянь та аналіз ієрархій Сааті);
- статистичні методи обробки даних;
- або їх комбіноване застосування.

На основі цих оцінок формується інтегральний показник ризику, який дозволяє проводити комплексну оцінку складних систем. Такий підхід спрощує процес прийняття рішень, оскільки забезпечує порівняння різних об’єктів або сценаріїв за єдиною шкалою, виділяє пріоритетні напрями для мінімізації ризиків та підвищує обґрунтованість управлінських заходів.

Сучасні ризики в енергетичному менеджменті мають комплексний та багатофакторний характер, що зумовлює необхідність застосування математичних і статистичних методів для їх аналізу. Найбільш поширеними інструментами є регресійний аналіз, факторний і кластерний аналіз, а також метод головних компонент. Ці підходи дозволяють виявляти приховані взаємозв’язки між показниками, визначати критично важливі фактори впливу та прогнозувати поведінку системи в умовах невизначеності та динамічних змін.

Разом із цифровізацією енергетичного сектору виникає новий клас ризиків, пов’язаних із кіберзагрозами. Традиційні кваліметричні методики, орієнтовані на технічні та організаційні аспекти, потребують адаптації для інтеграції показників інформаційної безпеки. Це передбачає включення таких критеріїв, як рівень захищеності інформаційних систем, кількість і критичність виявлених уразливостей, ефективність засобів аутентифікації та здатність до відновлення після кіберінцидентів. Такий підхід забезпечує комплексну оцінку ризиків, охоплюючи як матеріальні, так і інформаційні активи підприємства.

Особливу увагу слід приділяти своєчасності виявлення та нейтралізації загроз, стійкості систем до нових типів атак та рівню підготовки персоналу. Кваліметричні моделі повинні враховувати критерії швидкодії, адаптивності та відповідності міжнародним стандартам кібербезпеки, таким як ISO/IEC 27001 та рекомендації NIST. Оскільки спектр кіберзагроз постійно змінюється, значущість окремих факторів ризику також змінюється, що вимагає

застосування методів машинного навчання, багатофакторного аналізу та динамічного оновлення ваг показників.

Інтеграція цих підходів дозволяє не лише підвищити точність оцінки ризиків, а й створити адаптивну систему моніторингу та управління ризиками, яка здатна оперативно реагувати на нові загрози, прогнозувати потенційні наслідки та забезпечувати стабільну роботу енергетичних підприємств у цифровому середовищі.

Перспективним напрямом у сучасному енергетичному менеджменті є інтеграція кваліметричних методів із системами моніторингу кіберзагроз, включаючи дані з IDS/IPS, SIEM-платформ та баз індикаторів компрометації. Такий підхід дозволяє отримувати актуальні оцінки ризику у реальному часі, перетворюючи кваліметричні моделі не лише на аналітичний інструмент, а й на ефективний елемент оперативного управління інформаційною безпекою.

Пропонується алгоритм оцінки ризиків із врахуванням кіберкомпоненту для енергетичного підприємства, що включає такі етапи (рис. 1):

Етап 1. Визначення об’єкта аналізу та ідентифікація активів. Аналізується структура підприємства, його енергетична система та процеси, включно з виконавчими та забезпечуючими функціями. Визначаються критично важливі цифрові ресурси, інформаційні системи, бази даних та канали комунікації, які потребують захисту.

Етап 2. Ідентифікація загроз. Формується перелік потенційних загроз, у тому числі кіберзагроз: технічні збої, шкідливе ПЗ, фішингові атаки, витоки конфіденційних даних та інші. Повнота переліку та врахування взаємозв’язків між загрозами підвищують точність подальшого аналізу.

Етап 3. Формування системи показників ризику. Для кожної загрози визначаються ключові параметри оцінки: ймовірність настання події, масштаб можливих наслідків, час відновлення після інциденту та рівень готовності системи до протидії загрозам.

Етап 4. Побудова вагових коефіцієнтів. Значущість кожного показника визначається експертно або за допомогою статистичних методів. Для кіберкомпонентів використовується адаптивна модель ваг, що змінюється залежно від поточної загрозової ситуації, наприклад, у разі підвищення ризику фішингових атак або експлуатації уразливостей нульового дня. Враховується також взаємний вплив кіберзагроз на технічні ризики та персонал.

