https://doi.org/10.26565/2079-1747-2025-36-10
УДК 658.62.018.012

[1]А. Я. ЛИСЕНКО,
аспірант кафедри автоматизації, метрології та енергоефективних технологій
e-mail: dagost@ukr.net ORCID: https://orcid.org/0009-0007-3916-8029
[1]Р. С. НОС,
аспірант кафедри автоматизації, метрології та енергоефективних технологій
e-mail: nosruslan@gmail.com ORCID: https://orcid.org/0009-0006-5391-7703
[1]К. І. МАЗОРЧУК,
аспірантка кафедри автоматизації, метрології та енергоефективних технологій
e-mail: ekaterina.mazorchuk@gmail.com ORCID: https://orcid.org/0009-0001-0769-4872
[1]С. С НЕГОДОВ,
аспірант кафедри автоматизації, метрології та енергоефективних технологій
e-mail: titansv2017@gmail.com ORCID: https://orcid.org/0000-0003-3561-6924
[1]Харківський національний університет ім. В. Н. Каразіна
майдан Свободи, 4, м. Харків, 61022, Україна.

УДОСКОНАЛЕННЯ КВАЛІМЕТРИЧНИХ ПІДХОДІВ ДО ОЦІНЮВАННЯ РИЗИКІВ ЕНЕРГОПІДПРИЄМСТВ З УРАХУВАННЯМ АСПЕКТІВ КІБЕРБЕЗПЕКИ

У статті розглянуто можливість застосування кваліметричних підходів до оцінювання ризиків з урахування сучасних аспектів кіберзагроз, що виникають на енергетичних підприємствах. З метою оцінювання і управління ризиками проаналізовано науко-технічну і нормативну базу і запропоновано алгоритм-схему яка враховує кіберкомпонент, який є як окремою загрозою для функціонування енергопідприємства, так і може впливати на інші загрози різного характеру, і як наслідок підвищити рівень загального ризику. У ході проведеного дослідження було розроблено науково-обґрунтовану методику оцінювання рівня безпеки підприємства з урахуванням кіберзагроз. Запропонований підхід поєднує кваліметричні методи та модифіковану систему вагових коефіцієнтів, що дало змогу сформувати інтегральну модель аналізу ризиків, що забезпечує більш комплексне уявлення про стан захищеності об'єкта та дає можливість своєчасно виявляти критичні вразливості як на етапі планування заходів безпеки, так і під час ухвалення управлінських рішень у процесі функціонування. У дослідженні проаналізовано базові загрози для атомної електростанції, що дозволило ідентифікувати приховані загрози, а саме, встановлено, що відмова систем охолодження може бути спричинена не лише фізичними несправностями, а й цілеспрямованим втручанням у програмне забезпечення чи спотворенням сигналів датчиків, що враховано під час оцінки ризиків. В роботі представлено візуалізація оцінювання ризиків у вигляді 3D матриці ризиків з кіберкомпонентом, яка дає краще уявлення та допомагає керівникам енергопідприємств швидко ідентифікувати найбільш критичні ризики, у яких кіберфактор суттєво посилює загрозу. Застосування інтегральної моделі засвідчило, що фактичний рівень ризиків атомної електростанції істотно зростає за рахунок кіберкомпонента. У порівнянні з базовим варіантом оцінювання, інтегральний показник ризику з врахуванням кіберкомпонента підвищується на 10–25 %, що підтверджує необхідність системного включення заходів кіберзахисту до загальної політики безпеки атомної енергетики.

КЛЮЧОВІ СЛОВА: ризик, кваліметричний підхід, енергетичні підприємства, кіберзагрози, оцінювання, матриці ризику

Як цитувати: Лисенко А. Я., Нос Р. С., Мазорчук К. І., Негодов С. С. Удосконалення кваліметричних підходів до оцінювання ризиків енергопідприємств з урахуванням аспектів кібербезпеки. *Машинобудування*. 2025. Вип. 36. С. 102-118. https://doi.org/10.26565/2079-1747-2025-36-10

Постановка проблеми та її зв'язок із важливими науковими чи практичними завданнями

У сучасних умовах динамічного розвитку технологій та підвищення вимог до безпеки підприємств, процес оцінювання ризиків стає невід'ємним елементом ефективного управління якістю функціонування та забезпечення відповідності нормативним вимогам та параметрам. Ризики можуть виникати на всіх етапах життєвого циклу підприємства - від проектування та виробництва (функціонування) до експлуатації в позапроєктні терміни, зняття з експлуатації та утилізації відпрацьованих матеріалів та обладнання. Своєчасна ідентифікація та мінімізація ризиків дозволяє не лише запобігти потенційним загрозам для соціума та навколишнього середовища, але й оптимізувати процеси, зменшити витрати та підвищити конкурентоспроможність підприємства.

Сучасні енергопідприємства функціонують у складному середовищі, що зумовлено постійними змінами, як вихідних параметрів, так і вимог до процесів, де ефективність виробництва та надійність постачання енергії залежать не лише від технічного стану обладнання, а й від здатності своєчасно ідентифікувати та мінімізувати ризики. Цифровізація енергетичної галузі, що передбачає впровадження автоматизованих систем управління, інтелектуальних мереж (smart grids), інтернету речей (IoT) та технологій великих даних (Big Data), значно розширює можливості функціонування, забезпечення безпеки, моніторингу та прогнозування подальшого технічного стану, але водночас створює нові виклики і загрози.

В умовах переходу до «цифрової енергетики» традиційні підходи до оцінювання ризиків втрачають ефективність, адже зростає кількість потенційних загроз, зокрема кіберризиків, техногенних аварій, збоїв у цифрових системах управління та помилок у роботі алгоритмів функціонування, що потребує удосконалення методології ризик-менеджменту з урахуванням інтеграції цифрових технологій, забезпечення кібербезпеки та підвищення стійкості інфраструктури до комплексних впливів.

Таким чином, актуальність дослідження полягає у необхідності формування сучасних методів оцінювання ризиків для енергопідприємств, які здатні адаптуватися до умов цифровізації та забезпечити безперервність, безпеку й ефективність енергетичних процесів.

Аналіз останніх досліджень і публікацій

Кваліметричний підхід, як один з науково-практичних методів, використовують до кількісної оцінки якості складних об'єктів і процесів шляхом побудови інтегральних показників на безрозмірних шкалах, нормування та зважування компонентів якості, що успішно впроваджується та досліджується науковцями в машинобудуванні, харчовій промисловості, енергетичній сфері, фінансовій діяльності, освіті, тощо [1-5]. У застосуванні до ризик-менеджменту кВаліметричні методи дозволяють перетворити якісні (експертні) судження про фактори ризику у формалізовані числові показники, що спрощує ранжування ризиків та прийняття управлінських рішень [6, 7].

У класичних кваліметричних схемах використовують багатоступеневе зважування критеріїв (експертні ваги), приведення показників до єдиної безрозмірної шкали (нормалізація), та агрегування (сума, зважена сума або складніші функції). Для частини ідентифікації та оцінювання ризиків, в якості інструментів використовують матриці оцінок, шкали Лайкерта, методи ранжування та багатокритеріальний аналіз [8-10]. Сучасні роботи також пропонують отримувати розподіли показників і ризиків через статистичне моделювання щільності оцінок, що дає змогу визначати ймовірнісні інтервали ризику [11, 12].

У енергетичному секторі використовуються як суто кількісні підходи (QRA, Monte-Carlo), так і напівкількісні та кваліметричні методики для швидкої рангової оцінки великої кількості ризиків: технічних, організаційних, екологічних та дедалі частіше апелюють до необхідності врахування кіберризиків. Практичні посібники для енергетичної інфраструктури під креслюють важливість поєднання якісних експертних оцінок з кількісними інструментами, аби методика була водночас обґрунтованою, прозорою та застосовною у ресурсних обмеженнях, адже часто прогнозування ризиків ускладнено у звязку з обмеженістю статистичної інформації [13-16].

