Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА

Кіберфізична система управління системами енергозабезпечення центрів комутації телекомунікаційних мереж
Назва теми

Рівень вищої освіти *другий (магістерський)*

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *123 «Комп'ютерна інженерія»*
Шифр, назва

Освітня програма *«Комп'ютерна інженерія та програмування»*
Назва

Шифр КвРКІ 240106.24.01.05 ПЗ

Виконав здобувач II курсу, група КІ2м-24-1 _____ Олександр ВАСЬКОВ
Підпис Ініціали, прізвище

Керівник канд.-техн. наук, доцент _____ Олексій ІВАНОВ
Науковий ступінь, учене звання Підпис Ініціали, прізвище

Нормоконтролер д. техн. наук, професор _____ Сергій ЛИСЕНКО
Науковий ступінь, учене звання Підпис Ініціали, прізвище

_____ Ольга ПАВЛОВА
Підпис Ініціали, прізвище

До захисту допускаю:
завідувач кафедри КІІС
«01» _травня_ 2026 р.
дата

Хмельницький 2026

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Рівень вищої освіти ДРУГИЙ (МАГІСТЕРСЬКИЙ)

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА ПРОГРАМУВАННЯ»

ЗАТВЕРДЖУЮ
Завідувачка кафедри КІІС
_____ Ольга ПАВЛОВА

" 12 " 01 2026 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Васькову Олександру Вікторовичу
Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Кіберфізична система управління системами енергозабезпечення центрів комутації телекомунікаційних мереж
Керівник проекту (роботи) Іванов Олексій Валентинович, к.т.н., доцент.
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 12.01.2026 р. № 6

2. Термін подання здобувачем роботи на кафедру 01.05.2026 р.

3. Вихідні дані до роботи Завдання на кваліфікаційну роботу

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Аналіз відомих моделей, методів та засобів управління енергозабезпеченням телекомунікаційних об'єктів на основі кіберфізичних систем
Розроблення концепції та структурно-функціональної моделі кіберфізичної системи управління енергозабезпеченням центрів комутації
Розроблення методу адаптивного управління енергозабезпеченням з предиктивною оцінкою технічного стану
Розроблення алгоритмів та проєктування програмного забезпечення кіберфізичної системи
Програмна реалізація прототипу та дослідження ефективності розробленого методу

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень) _____

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийня

7. Дата видачі завдання «_12_»_____01_____2026 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи магістра	Термін виконання етапів проекту (роботи)	Примітк
1	Вибір напряму дослідження та узгодження тематики КвРМ з керівником	12.01.2026	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	15.01.2026	виконан
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	01.02.2026	виконан
4	Робота над розділом 2 – розробка моделей для вирішення поставленої задачі	01.03.2026	виконан
5	Робота над науковою статтею	05.03.2026	виконан
6	Робота над розділом 3 – розробка методів для вирішення поставленої задачі	20.03.2026	виконан
7	Робота над розділом 4 – проєктування та розробка ПЗ для вирішення поставленої задачі, експериментальна частина	01.04.206	виконан
8	Оформлення пояснювальної записки згідно вимог	18.04.2026	виконан
9	Попередній захист ДРМ	29.04.2026	виконан
10	Захист ДРМ на засіданні ЕК	травень 2026 року	

Здобувач_____ ___Олександр ВАСЬКОВ___
Підпис Ім'я, ПРІЗВИЩЕ

Керівник кваліфікаційної роботи_____ ___Олексій ІВАНОВ___
Підпис Ім'я, ПРІЗВИЩЕ

РЕФЕРАТ

Тема кваліфікаційної роботи магістра: «Кіберфізична система управління системами енергозабезпечення центрів комутації телекомунікаційних мереж».

Автор роботи: Васьков Олександр Вікторович.

Керівник роботи: Іванов Олексій Валентинович, к.т.н., доцент.

Пояснювальна записка: 86 с., 12 рис., 15 табл., 4 додатки, 80 джерел.

КІБЕРФІЗИЧНА СИСТЕМА, ЕНЕРГОЗАБЕЗПЕЧЕННЯ, ЦЕНТР КОМУТАЦІЇ, ТЕЛЕКОМУНІКАЦІЙНА МЕРЕЖА, СИСТЕМА БЕЗПЕРЕБІЙНОГО ЖИВЛЕННЯ, ПРЕДИКТИВНА АНАЛІТИКА, MQTT, MODBUS, IOT, ТЕЛЕМЕТРІЯ.