Етап 5. Обчислення інтегрального показника ризику. Кваліметрична модель дозволяє сформувати узагальнену оцінку, що включає як технічні, так і інформаційні параметри. Отриманий інтегральний показник служить для класифікації ризиків за рівнями: низький, середній, високий, критичний.

Етап 6. Моделювання сценаріїв впливу кіберзагроз. Застосування багатофакторного аналізу та імітаційного моделювання дозволяє прогнозувати наслідки атак різного масштабу, оцінювати потенційні втрати та визначати оптимальні стратегії реагування.

Етап 7. Формування рекомендацій та управлінських рішень. На основі інтегральних оцінок та змодельованих сценаріїв визначаються пріоритети захисних заходів, потреби у фінансуванні кіберзахисту, а також розробляються процедури оперативного реагування на інциденти.

Таким чином, запропонований алгоритм поєднує кваліметричні підходи з методами кіберризик-менеджменту, створюючи динамічну, адаптивну систему оцінки ризиків, що забезпечує підвищену стійкість енергетичного підприємства до кіберзагроз та дозволяє своєчасно реагувати на нові виклики цифрового середовища.

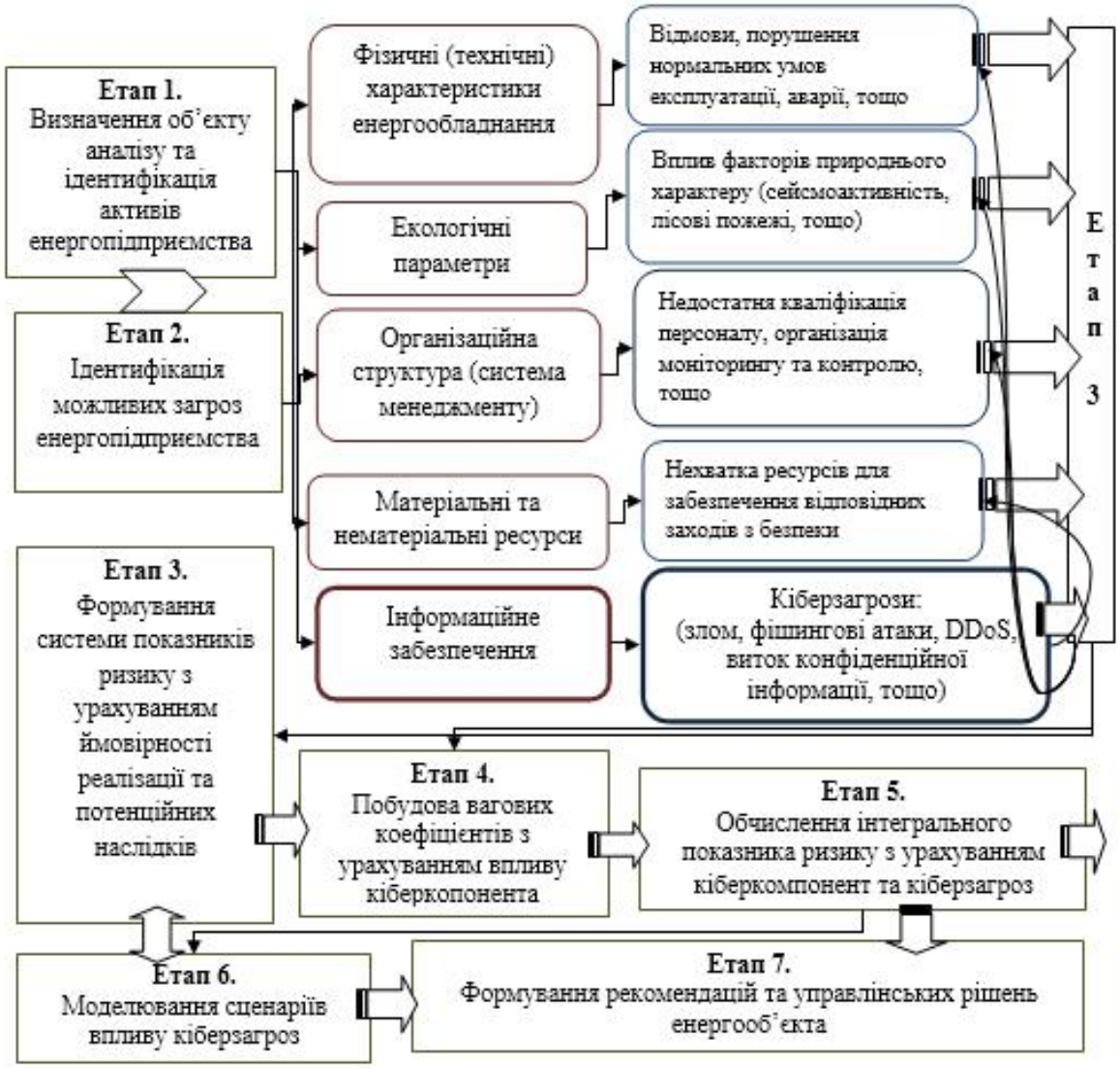


Рис.1 Схема-алгоритм оцінки ризиків з кіберкомпонентом для енергопідприємства

Визначення вагових коефіцієнтів для кожного типу загроз є ключовим етапом побудови ефективної системи оцінки ризиків. У класичних кваліметричних моделях ці коефіцієнти формуються на основі експертних оцінок, аналізу статистичних даних та ймовірності настання подій. Інтегральний показник ризику розраховується з урахуванням сукупності ваг, що відображають відносну значущість різних факторів і дозволяють комплексно оцінити вплив усіх загроз на діяльність підприємства.

З урахуванням зростаючої ролі цифрових загроз доцільно вводити додаткові показники, які характеризують рівень захищеності інформаційно-