Останні дослідження [17-19] показують, що для енергопідприємств ефективна методика повинна бути багаторівневою: (1) інвентаризація об'єктів/систем, (2) ідентифікація загроз і вразливостей, (3) експертне присвоєння показників якості/уразливості, (4) нормалізація та агрегування у інтегральний ризик. У роботах [20-22], що досліджують енергетику та суміжні галузі (нафтогаз, відновлювана енергетика), відзначається тренд до комбінування кваліметричних оцінок з моделями часово-залежного ризику і сценарним аналізом. Іншим напрямом досліджень, є розгляд можливості поєднання кваліметрії з інструментами машинного навчання, аналізом великих даних і онлайн-моніторингом, що дає змогу автоматизувати збір оцінок, уточнювати вагові коефіцієнти на основі ретроспективних даних, щодо інцидентів, збоїв, відмов, моделювати розподіли ймовірностей та оперативно перераховувати інтегральні ризики у разі зміни стану системи. Особливо важливим стає включення окремих кіберпоказників у загальну кваліметричну модель (уразливість інформаційно-технічної системи, час виявлення інциденту, можливість відновлення), оскільки кіберінциденти впливають як на доступність, так і на цілісність та конфіденційність енергосервісів[5, 13].

Як відзначають автори [23, 24] перевагами застосування кваліметричного підходу для енергетичних систем є його придатність для оцінювання багатопарметричних об'єктів, можливості швидкого ранжування, прозорість для прийняття управлінських рішень, гнучкість відносно додавання нових показників та параметрів відповідно до модернізації систем та перерозподіл загроз і критеріїв оцінки. Разом з тим, кваліметричні підходи мають і ряд обмежень, що необхідно враховувати при їх застосуванні, як то відповідний професіоналізм та неупередженість експерттів, проблеми зі статистичною валідацією у разі відсутності великих наборів даних інцидентів, що характерно для великих енергетичних комплексів, як атомні станції, необхідність інтеграції з кількісними моделями для оцінки великих технічних ризиків (наприклад, вибухів, пожеж, механічних відмов, тощо).

Аналіз літератури [25-28] показує ключові прогалини в сучасних наукових алгоритмах оцінювання ризиків, особливо для українських енергосистем, а саме потреба в стандартизованих наборах кіберіндикаторів для енергосектора, розрбки методів об'єктивізації експертних ваг (наприклад, через агрегування даних про інциденти або машинне навчання), інтеграція кваліметрії з реальним time-series моніторингом та сценарним аналізом стійкості, розробка підходів валідації кваліметричних моделей на основі історичних кейсів і симуляцій.

Кваліметричні методи є практичним інструментом для оцінювання ризиків у енергетиці, особливо коли потрібно швидко ранжувати багато різнорідних загроз та врахувати якісні фактори (включно з кібербезпекою). Однак для підвищення надійності результатів їх потрібно комбінувати з кількісними методами, удосконалювати процедури отримання й перевірки експертних ваг та використовувати можливості IT (аналітика великих даних, ML) для зниження суб'єктивності та підвищення адаптивності моделей.

Також, слід зазначити, що у сфері управління ризиками та кібербезпеки для енергетичних підприємств ключове значення мають міжнародні стандарти, які задають методологічні основи та практичні інструменти оцінювання. Так, ISO 31000 "Risk Management – Guidelines" [29] визначає загальні принципи, структуру та процеси управління ризиками та забезпечує універсальну методологічну основу, яка дозволяє адаптувати управління ризиками до специфіки енергетичних підприємств. Важливо зазначити, що ISO 31000 орієнтований на системний підхід і передбачає ідентифікацію, аналіз, оцінювання та обробку ризиків з урахуванням як технічних, так і організаційних факторів. У контексті кваліметрії цей стандарт формує основу для розробки кількісних та якісних критеріїв оцінювання ризиків. В свою чергу, ISO/IEC 27001 "Information Security Management Systems" [30] є провідним стандартом у сфері інформаційної безпеки, що регламентує створення, впровадження та підтримку систем управління інформаційною безпекою (СУІБ). Для енергетичних підприємств цей стандарт особливо актуальний через зростання рівня цифровізації, підключення до "розумних мереж" (smart grids) та використання

SCADA-систем. Інтеграція положень ISO/IEC 27001 дозволяє врахувати аспекти кіберзагроз у загальній системі управління ризиками та поєднати їх із кваліметричними методами оцінювання. NIST SP 800-82 “Guide to Industrial Control Systems (ICS) Security” [31] надає рекомендації щодо захисту промислових систем управління, зокрема SCADA (Supervisory Control and Data Acquisition), DCS (Distributed Control System) та інших технологій, які широко застосовуються в енергетиці. На відміну від ISO-стандартів, документ NIST орієнтований на практичні технічні заходи, що дозволяє деталізувати підхід до оцінювання ризиків кіберзагроз [32, 33]. Так, у [34] Національного інституту стандартів і технологій США (NIST) розроблено дорожню карту розвитку кібербезпеки для критичної інфраструктури та виділено напрями, що потребують пріоритетної уваги: автентифікація, автоматизований обмін індикаторами загроз, оцінка відповідності, підготовка кадрів, аналіз даних, управління ланцюгами постачання, міжнародна співпраця та стандарти у сфері конфіденційності. Дорожня карта стала основою для формування підходів до гармонізації кіберзахисту в промислових та енергетичних системах.

Table 1

Comparison of international regulatory documents on risk management and cybersecurity in the energy sectorenergy sector

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-менеджмент	Дозволяє захистити дані, мережеву інфраструктуру та SCADA-системи енергопідприємств від кіберзагроз
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

Використання рекомендацій NIST у поєднанні з ISO 31000 та ISO/IEC 27001 створює комплексну основу для інтегрованої системи управління ризиками та забезпечує методологічну та практичну базу для розробки удосконалених кваліметричних підходів. Вони дозволяють гармонізувати кількісні та якісні методи оцінювання ризиків, враховуючи не лише технічні параметри обладнання, але й інформаційно-кібернетичні аспекти, що дедалі більше впливають на безпеку функціонування енергопідприємств (табл. 1).

В Європейському просторі, питання забезпечення кібербезпеки також мають важливе значення і активно обговорюються Європейською комісією (ЄК) з метою забезпечення захисту критичної інфраструктури. Так, ЄК запропонувала комплексну програму для посилення захисту критичної інфраструктури (CIP) у державах-членах ЄС, у звязку з цим розробила відповідний документ [35], який визначає основні принципи управління ризиками, пов'язаними з фізичними та кіберзагрозами, та окреслює рамки співпраці між країнами ЄС. Основний акцент робиться на ідентифікації об'єктів критичної інфраструктури, створенні єдиного механізму оцінювання загроз і запровадженні підходів до превентивного управління ризиками. У 2015 році Європейська Комісія запропонувала концепцію «Енергетичного союзу», спрямованого на підвищення стійкості енергетичної системи ЄС, зменшення залежності від зовнішніх постачальників енергоресурсів і адаптацію до викликів зміни клімату [36], що зумовлює необхідність інтеграції внутрішнього енергетичного ринку, інвестування у відновлювану енергетику та підвищення рівня енергетичної безпеки за допомогою диверсифікації джерел постачання та цифровізації енергосистем з акцентом на кіберзахисті енергетичної інфраструктури.

Розглянуті нормативні документи демонструють еволюцію міжнародних підходів до управління ризиками та захисту критичної інфраструктури, що включає як загальну методологію і системний підхід, які запропоновані в міжнародних стандартах ISO до конкретних технічних та організаційних кроків з розвитку кіберзахисту, як в стандартах NIST. Європейська Комісія, у свою чергу, зосереджується на інтеграції політик безпеки та енергетики в рамках ЄС, але спільною рисою на всіх рівнях є акцент на системному управлінні ризиками, посиленні кібербезпеки та розвитку міжнародної співпраці для забезпечення стійкості енергетичних та інфраструктурних систем.