Об'єктом дослідження є процес управління системами енергозабезпечення центрів комутації телекомунікаційних мереж в умовах впровадження кіберфізичних технологій.

Предметом дослідження є моделі, методи та програмні засоби побудови кіберфізичної системи управління, що забезпечують підвищення надійності та ефективності функціонування систем електроживлення телекомунікаційного обладнання.

Метою кваліфікаційної роботи магістра є підвищення надійності, спостережуваності та енергоефективності систем енергозабезпечення центрів комутації телекомунікаційних мереж шляхом створення кіберфізичної системи управління, яка інтегрує телеметрію, предиктивну аналітику стану обладнання та сценарне автоматизоване реагування на аварійні події.

Для розв'язання поставлених задач використовувалися: системний аналіз, теорія кіберфізичних систем, методи математичного моделювання, методи теорії множин, теорія автоматичного управління, методи оцінювання надійності та живучості, методи об'єктно-орієнтованого проєктування програмного забезпечення.

Наукова новизна отриманих результатів:

1. Удосконалено метод управління системами енергозабезпечення центрів комутації телекомунікаційних мереж за рахунок інтеграції предиктивної оцінки технічного стану обладнання, моделі ієрархічного подієво-станового керування та

сценарного реагування, що, на відміну від відомих рішень, дозволяє забезпечити перехід від реактивного до проактивного режиму експлуатації енергетичної інфраструктури.

2. Набули подальшого розвитку програмні засоби кіберфізичного управління енергозабезпеченням за рахунок реалізації уніфікованого шару абстракції даних поверх гетерогенних телеметричних протоколів (Modbus, MQTT, SNMP), що дозволяє інтегрувати в єдиний контур керування обладнання різних виробників та поколінь.

Практична цінність отриманих результатів. У роботі розроблено програмні засоби кіберфізичної системи управління енергозабезпеченням, які дозволяють підвищити доступність та надійність роботи телекомунікаційного обладнання, скоротити час виявлення й локалізації відмов, забезпечити прогнозування часу автономної роботи критичних сервісів. Результати роботи можуть бути впроваджені на майданчиках операторів зв'язку та центрів обробки даних різного масштабу.

Апробація результатів. За темою кваліфікаційної роботи магістра опубліковано тези доповіді на VII Міжнародній науково-практичній конференції Таврійського національного університету імені В. І. Вернадського.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

АВР – автоматичне ввімкнення резерву;

АКБ – акумуляторна батарея;

БД – база даних;

ДБЖ – джерело безперебійного живлення;

ДГУ – дизель-генераторна установка;

ЕОМ – електронно-обчислювальна машина;

ЛОМ – локальна обчислювальна мережа;

ОС – операційна система;

ПЗ – програмне забезпечення;

ЦКТМ – центр комутації телекомунікаційної мережі;

BMS – Battery Management System (система управління акумуляторами);

CPS – Cyber-Physical System (кіберфізична система);

DCIM – Data Center Infrastructure Management;

EMS – Energy Management System (система управління енергією);

HMI – Human-Machine Interface (людино-машинний інтерфейс);

IoT – Internet of Things (Інтернет речей);

LiFePO4 – літій-залізо-фосфатний акумулятор;

MQTT – Message Queuing Telemetry Transport;

OPC UA – Open Platform Communications Unified Architecture;

PDU – Power Distribution Unit (блок розподілу живлення);

PLC – Programmable Logic Controller (програмований логічний контролер);

REST – Representational State Transfer;

RTU – Remote Terminal Unit (віддалений термінал);

SCADA – Supervisory Control and Data Acquisition;

SNMP – Simple Network Management Protocol;

SoC – State of Charge (рівень заряду);

SoH – State of Health (стан здоров'я акумулятора);

UPS – Uninterruptible Power Supply (джерело безперебійного живлення).