комунікаційних систем підприємства та потенційний вплив кіберінцидентів на критичну інфраструктуру. Це дозволяє інтегрувати оцінку цифрових ризиків у загальну систему управління ризиками, підвищуючи точність і адаптивність моделей.

Пропонується модифікація вагових коефіцієнтів шляхом введення **додаткового коефіцієнта кіберкомпонента (W)**, що відображає рівень уразливості інформаційних систем та можливі наслідки кібератак для технологічних процесів підприємства. Наприклад, для SCADA-систем W зазвичай перевищує значення ваги для офісної IT-інфраструктури, оскільки їх порушення безпосередньо впливає на стабільність виробничих процесів.

Значення ваг можуть коригуватися динамічно залежно від поточного рівня кіберзагроз, визначеного за рамками NIST Cybersecurity Framework або ISO/IEC 27005, а також на основі наявності зареєстрованих інцидентів і критичності конкретного об’єкта для безперервного функціонування системи. Такий підхід дозволяє створити адаптивну модель ризик-менеджменту, яка враховує не лише традиційні технічні та організаційні ризики, а й нові виклики цифрової трансформації, забезпечуючи комплексну і реалістичну оцінку потенційних загроз.

Формула інтегральної ваги з урахуванням кіберфактора для енергетичного підприємства матиме вигляд:

$$W_i' = W_i(1 + \alpha C_r), \quad (1)$$

де W_i' – коефіцієнт ваги показника з модифікацією, W_i – начальна вага, C_r – коефіцієнт кіберризику (0…1), α – коефіцієнт що враховує чутливість моделі до кіберзагроз.

Інтегральний показник із врахуванням кіберфактору дозволяє точніше оцінити взаємодію технічних, організаційних, екологічних, економічних та інших чинників, підвищує об’єктивність комплексної оцінки безпеки підприємства, сприяє порівнянню різних об’єктів, відстеженню змін рівня безпеки та прогнозуванню впливу кіберзагроз на критичні процеси. Це

забезпечує більш збалансоване формування пріоритетів у системі управління ризиками.