Виклад основного матеріалу

Кваліметрія як наука про кількісне оцінювання якості базується на ідеї об'єктивного відображення властивостей об'єкта через систему вимірюваних показників. У контексті управління ризиками цей підхід дозволяє перейти від якісних суджень до кількісних оцінок, що підвищує точність прийняття управлінських рішень. Основними принципами є: системність (урахування всіх аспектів ризику), комплексність (охоплення технічних, організаційних та соціальних чинників), порівнюваність (можливість співставлення результатів різних об'єктів або процесів), а також адекватність (відповідність оцінки реальним умовам функціонування системи).

Ефективність кваліметричного аналізу значною мірою залежить від правильності добору показників, які відображають сутність ризиків та відповідають вимогам повноти, вимірюваності, не залежності та значущості [37]. Для оцінювання ризиків у виробничих та технічних системах використовуються як кількісні показники (ймовірність відмов, інтенсивність відмов, фінансові втрати), так і якісні характеристики (рівень підготовки персоналу, відповідність нормативним вимогам). Застосування багаторівневих ієрархій критеріїв дозволяє структурувати ризики за сферами прояву: технічні, організаційні, інформаційні, екологічні тощо [38, 39]. Разом з тим, однією з ключових задач кваліметрії є визначення відносної значущості (ваги) кожного показника у загальній структурі ризику. Для цього застосовуються методи експертних оцінок (метод парних порівнянь, аналіз ієрархій Сааті), статистичні методи або комбіновані підходи. Побудова інтегрального показника ризику забезпечує можливість комплексної оцінки складних систем і спрощує процес прийняття рішень на основі узагальненого рівня ризику, що дозволяє порівнювати різні об'єкти чи сценарії за єдиною шкалою [40, 41].

Особливістю сучасних ризиків в системі енергетичного менеджменту є їх багатофакторний характер, що вимагає застосування методів математичного та статистичного аналізу. До найбільш поширених належать регресійний аналіз, факторний та кластерний аналіз, метод головних компонент, використання яких дозволяє виявити приховані залежності між показниками, визначити найбільш критичні фактори впливу та прогнозувати поведінку системи в умовах невизначеності.

Сучасні умови цифровізації виробничих і управлінських процесів призвели до появи нового класу ризиків, пов'язаних із кіберзагрозами. Традиційні кваліметричні методики, орієнтовані переважно на технікні та організаційні фактори, потребують удосконалення для адекватного врахування специфіки інформаційної безпеки, що можливо при врахуванні показників оцінювання ризиків що зумовлені кіберзагрозам, розробки специфічних критеріїв оцінки, використання динамічних показників та інтеграції цих підходів в існуючи системи. Для реалізації такого підходу необхідно до традиційних параметрів ризику додати нові, пов'язані з цифровою інфраструктурою: рівень захищеності інформаційних систем, кількість та критичність уразливостей, ефективність засобів аутентифікації, здатність до відновлення після кіберінцидентів, що забезпечить комплексний погляд на ризик, який охоплює як матеріальні, так і інформаційні активи.

У сфері кібербезпеки значну роль відіграє своєчасність виявлення та нейтралізації загроз, стійкість до нових видів атак, рівень підготовки персоналу у сфері кіберзахисту. Відповідно, у кваліметричні моделі слід інтегрувати критерії швидкодії, адаптивності та відповідності міжнародним стандартам кібербезпеки (ISO/IEC 27001, NIST тощо). А оскільки спектр кіберзагроз постійно змінюється, значущість окремих факторів ризику також варіює, що потребує застосування методів машинного навчання та багатофакторного аналізу для автоматиного коригування ваг показників залежно від актуальних умов. Крім того, перс пективним є інтегрування кваліметрії з системами моніторингу кіберзагроз, а саме використання даних із систем виявлення вторгнень, SIEM-платформ (Security Information and Event Management) та баз індикаторів компрометації дозволяє формувати актуалізовану оцінку ризику в режимі реального часу. Таким чином, квалітетричні моделі стають не лише інструментом аналітики, а й складовою системи оперативного управління інформаційною безпекою.

Для цього пропонується алгоритм оцінки ризиків з кіберкомпонентом для енергетичного підприємства, який складається з наступних етапів (рис.1):

Eman 1. Визначення об'єкту аналізу та ідентифікація активів. На цьому етапі проводиться аналіз енергетичного підприємства, його структура, компоненти енергетичної системи, процеси, як виконавчі, так і забезпечуючі, визначаються інформаційні системи, бази даних, канали комунікації та критичні цифрові ресурси, що підлягають захисту.

Eman 2. Ідентифікація загроз енергопідприємства. На цьому етапі паралельно з Етапом 1 формується перелік потенційних загроз з урахуванням можливих кіберзагроз - від технічних збоїв та шкідливого програмного забезпечення до фішингових атак і витоку конфіденційних даних. Слід зауважити, чим повніший буде перелік можливих загроз, як внутрішніх, так і зовнішніх, тим якісніше буде аналіз, разом з тим необхідно враховувати взаємозв'язок зовнішніх факторів на внутрішні процеси енергетичної системи.

Eman 3. Формування системи показників ризику. Для кожної загрози визначаються параметри оцінки: імовірність виникнення, масштаб можливих наслідків, час відновлення після інциденту, рівень готовності системи до протидії атакам.

Eman 4. Побудова вагових коефіцієнтів. Важливість кожного показника визначається експертним шляхом або за допомогою статистичних методів. Для кіберкомпонентів застосовується адаптивна модель ваг, яка змінюється залежно від актуальної загрозової ситуації (наприклад, зростання ваги факторів «фішингові атаки» чи «використання вразливостей нульового дня»). При реалізації цього етапу необхідно врахувати кіберкомпоненту і її вплив на інші можливі загрози, ймовірності їх настання в результаті кіберзагрози та відповідні наслідки, тобто , наприклад, вплив кібератак на технічні системи енергооб'єкту, на можливості реагування персоналу (професійність та кваліфікація) у разі порушення роботи систем моніторингу, тощо.

Eman 5. Обчислення інтегрального показника ризику. На основі кваліметричної моделі формується узагальнена оцінка, яка враховує як технічні, так і інформаційні параметри. Інтегральний показник дозволяє класифікувати ризики за рівнями: низький, середній, високий, критичний.

Eman 6. Моделювання сценаріїв впливу кіберзагроз. Використання методів багатофакторного аналізу та імітаційного моделювання дозволяє прогнозувати наслідки атак різного масштабу та визначати оптимальні стратегії реагування.

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

Таким чином, запропонований алгоритм інтегрує кваліметричні підходи з методами кіберризик-менеджменту, що дозволяє створити динамічну систему оцінювання та підвищити рівень стійкості організації до кіберзагроз.

Важливим етапом формування ефективної оцінки ризиків є визначення вагових коефіцієнтів для кожного виду загроз. У традиційних кваліметричних моделях вагові коефіцієнти формуються на основі експертних оцінок, статистичних даних та аналізу ймовірності реалізації ризиків, а моделі ризик-менеджменту передбачають розрахунок інтегрального показника ризику на основі набору вагових коефіцієнтів, що відображають відносну значущість різних факторів. Проте з огляду на зростання кіберзагроз, доцільно враховувати додатковий набір показників, пов'язаних із захищеністю інформаційно-комунікаційних систем енергопідприємства, які здатні істотно впливати на функціонування критичної інфраструктури. Така модифікація дозволяє інтегрувати цифрові ризики у загальну модель оцінювання. Для інтеграції кіберризиків до системи оцінювання пропонується модифікація вагових коефіцієнтів шляхом введення додаткового коефіцієнта кіберкомпонента (W_C), який враховує рівень уразливості інформаційних систем підприємства, а також потенційний вплив атак на технологічні процеси. Наприклад, для SCADA-систем коефіцієнт може мати вищу вагу, ніж для офісної IT-інфраструктури. Ваги можуть змінюватися залежно від: поточного рівня кіберзагроз (визначається з використанням NIST Cybersecurity Framework або ISO/IEC 27005); наявності виявлених інцидентів; ступеня критичності енергетичного об'єкта.

Формула інтегральної ваги з кіберфактором для енергетичного підприємства буде мати вигляд:

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

де W_i'– модифікований ваговий коефіцієнт показника, W_i – початкова вага без урахування кіберфактора, C_r – коефіцієнт кіберризику (0…1), α – коефіцієнт чутливості моделі до кіберзагроз.

Інтегральний показник з урахуванням кіберфактору дозволяє точніше врахувати взаємодію технічних, організаційних, екологічних, економічних та інших факторів, підвищити об'єктивність інтегральної оцінки безпеки підприємства, порівнювати підприємства між собою, визначати динаміку зміни рівня безпеки та прогнозувати вплив кіберзагроз на критичні процеси, даючи змогу формувати більш збалансовану систему пріоритетів у управлінні ризиками.

Розглянемо застосування запропонованої моделі для атомних електростанцій на основі модифікація вагових коефіцієнтів із урахуванням кіберризиків, що дозволяє більш адекватно відображати реальну картину безпеки об'єкта критичної інфраструктури, яким є атомна електростанція. У класичних підходах оцінка ризиків для АЕС традиційно концентрувалася на фізичних загрозах: технічних відмовах, помилках персоналу, природних катастрофах, порушеннях систем охолодження чи енергопостачання. Проте в умовах цифровізації технологічних процесів, активного використання SCADA-систем, інтелектуальних датчиків та автоматизованих систем керування, зростає вплив кіберфакторів. Виокремо основні загрози і їх вагові показники для АЕС (табл. 2) для наочності відображення запропонованої моделі.

Для кожної загрози визначається коефіцієнт кіберризику C_r (0 – відсутній, 1 – максимальний) і виконується модифікація ваг за формулою (1), де чутливість моделі α=0,5 (табл. 3).

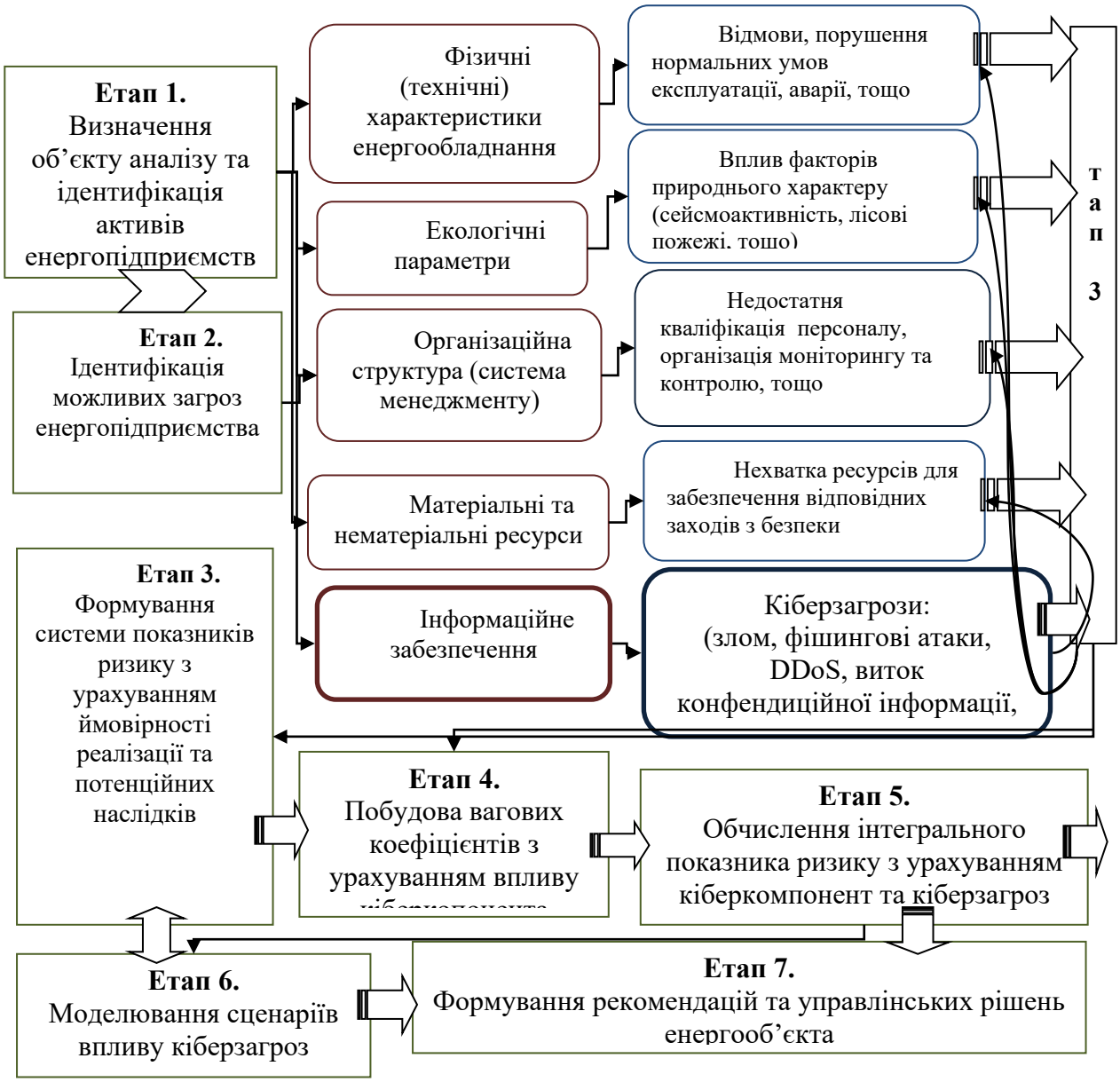

Рис. 1– Схема-алгоритм оцінки ризиків з кіберкомпонентом для енергопідприємства
Fig. 1 – Risk assessment algorithm with a cyber component for an energy enterprise

Table 2
Basic threats to a nuclear power plant (without cyber component)
Таблиця 2
Базові загрози для атомної електростанції (без кіберкомпонента)

№	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)	

Table 3

Modified weighting factor taking into account the cyber component for a nuclear power plant

Таблиця 3

Модифікований ваговий коефіцієнт з урахуванням кіберкомпонента для атомної електростанції

№	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 отриманих даних розрахунку модіфікованого вагового коефіцієнту видно, що зросла важливість технічних і організаційних ризиків, що мають кіберкомпонент (системи охолодження, технологічне обладнання); природні фактори залишилися без змін, оскільки кіберзагрози їх не посилюють, а ризик людського фактору підвищився через вплив кіберсоціальних атак. При цьому інтегральний розрахунок ризику для АЕС показав, інтегральний індекс без кіберкомпонента дорівнює 10,65, а інтегральний індекс з кіберкомпонентом - 13.57, що свідчить про приріст: +27.4%.

Для візуалізації отриманих даних і оцінювання загального рівня з метою визначення прийнятності ризику та розробки рекомендацій для подальшого управління енергопідприємством використовують матриці ризику. Класичні матриці ризику ґрунтуються на комбінації ймовірності події та ступеня її наслідків. Додавання кіберкомпонента передбачає включення третього виміру – інформаційного впливу (наприлад, вплив на доступність, цілісність та конфіденційність даних) (табл. 4). Це дозволяє отримати багатовимірні матриці - 3D-матриці ризиків, де на осях відображаються ймовірність, наслідки та кіберфактор (рис. 2), де чим вище ризик, тим ближче колір точки до червоного, а при низькому ризику - зелений. Таке представлення допомагає керівникам енергопідприємств швидко ідентифікувати найбільш критичні ризики, у яких кіберфактор суттєво посилює загрозу.