Розглянемо застосування запропонованої моделі на прикладі атомних електростанцій із модифікацією вагових коефіцієнтів з урахуванням кіберризиків. Такий підхід дозволяє більш адекватно відобразити реальний стан безпеки об'єкта критичної інфраструктури, яким є АЕС. У традиційних методиках оцінка ризиків для АЕС зосереджувалася переважно на фізичних загрозах, таких як технічні відмови, помилки персоналу, природні катастрофи або порушення роботи систем охолодження та енергопостачання. Проте у сучасних умовах цифровізації технологічних процесів та активного застосування SCADA-систем, інтелектуальних датчиків і автоматизованих систем управління значно зростає роль кіберфакторів. Для наочності основні загрози та їхні вагові показники для АЕС наведено в таблиці 2, що ілюструє роботу запропонованої моделі.

Таблиця 2. Показники оцінки

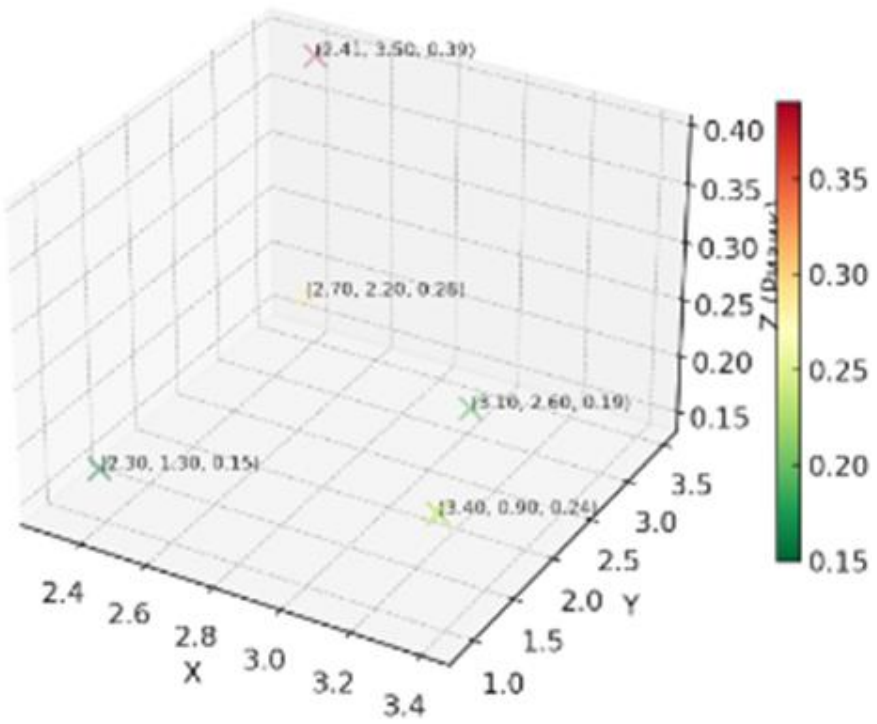
№	Загроза	Початковий ваговий коефіцієнт W_i
1	Відмова основного технологічного обладнання (реактор, турбіна, насоси)	0,30
2	Помилка персоналу при управлінні технологічними процесами	0,20
3	Зовнішні природні фактори (землетруси, повені, екстремальні температури)	0,15
4	Відмова систем охолодження	0,20
5	Порушення електропостачання ззовні	0,15
Сума ваг: **1,00** (нормована)		

Коефіцієнт кіберризику визначається для окремих можливих загроз C_r (0 – немає, 1 – максимум) і робиться зміна ваг (1), при якій α=0,5 (табл. 2.3).

Таблиця 2.3 Показники з урахуванням кіберкомпоненти

№	Загроза	Початковий ваговий коефіцієнт W_i	Коефіцієнт кіберризику C_r	Модифікований ваговий коефіцієнт W_i'
1	Відмова основного технологічного обладнання (реактор, турбіна, насоси)	0,30	0,6 (кібератака може вплинути на системи контролю)	0,39
2	Помилка персоналу при управлінні технологічними процесами	0,20	0,4 (соціальна інженерія, фішинг)	0,24
3	Зовнішні природні фактори (землетруси, повені, екстремальні температури)	0,15	0 (кіберзагрози не впливають)	0,15
4	Відмова систем охолодження	0,20	0,8 (маніпуляції з датчиками, SCADA)	0,28
5	Порушення електропостачання ззовні	0,15	0,5 (кібератаки на енергомережу)	0,19