Запропонована методика оцінювання рівня ризиків, що поєднує кваліметричні підходи з урахуванням кіберзагроз, має низку переваг, а її застосування дозволяє отримати більш комплексну картину безпеки підприємства, оскільки в аналіз інтегруються технічні, організаційні та кіберфактори. Гнучкість системи вагових коефіцієнтів забезпечує можливість адаптації моделі до динамічних змін середовища та появи нових типів загроз. Важливим результатом є можливість візуалізації оцінок у вигляді багатовимірних матриць ризиків, що істотно спрощує процес прийняття управлінських рішень і підвищує точність прогнозування. Разом з тим методика має певні обмеження, які необхідно враховувати при практичному застосуванні. Насамперед результати значною мірою залежать від якості вихідних даних: достовірності статистики інцидентів, повноти інформації щодо кіберзагроз та коректності формування показників. Для забезпечення об’єктивності оцінок виникає потреба у залученні експертів для встановлення та коригування вагових коефіцієнтів, що може зумовлювати певну суб’єктивність та потребує підготовку вимог та критеріїв професійних та етичних якостей, які висуваються до експертів. Додатковим викликом є масштабування методики для великих підприємств із різнорідними технологічними процесами, що ускладнює її практичне використання без попередньої адаптації, що особливо важливо для об’єктів підвищеної небезпеки, критичної інфраструктури, тощо.

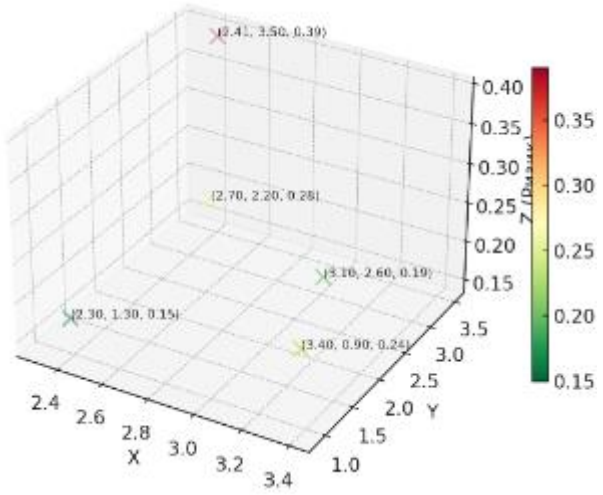

Рис. 2– Візуалізація 3D-матриці ризиків для базових загроз АЕС з урахуванням часу виявлення загрози *D*: X – ймовірність події (*P*); Y – вплив/наслідки небажаної події (*I*); Z – кіберкомпонент (*C*)
Fig. 2 – Visualization of the 3D risk matrix for basic NPP threats taking into account the threat detection time D: X – probability of an event (P); Y – impact/consequences of an undesirable event (I); Z – cyber component (C)

Table 4
Table of indicators with weights for the occurrence of an undesirable event (threat) at an energy enterprise
Таблиця 4
Таблиця показників з вагами настання небажаної події (загроз) на енергетичному підприємстві

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

Висновки

Сучасний розвиток інформаційних технологій дає можливості для розвитку та автоматизації складних систем та інфраструктур, та разом з тим постають питання та виклики щодо забезпечення безпеки з урахуванням можливих загроз небажаного втручання в роботу автоматизованих інформаційних систем, що необхідно враховувати при розробки стратегії управління підприємствами. Проведене дослідження дозволило сформувати науково обґрунтовану методику оцінювання рівня безпеки підприємства з урахуванням кіберзагроз, яка поєднує кваліметричні підходи та модифіковану систему вагових коефіцієнтів. У результаті було отримано інтегральну модель оцінювання ризиків, що забезпечує більш повне уявлення про стан захищеності об’єкта та дозволяє виявляти критичні вразливості ще на етапі планування заходів безпеки, або ж при прийнятті рішень в процесі функціонування. Практичне значення роботи полягає у можливості адаптації методики до специфіки атомно-енергетичного комплексу, де поєднання традиційних техногенних загроз і сучасних кіберризиків формує особливо високий рівень потенційної небезпеки. Так, в роботі розглянуто базові загрози для атомної електростанції, що дало можливість: виділити приховані уразливості – наприклад, відмова систем охолодження може бути не лише наслідком фізичної несправності, а й результатом маніпуляції програмним забезпеченням чи викривлення даних від датчиків, що було враховано при

оцінки ризику. Таким чином, застосування моделі демонструє, що реальна картина ризиків АЕС значною мірою змінюється за рахунок кіберкомпонента. У порівнянні з класичними оцінками, інтегральний рівень ризику підвищується на 10–25 %, що свідчить про необхідність системної інтеграції заходів кіберзахисту в загальну політику безпеки атомної енергетики.

Подальшим напрямом розвитку дослідження є застосування технологій штучного інтелекту для автоматизації оброблення великих масивів даних і побудови адаптивних систем управління ризиками. Використання алгоритмів машинного навчання дозволить не лише підвищити точність інтегральних оцінок, але й реалізувати прогнозування появи нових кіберзагроз, що наразі є одним із ключових викликів для систем критичної інфраструктури. Очікується, що розвиток цих підходів сприятиме створенню інтелектуальних систем моніторингу, які забезпечать проактивне реагування на ризики та підвищать стійкість підприємств у динамічному середовищі сучасних загроз

Конфлікт інтересів

Автори заявляють, що конфлікту інтересів щодо публікації рукопису немає. Крім того, автори повністю дотримувались етичних норм, включаючи плагіат, фальсифікацію даних та подвійну публікацію.

Список використаних джерел:

1. Khimicheva H. Mathematical model of an educational program quality assessment / H. Khimicheva, A. Volivach // Proceedings of National Aviation University. – 2020. – № *84*(3). – Pp. 71–79. DOI: https://doi.org/10.18372/2306-1472.84.14956
2. Грінченко Г. С., Мацько А. М. Інтеграція кваліметричних підходів у сучасні інформаційно-вимірювальні технології освіти. Машнобудування. 2024. Вип. 34 С. 39-50. DOI: https://doi.org/10.26565/2079-1747-2024-34-04
3. Кучерук В. Ю. Покращення якості рекомендаційних систем на основі кваліметричних методів вимірювання / В. Ю. Кучерук, М. В. Глушко // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2022. – № *2*. – С. 65–72. DOI: https://doi.org/10.31891/2219-9365-2022-70-2-9
4. Біловодська О. Кваліметричний підхід оцінювання стратегічної діяльності управління дистрибуцією інноваційних продуктів у маркетинговій логістиці / О. Біловодська // Економічний часопис Волинського національного університету імені Лесі Українки. – 2021. – № 1*(*25). – С. 175–183. DOI: https://doi.org/10.29038/2786-4618-2021-01-175-183
5. Qualimetric method of assessing risks of low quality products / Trishch R., Nechuiviter O., Dyadyura K., Vasilevskyi O., Tsykhanovska I., Yakovlev M. // MM Science Journal. – 2021. – № 10. – Pp. 4769–4774. DOI: https://doi.org/10.17973/MMSJ.2021_10_2021030
6. Assessment of the occupational health and safety management system by qualimetric methods / Trishch R., Cherniak O., Zdenek D., Petraskevicius V. // Engineering Management in Production and Services. – 2024. – № 16(2). – Pp. 118–127. DOI: https://doi.org/10.2478/emj-2024-0017
7. Assessment of safety risks using qualimetric methods / Trishch R., Nechuiviter O., Hrinchenko H., Bubela T., Riabchykov M., Pandova I. // MM Science Journal. – 2023. – № 10. – P. 6668. DOI: https://doi.org/10.17973/MMSJ.2023_10_2023021
8. Розвиток нормативного підходу до оцінювання ризиків енергопідприємств / Грінченко Г. С., Кіпоренко О. В., Негодов С. С., Лисенко А. Я., Мазорчук К. К., Нос Р. С. // Машинобудування: зб. наук. пр. / Укр. інж.-пед. акад. – Харків, 2024. – Вип. 34. – С. 17–30. DOI: https://doi.org/10.26565/2079-1747-2024-34-02
9. Peček B. Methodology of monitoring key risk indicators / Peček, B., & Kovačič, A. (2019).. Economic Research-Ekonomska Istraživanja. – 2019. – № *32*(1). – С. 3485–3501. DOI: https://doi.org/10.1080/1331677X.2019.1658529
10. Застосування методів кваліметрії для оцінки комплексних показників якості багатопараметричних об'єктів / П. Ф. Буданов та інші // Машинобудування: зб. наук. пр. / Укр. інж.-пед. акад. – Харків, – 2022. – Вип. 30. – С. 73–84. DOI: https://doi.org/10.32820/2079-1747-2022-30-73-84
11. Сороколат Н. А. Застосування функції помилок для оцінювання якості об’єктів кваліметрії / Н. А. Сороколат, Л. Ю. Фатєєва // Вісник НТУ «ХПІ». Серія: Нові рішення в сучасних технологіях. – 2022. – № *4*(14). – С. 53–58. DOI: https://doi.org/10.20998/2413-4295.2022.04.08

12. Ginevičius R. Quantitative assessment of quality management systems' processes / Ginevičius R., Trishch H., Petraškevičius V. // Economic Research-Ekonomska Istraživanja. – 2015. – № *28*(1). – Pp. 1096–1110. DOI: https://doi.org/10.1080/1331677X.2015.1087676
13. Risk assessment essentials guide for state energy security plans. Office of Cybersecurity, Energy Security, and Emergency Response. – 2024/ – Access mode: https://www.energy.gov/sites/default/files/2024-05/DOE%20CESER-Risk%20Assessment%20Essentials%20Guide%20for%20State%20Energy%20Security%20Plans.pdf (Last accessed October 28, 2025)
14. Quantitative and qualitative risk-informed energy investment for industrial companies / Urbano E. M., Martinez-Viol V., Kampouropoulos K., Romeral L. // Energy Reports. – 2023. – no 9. – Pp. 3290–3304. DOI: https://doi.org/10.1016/j.egyr.2023.01.131
15. Assessing qualitative and quantitative dimensions of uncertainty in energy modelling for policy support in the United Kingdom / Pye, S., Li, F. G. N., Petersen, A., Broad, O., McDowall, W., Price, J., Usher, W. // Energy Research & Social Science. – 2018. – № 46. – Pp. 332–344. DOI: https://doi.org/10.1016/j.erss.2018.07.028
16. Evaluating the strategies for sustainable energy planning in Pakistan: An integrated SWOT-AHP and Fuzzy-TOPSIS approach / Solangi, Y. A., Tan, Q., Mirjat, N. H., Ali, S. // Journal of Cleaner Production. – 2019. – № 236. – 117655. DOI: https://doi.org/10.1016/j.jclepro.2019.117655
17. The role of data analytics within operational risk management: A systematic review from the financial services and energy sectors / Cornwell, N., Bilson, C., Gepp, A., Stern, S., Vanstone, B. J. // Journal of the Operational Research Society. – 2022. – № 74*(1)*. – Pp. 374–402. DOI: https://doi.org/10.1080/01605682.2022.2041373
18. Gorzeń-Mitka I. Mapping the energy sector from a risk management research perspective: A bibliometric and scientific approach / I. Gorzeń-Mitka, M. Wieczorek-Kosmala // Energies. – 2023. – № 16*(4)*. DOI: https://doi.org/10.3390/en16042024
19. Creamer G. G. Volatility and risk in the energy market: A trade network approach / G. G. Creamer, T. Ben-Zvi // Sustainability. – 2021. – № 13*(*18). – 10199. DOI: https://doi.org/10.3390/su131810199
20. Kaka S. A comprehensive analysis of factors influencing biogas plant location / Kaka S., Memon M., Mari S. // Proceedings of the 9th North American Conference on Industrial Engineering and Operations Management. – 2024. – DOI: https://doi.org/10.46254/NA09.20240143
21. Irfan M. Consumers' intention-based influence factors of renewable energy adoption in Pakistan: A structural equation modeling approach / Irfan M., Zhao Z. Y., Rehman A. // Environmental Science and Pollution Research. – 2021. – № 28. – Pp. 432–445. DOI: https://doi.org/10.1007/s11356-020-10504-w
22. Research on TBM parameter optimization based on failure probability / Zhang Q., Nie Y., Zhao W., Du L. // Engineering Failure Analysis. – 2025. – № *167*(B). – 109036. DOI: https://doi.org/10.1016/j.engfailanal.2024.109036
23. Ikwan F. Safety evaluation of leak in a storage tank using fault tree analysis and risk matrix analysis / F. Ikwan, D. Sanders, M. Hassan // Journal of Loss Prevention in the Process Industries. – 2021. – № *73*. – 104597. DOI: https://doi.org/10.1016/j.jlp.2021.104597
24. Proactive approaches of dynamic risk assessment based on indicators / Paltrinieri N., Landucci G., Nelson W. R., Hauge S. // Dynamic risk analysis in the chemical and petroleum industry / eds. N. Paltrinieri, F. Khan. – Butterworth-Heinemann, 2016. – Pp. 63-73. DOI: https://doi.org/10.1016/B978-0-12-803765-2.00006-8
25. Gorzeń-Mitka I. Mapping the energy sector from a risk management research perspective: A bibliometric and scientific approach / I. Gorzeń-Mitka, M. Wieczorek-Kosmala // Energies. – 2024. – № *16*(4). DOI: https://doi.org/10.3390/en16042024
26. Zhu X. Application of multiple criteria decision making methods in construction: A systematic literature review / Zhu X., Meng X., Zhang M. // Journal of Civil Engineering and Management. – 2021. – № 27*(*6). Pp. 372–403. DOI: https://doi.org/10.3846/jcem.2021.15260
27. A survey on power system blackout and cascading events: Research motivations and challenges / Haes Alhelou H., Hamedani-Golshan M. E., Njenda T. C., Siano P. // Energies. – 2019. – № 12(4). – Pp. 682. DOI: https://doi.org/10.3390/en12040682
28. Le Coq C. Measuring the security of external energy supply in the European Union / C. Le Coq, H. Paltseva // Energy Policy. – 2009. – № 37*(*11). – Pp. 4474–4481. DOI: https://doi.org/10.1016/j.enpol.2009.05.069
29. ISO 31000:2018 Risk management – Guidelines : (2nd ed.) / International Organization for Standardization. – Access mode : https://www.iso.org/standard/31000 (Last accessed October 28, 2025)

30. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements : (3rd ed.) / International Organization for Standardization. – 2022. – Access mode : https://www.iso.org/standard/27001 (Last accessed October 28, 2025)

31. Guide to industrial control systems (ICS) security / Stouffer K., Lightman S., Pillitteri V., Abrams M., Hahn A. // (NIST Special Publication 800-82 Rev. 2) / National Institute of Standards and Technology. – 2015. DOI: https://doi.org/10.6028/NIST.SP.800-82r2
32. Hussain M. A. A survey on malware attacks in industrial air-gap systems / Hussain M. A., Samrouth K., Bakir N. // International Journal of Information Security. – 2025. – № 24. – P. 146. DOI: https://doi.org/10.1007/s10207-025-01044-w
33. A dynamic spatiotemporal deep learning solution for cloud–edge collaborative industrial control system distributed denial of service attack detection / Cao Z., Liu B., Gao D., Zhou D., Han X., Cao J. // Electronics. – 2025. – № 14. – P. 1843. DOI: https://doi.org/10.3390/electronics14091843
34. NIST roadmap for improving critical infrastructure cybersecurity / National Institute of Standards and Technology. – 2014. – Access mode : http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf (Last accessed October 28, 2025)
35. Communication from the Commission on a European Programme for Critical Infrastructure Protection (COM(2006) 786 final) / European Commission. – Brussels, 2006. – Access mode : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52006DC0786 (Last accessed October 28, 2025)
36. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank: A framework strategy for a resilient energy union with a forward-looking climate change policy (COM(2015) 80 final) / European Commission. – Brussels, 2015. – Access mode : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015DC0080 (Last accessed October 28, 2025)
37. Torregosa, R. F., & Hu, W. (2013). Probabilistic risk analysis of fracture of aircraft structures using a Bayesian approach to update the distribution of the equivalent initial flaw sizes. *Fatigue & Fracture of Engineering Materials & Structures, 36,* 1092–1101. DOI: https://doi.org/10.1111/ffe.12103
38. A simheuristic for project portfolio optimization combining individual project risk, scheduling effects, interruptions, and project risk correlations / Saiz M., Calvet L., Juan A. A., Lopez-Lopez D. // Computers & Industrial Engineering. – 2024. – № 198. – 110694. DOI: https://doi.org/10.1016/j.cie.2024.110694
39. Chu C. Dynamic fault tree generation and quantitative analysis of system reliability for embedded systems based on SysML models / Chu C., Yang W., Chen Y. // Sensors. – 2024. – № 24. – P. 6021. DOI: https://doi.org/10.3390/s24186021
40. Markulik Š. Use of risk management to support business sustainability in the automotive industry / Markulik Š., Šolc M., Blaško P. // Sustainability. – 2024. – № 16. – P. 4308. DOI: https://doi.org/10.3390/su16104308
41. Karanikas N. Redefining health, risk, and safety for occupational settings: A mixed-methods study / N. Karanikas, H. Zerguine // Safety Science. – 2025. – № 181. – 106698. DOI: https://doi.org/10.1016/j.ssci.2024.106698