З розрахунків модифікованого вагового коефіцієнта видно, що значущість технічних і організаційних ризиків з урахуванням кіберкомпонента зросла, зокрема для систем охолодження та технологічного обладнання. Водночас природні фактори залишилися на попередньому рівні, оскільки на них кіберзагрози не впливають. Ризик, пов’язаний із людським фактором, збільшився через потенційний вплив кіберсоціальних атак. Інтегральний показник ризику для АЕС без врахування кіберкомпонента становив 10,65, а з урахуванням кіберфактору він підвищився до 13,57, що відповідає зростанню на 27,4%.



3D-матриця ризиків в якій враховується часу виявлення загрози D на атомних електростанціях:

- X — ймовірність настання події (P);
- Y —небажана подія і її вплив (I);
- Z — кіберкомпонент (C).

Для комплексної оцінки загального рівня ризику, визначення його прийнятності та формування обґрунтованих управлінських рішень застосовують матриці ризику. Традиційні підходи ґрунтуються на поєднанні ймовірності настання події та потенційного масштабу її наслідків. Введення кіберкомпонента додає третій вимір, що відображає інформаційний вплив загрози, включаючи рівень доступності, цілісності та конфіденційності даних.

Завдяки цьому з’являється можливість формування багатовимірних 3D-матриць ризику, де три осі відображають ймовірність події, потенційні наслідки та вагу кіберфактора (рис. 2.2, табл. 2.4). Колірне кодування точок на матриці забезпечує швидке сприйняття рівня ризику: червоний — високий, жовтий — середній, зелений — низький.

Такі матриці дозволяють керівництву енергетичних підприємств оперативно ідентифікувати найбільш критичні ризики, у яких інформаційний

компонент значно підсилює загрозу. Крім того, багатовимірні матриці сприяють пріоритизації заходів управління ризиками, оскільки вони демонструють не лише технічні та організаційні аспекти, а й взаємозв'язок між традиційними та цифровими загрозами.

Для підвищення точності оцінки рекомендується використовувати адаптивні матриці, де значення кіберкомпонента оновлюються на основі даних із систем моніторингу кіберзагроз (IDS/IPS, SIEM, бази індикаторів компрометації) та результатів проведених аудиторських перевірок. Це дозволяє перетворити матриці ризику з аналітичного інструменту на динамічний інструмент підтримки прийняття управлінських рішень у реальному часі.

Показник оцінки ризику	Опис	Одиниці вимірювання	Вага (W)
P – Ймовірність настання небажаної події	Частота виникнення події	бал (1–5)	0,3
I – Вплив, наслідки	Рівень шкоди (фінансової, репутаційної)	бал (1–5)	0,4
C – Кіберкомпонент	Уразливість до кіберзагроз	бал (1–5)	0,2
D – Час виявлення	Швидкість виявлення інциденту	години/дні	0,1

Запропонована методика оцінки рівня ризиків, яка інтегрує кваліметричні підходи з урахуванням кіберзагроз, має низку суттєвих переваг. Вона дозволяє формувати більш повну та системну картину безпеки підприємства, поєднуючи технічні, організаційні та інформаційні фактори. Гнучка структура вагових коефіцієнтів забезпечує адаптацію моделі до динамічних змін зовнішнього та внутрішнього середовища, а також до появи нових загроз. Використання багатовимірних матриць ризиків та можливість їх візуалізації спрощують процес прийняття управлінських рішень і підвищують точність прогнозування потенційних негативних сценаріїв.

Одночасно слід враховувати деякі обмеження методики при її практичному застосуванні. По-перше, достовірність оцінок значною мірою залежить від якості вихідних даних, зокрема точності статистики інцидентів,

повноти інформації про кіберзагрози та коректності формування показників. По-друге, для забезпечення об’єктивності результатів необхідне залучення експертів для визначення та коригування вагових коефіцієнтів, що може вносити певний суб’єктивний фактор і вимагає дотримання чітких професійних та етичних стандартів.