Отримано: 22.09.2025 Прийнято: 28.10.2025 Опубліковано: 30.12.2025

[1]LYSENKO A.,
Postgraduate student of the Department of Automation, Metrology and Energy Efficient Technologies
e-mail: dagost@ukr.net ORCID: https://orcid.org/0009-0007-3916-8029
[1]NOS R.,
Postgraduate student of the Department of Automation, Metrology and Energy Efficient Technologies
e-mail: nosruslan@gmail.com ORCID: https://orcid.org/0009-0006-5391-7703
[1]MAZORCHUK K.,
Postgraduate student of the Department of Automation, Metrology and Energy Efficient Technologies
e-mail: ekaterina.mazorchuk@gmail.com ORCID: https://orcid.org/0009-0001-0769-4872
[1]NEHODOV S.,
Postgraduate student of the Department of Automation, Metrology and Energy Efficient Technologies
e-mail: titansv2017@gmail.com ORCID: https://orcid.org/0000-0003-3561-6924
[1]V. N. Karazin Kharkiv National University
Svobody square, 4, Kharkiv, 61022, Ukraine

IMPROVING QUALIMETRIC APPROACHES TO RISK ASSESSMENT OF ENERGY COMPANIES TAKING INTO ACCOUNT CYBERSECURITY ASPECTS

The article considers the possibility of applying qualimetric approaches to risk assessment, taking into account modern aspects of cyber threats arising in energy enterprises. For the purpose of risk assessment and management, the scientific, technical and regulatory framework was analysed and an algorithmic scheme was proposed that takes into account the cyber component, which is both a separate threat to the functioning of an energy enterprise and can influence other threats of various nature, and as a result increase the overall risk level. In the course of the study, a scientifically based methodology for assessing the level of enterprise security, taking into account cyber threats, was developed. The proposed approach combines qualimetric methods and a modified system of weighting coefficients, which made it possible to form an integrated risk analysis model that provides a more comprehensive view of the state of security of the and enables the timely detection of critical vulnerabilities both at the stage of planning security measures and during the adoption of management decisions in the course of operations. The study analysed the basic threats to a nuclear power plant, which made it possible to identify hidden threats, namely, it was established that the failure of cooling systems can be caused not only by physical malfunctions, but also by deliberate interference with software or distortion of sensor signals, which is taken into account when assessing risks. The paper presents a visualisation of risk assessment in the form of a 3D risk matrix with a cyber component, which provides a better understanding and helps energy company managers quickly identify the most critical risks in which the cyber factor significantly increases the threat. The application of the integrated model has shown that the actual level of risk at a nuclear power plant increases significantly due to the cyber component. Compared to the baseline assessment, the integrated risk indicator, taking into account the cyber component, increases by 10–25%, confirming the need for the systematic inclusion of cyber protection measures in the overall nuclear energy security policy.

KEYWORDS: risk, qualimetric approach, energy companies, cyber threats, assessment, risk matrices

In cites: Lysenko A., Nos R., Mazorchuk K., Nehodov S. (2025), Improving qualimetric approaches to risk assessment of energy companies taking into account cybersecurity aspects. *Engineering, (36),* 102-118. https://doi.org/10.26565/2079-1747-2025-36-10 (in Ukraine)

Conflict of interest

The authors declare that there is no conflict of interest regarding the publication of the manuscript. In addition, the authors fully complied with ethical standards, including plagiarism, data falsification, and double publication.

References

1. Khimicheva, H & Volivach, A 2020, 'Mathematical model of an educational program quality assessment', *Proceedings of National Aviation University, 84*(3), Pp. 71–79. DOI: https://doi.org/10.18372/2306-1472.84.14956
2. Hrinchenko, H. S. & Matsko, A. M. (2024). Integration of qualimetric approaches into modern educational information measurement technologies. Engineering, (34), 39-50. https://doi.org/10.26565/2079-1747-2024-34-04 (in Ukraine)
3. Kucheruk, VYu & Hlushko, MV 2022, 'Improving the quality of recommender systems based on qualimetric measurement methods.', *Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh,* no 2, Pp. 65–72, DOI: https://doi.org/10.31891/2219-9365-2022-70-2-9
4. Bilovodska, O 2021, 'Qualimetric approach to evaluating strategic activities of distribution management of innovative products in marketing logistics', *Ekonomichnyi chasopys Volynskoho natsionalnoho universytetu imeni Lesi Ukrainky*, no 1(25), Pp. 175–183, DOI: https://doi.org/10.29038/2786-4618-2021-01-175-183
5. Trishch, R, Nechuiviter, O, Dyadyura, K, Vasilevskyi, O, Tsykhanovska, I & Yakovlev, M 2021, 'Qualimetric method of assessing risks of low quality products', *MM Science Journal,* no (10), Pp. 4769–4774, DOI: https://doi.org/10.17973/MMSJ.2021_10_2021030
6. Trishch, R, Cherniak, O, Zdenek, D & Petraskevicius, V 2024, 'Assessment of the occupational health and safety management system by qualimetric methods', *Engineering Management in Production and Services*, no 16*(*2), Pp. 118–127, DOI: https://doi.org/10.2478/emj-2024-0017
7. Trishch, R, Nechuiviter, O, Hrinchenko, H, Bubela, T, Riabchykov, M & Pandova, I 2023, 'Assessment of safety risks using qualimetric methods', *MM Science Journal,* no (10), P. 6668, DOI: https://doi.org/10.17973/MMSJ.2023_10_2023021
8. Hrinchenko, HS, Kiporenko, OV, Nehodov, SS, Lysenko, AYa, Mazorchuk, KK & Nos, RS 2024, 'Development of a regulatory approach to assessing the risks of energy enterprises', *Mashynobuduvannia*, Iss. 34, Pp. 17–30, DOI: https://doi.org/10.26565/2079-1747-2024-34-02
9. Peček, B & Kovačič, A 2019, 'Methodology of monitoring key risk indicators', *Economic Research-Ekonomska Istraživanja*, no 32*(1*), Pp. 3485–3501, DOI: https://doi.org/10.1080/1331677X.2019.1658529
10. Budanov, PF, Hrinchenko, HS, Nechuiviter, OP, Boiko, TH & Tsykhanovska, IV 2022, 'Application of qualimetry methods to assess complex quality indicators of multiparametric lenses', *Mashynobuduvannia*, Iss. 30, Pp. 73–84, DOI: https://doi.org/10.32820/2079-1747-2022-30-73-84
11. Sorokolat, NA & Fatieieva, LYu 2022, 'Application of the error function to assess the quality of quality objects', *Visnyk NTU «KhPI». Seriia: Novi rishennia v suchasnykh tekhnolohiiakh*, no 4(14), Pp. 53–58. DOI: https://doi.org/10.20998/2413-4295.2022.04.08
12. Ginevičius, R, Trishch, H & Petraškevičius, V 2015, 'Quantitative assessment of quality management systems' processes', *Economic Research-Ekonomska Istraživanja*, no 28(1), Pp. 1096–1110, DOI: https://doi.org/10.1080/1331677X.2015.1087676
13. U.S. Department of Energy 2024, *Risk assessment essentials guide for state energy security plans*. Office of Cybersecurity, Energy Security, and Emergency Response, viewed <https://www.energy.gov/sites/default/files/2024-05/DOE%20CESER-Risk%20Assessment%20Essentials%20Guide%20for%20State%20Energy%20Security%20Plans.pdf >
14. Urbano, EM, Martinez-Viol, V, Kampouropoulos, K & Romeral, L 2023, 'Quantitative and qualitative risk-informed energy investment for industrial companies', *Energy Reports*, no 9, Pp. 3290–3304, DOI: https://doi.org/10.1016/j.egyr.2023.01.131
15. Pye, S, Li, FGN, Petersen, A, Broad, O, McDowall, W, Price, J & Usher, W 2018, 'Assessing qualitative and quantitative dimensions of uncertainty in energy modelling for policy support in the United Kingdom', *Energy Research & Social Science,* no 46, Pp. 332–344, DOI: https://doi.org/10.1016/j.erss.2018.07.028
16. Solangi, YA, Tan, Q, Mirjat, NH & Ali, S 2019, 'Evaluating the strategies for sustainable energy planning in Pakistan: An integrated SWOT-AHP and Fuzzy-TOPSIS approach', *Journal of Cleaner Production*, no 236*,* 117655, DOI: https://doi.org/10.1016/j.jclepro.2019.117655