Ще однією складністю є масштабування методики для великих підприємств із різнорідними технологічними процесами, особливо для об’єктів підвищеної небезпеки та критичної інфраструктури. У таких випадках доцільне впровадження попередньої адаптації моделі, включно з деталізацією рівнів оцінки ризиків за підрозділами, процесами та окремими критичними активами. Додатково рекомендується періодично оновлювати показники та ваги кіберкомпонента, використовуючи дані моніторингу кіберзагроз, аналітику інцидентів та сучасні стандарти інформаційної безпеки (ISO/IEC 27001, NIST), щоб підтримувати актуальність і точність оцінки ризиків у реальному часі.

Завдяки таким удосконаленням методика стає не лише аналітичним інструментом, а й ефективним засобом оперативного управління ризиками, що дозволяє енергетичним підприємствам підвищувати стійкість до технічних, організаційних та кіберзагроз.

ВИСНОВКИ

Сучасні енергетичні підприємства потребують ефективних стратегій управління для забезпечення безпеки та стабільності своєї діяльності. Впровадження таких стратегій можливе через застосування підходів до управління та оцінки ризиків на основі нормативних вимог, зокрема міжнародних стандартів ISO 9001 (управління якістю) та ISO 31000 і IEC 31010 (управління ризиками). На основі цих стандартів була розроблена модель управління ризиками для енергетичного підприємства з докладним описом кожного етапу її реалізації.

На етапі оцінки ризиків рекомендується, відповідно до нормативних документів, виконувати як якісний, так і кількісний аналіз ймовірності настання небажаних подій і оцінювати їхні наслідки. При цьому слід враховувати вплив технічних змін енергетичного обладнання та факторів зовнішнього середовища, таких як несприятливі метеоумови або сейсмоактивність.

Оцінка наслідків порушень функціонування передбачає врахування внутрішніх факторів — можливості ремонту, модернізації обладнання, зміни режимів експлуатації, — а також впливу на навколишнє середовище у разі настання інцидентів. Для визначення ймовірності подій та їхніх наслідків застосовується п’ятибальна шкала безпеки з кількісною оцінкою ймовірності загроз та п’ятибальна описова шкала для наслідків на обладнання та навколишнє середовище, що охоплює діапазон від повного відновлення до незворотних змін.

Управління ризиками на енергетичних підприємствах є комплексним процесом, який включає технічні, організаційні та інформаційно-кіберні аспекти. Ефективна оцінка ризиків забезпечує стійкість підприємства до внутрішніх і зовнішніх загроз, мінімізує потенційні втрати та сприяє безперебійному постачанню енергоресурсів.

Кваліметричні підходи дозволяють кількісно оцінювати рівень ризиків та ранжувати їх за значущістю. Інтеграція експертних оцінок, статистичних даних та сучасних методів моделювання забезпечує об’єктивність, прозорість та комплексність аналізу.

Врахування кіберкомпонента є обов’язковим у сучасних умовах цифровізації енергетичних систем. Показники інформаційної безпеки, рівень уразливості цифрових систем та ймовірність реалізації кіберзагроз повинні бути інтегровані в загальну систему оцінки ризиків, що підвищує точність та актуальність результатів.

Використання багатовимірних матриць ризиків, інтегральних показників та адаптивних вагових коефіцієнтів дозволяє керівництву енергетичних підприємств оперативно ідентифікувати критично важливі загрози та пріоритизувати заходи щодо їхнього зниження.

Методика оцінки ризиків є гнучкою і придатною для масштабування на різні підприємства та об’єкти підвищеної небезпеки. Проте ефективність її застосування залежить від достовірності вихідних даних, залучення кваліфікованих експертів та регулярного оновлення інформації про кіберзагрози та стан технічних систем.

Впровадження запропонованої методики дозволяє не лише підвищити рівень безпеки та надійності енергетичних підприємств, а й створює основу для системного управління ризиками, інтегрованого у стратегію розвитку та планування, сприяючи довгостроковій стійкості підприємства.