17. Cornwell, N, Bilson, C, Gepp, A, Stern, S & Vanstone, BJ 2022, 'The role of data analytics within operational risk management: A systematic review from the financial services and energy sectors', *Journal of the Operational Research Society*, no 74(1), Pp. 374–402, DOI: https://doi.org/10.1080/01605682.2022.2041373
18. Gorzeń-Mitka, I & Wieczorek-Kosmala, M 2023, 'Mapping the energy sector from a risk management research perspective: A bibliometric and scientific approach', *Energies*, no 16*(4),* DOI: https://doi.org/10.3390/en16042024
19. Creamer, GG & Ben-Zvi, T 2021, 'Volatility and risk in the energy market: A trade network approach', *Sustainability*, no 13(18), 10199, DOI: https://doi.org/10.3390/su131810199
20. Kaka, S, Memon, M & Mari, S 2024, 'A comprehensive analysis of factors influencing biogas plant location', *Proceedings of the 9th North American Conference on Industrial Engineering and Operations Management,* DOI: https://doi.org/10.46254/NA09.20240143
21. Irfan, M, Zhao, ZY & Rehman, A 2021, 'Consumers' intention-based influence factors of renewable energy adoption in Pakistan: A structural equation modeling approach', *Environmental Science and Pollution Research*, no 28*,* Pp. 432–445, DOI: https://doi.org/10.1007/s11356-020-10504-w
22. Zhang, Q, Nie, Y, Zhao, W & Du, L 2025, 'Research on TBM parameter optimization based on failure probability', *Engineering Failure Analysis*, no 167*(*B), 109036, DOI: https://doi.org/10.1016/j.engfailanal.2024.109036
23. Ikwan, F, Sanders, D & Hassan, M 2021, 'Safety evaluation of leak in a storage tank using fault tree analysis and risk matrix analysis', *Journal of Loss Prevention in the Process Industries*, no 73*,* 104597, DOI: https://doi.org/10.1016/j.jlp.2021.104597
24. Paltrinieri, N, Landucci, G, Nelson, WR & Hauge, S 2016, 'Proactive approaches of dynamic risk assessment based on indicators', In N. Paltrinieri & F. Khan (Eds.), *Dynamic risk analysis in the chemical and petroleum industry,* Butterworth-Heinemann, Pp. 63-73, DOI: https://doi.org/10.1016/B978-0-12-803765-2.00006-8
25. Gorzeń-Mitka, I & Wieczorek-Kosmala, M 2023, 'Mapping the energy sector from a risk management research perspective: A bibliometric and scientific approach', *Energies*, no 16*(4*), DOI: https://doi.org/10.3390/en16042024
26. Zhu, X, Meng, X & Zhang, M 2021, 'Application of multiple criteria decision making methods in construction: A systematic literature review', *Journal of Civil Engineering and Management*, no 27*(6*), Pp. 372–403. DOI: https://doi.org/10.3846/jcem.2021.15260
27. Haes Alhelou, H, Hamedani-Golshan, ME, Njenda, TC & Siano, P 2019, 'A survey on power system blackout and cascading events: Research motivations and challenges', *Energies*, no 12*(4*), P. 682. DOI: https://doi.org/10.3390/en12040682
28. Le Coq, C & Paltseva, E 2009, 'Measuring the security of external energy supply in the European Union', *Energy Policy*, no 37(11), Pp. 4474–4481, DOI: https://doi.org/10.1016/j.enpol.2009.05.069
29. International Organization for Standardization 2018, *ISO 31000:2018 Risk management – Guidelines* (2nd ed.), viewed <https://www.iso.org/standard/31000>
30. International Organization for Standardization 2022, *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements* (3rd ed.), viewed <https://www.iso.org/standard/27001>
31. Stouffer, K, Lightman, S, Pillitteri, V, Abrams, M & Hahn, A 2015, *Guide to industrial control systems (ICS) security* (NIST Special Publication 800-82 Rev. 2), DOI: https://doi.org/10.6028/NIST.SP.800-82r2
32. Hussain, MA, Samrouth, K & Bakir, N 2025, 'A survey on malware attacks in industrial air-gap systems', *International Journal of Information Security*, no 24, P. 146, DOI: https://doi.org/10.1007/s10207-025-01044-w
33. Cao, Z, Liu, B, Gao, D, Zhou, D, Han, X & Cao, J 2025, 'A dynamic spatiotemporal deep learning solution for cloud–edge collaborative industrial control system distributed denial of service attack detection', *Electronics,* no 14*,* P. 1843. DOI: https://doi.org/10.3390/electronics14091843
34. National Institute of Standards and Technology 2014, *NIST roadmap for improving critical infrastructure cybersecurity,* viewed <http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf>

35. European Commission 2006, *Communication from the Commission on a European Programme for Critical Infrastructure Protection* (COM(2006) 786 final), Brussels, viewed <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52006DC0786>
36. European Commission 2015, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank: A framework strategy for a resilient energy union with a forward-looking climate change policy* (COM(2015) 80 final), Brussels, viewed <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015DC0080>
37. Torregosa, RF & Hu, W 2013, 'Probabilistic risk analysis of fracture of aircraft structures using a Bayesian approach to update the distribution of the equivalent initial flaw sizes', *Fatigue & Fracture of Engineering Materials & Structures,* no 36, Pp. 1092–1101. DOI: https://doi.org/10.1111/ffe.12103
38. Saiz, M, Calvet, L, Juan, A. A & Lopez-Lopez, D 2024, 'A simheuristic for project portfolio optimization combining individual project risk, scheduling effects, interruptions, and project risk correlations', *Computers & Industrial Engineering,* no 198, 110694. DOI: https://doi.org/10.1016/j.cie.2024.110694
39. Chu, C, Yang, W & Chen, Y 2024, 'Dynamic fault tree generation and quantitative analysis of system reliability for embedded systems based on SysML models', *Sensors,* no 24, 6021. DOI: https://doi.org/10.3390/s24186021
40. Markulik, Š, Šolc, M & Blaško, P 2024, 'Use of risk management to support business sustainability in the automotive industry', *Sustainability,* no 16, 4308. DOI: https://doi.org/10.3390/su16104308
41. Karanikas, N & Zerguine, H 2025, 'Redefining health, risk, and safety for occupational settings: A mixed-methods study', *Safety Science,* no 181, 106698. DOI: https://doi.org/10.1016/j.ssci.2024.106698

Submission received: 09/22/2025 Accepted: 10/28/2025 Published: 12/30/2025