ВСТУП

Сучасний етап розвитку інформаційного суспільства характеризується стрімким зростанням обсягів даних, що циркулюють у телекомунікаційних мережах, підвищенням вимог до надійності та безперебійності їх функціонування. Центри комутації телекомунікаційних мереж є критично важливими об'єктами інфраструктури, від стану яких безпосередньо залежить якість зв'язку та рівень надання цифрових послуг. Забезпечення їх стабільної роботи неможливе без ефективного управління системами енергозабезпечення, що набуває особливого значення в умовах воєнного стану та нестабільності мережі електропостачання [1].

Аналіз української та зарубіжної науково-технічної літератури показав, що до сьогодні розв'язано низку важливих задач у галузі управління електроживленням телекомунікаційних об'єктів. Зокрема, запропоновано численні архітектурні рішення для побудови систем безперебійного живлення, розроблено стандарти інтерфейсів телекомунікаційного обладнання (ETSI EN 300 132, ITU-T L.1200), сформульовано вимоги до структури датацентрів та центрів комутації (EN 50600), напрацьовано рекомендації з кіберзахисту систем промислової автоматики (NIST SP 800-82, ISA/IEC 62443) [5, 22, 23, 28]. Розроблено низку програмних платформ типу BMS, DCIM, SCADA для моніторингу та диспетчеризації енергетичного обладнання.

Однак ще існує достатньо задач у галузі управління енергозабезпеченням ЦКТМ, на розв'язання яких спрямовані зусилля науковців та інженерів. Зокрема, слід відзначити такі задачі: інтеграція гетерогенних джерел телеметрії в єдиний інформаційний простір; перехід від реактивного до проактивного режиму експлуатації; побудова достовірної моделі технічного стану акумуляторного контуру; координація енергетичного та кліматичного контурів керування; забезпечення кіберстійкості систем управління критичної інфраструктури зв'язку.

Над цими задачами працюють провідні науковці, серед яких Е. А. Лі, Е. Гріффор, Дж. Стіпановітс (Sztipanovits) – у галузі формалізації кіберфізичних систем; К. Стауффер, В. Піллітері – у галузі безпеки промислових систем

керування; Л. Б. Ліщинська, Ю. Д. Катков – у галузі інтелектуального управління електроживленням телекомунікаційних об'єктів. Ними розроблено фундаментальні архітектурні принципи кіберфізичних систем, методи побудови розподілених систем збору телеметрії, основи аналізу ризиків та захисту систем технологічного управління [21–23, 42–44].

На сьогодні світові тенденції розвитку галузі пов'язані з розв'язанням таких задач: цифрова трансформація енергетичної інфраструктури критичних об'єктів; впровадження принципів автономних мереж (Autonomous Networks) [40]; інтеграція відновлюваних джерел та накопичувачів енергії в систему резервного живлення телекомунікаційних об'єктів; застосування edge-обчислень та предиктивної аналітики для раннього виявлення деградації обладнання [35–37, 45].

Актуальність роботи полягає у необхідності розроблення кіберфізичної системи управління енергозабезпеченням центрів комутації телекомунікаційних мереж, яка забезпечить інтегрований моніторинг гетерогенного енергетичного обладнання, підтримку предиктивної аналітики стану акумуляторного, випрямного й генераторного контурів, скоординоване реагування енергетичного та кліматичного контурів управління, а також виконання вимог кібербезпеки для систем критичної інфраструктури.

Метою кваліфікаційної роботи магістра є підвищення надійності, спостережуваності та енергоефективності систем енергозабезпечення центрів комутації телекомунікаційних мереж шляхом створення кіберфізичної системи управління, яка на основі інтегрованої телеметрії, моделей технічного стану та сценарного реагування забезпечує проактивний контроль критичної енергетичної інфраструктури.

Поставлена мета досягається розв'язанням таких основних задач:

− провести аналіз відомих моделей, методів та програмно-технічних засобів управління енергозабезпеченням телекомунікаційних об'єктів, виявити обмеження існуючих рішень;

− розробити концепцію та структурно-функціональну модель кіберфізичної системи управління енергозабезпеченням ЦКТМ;

− розробити інформаційну модель об'єкта та модель технічного стану елементів енергетичної інфраструктури;

− розробити метод адаптивного управління енергозабезпеченням з підтримкою предиктивної оцінки стану та сценарного реагування;

− розробити алгоритми та архітектурне проєктування програмного забезпечення кіберфізичної системи;

− реалізувати програмні засоби кіберфізичної системи та провести експериментальні дослідження їхньої ефективності.

Об'єктом дослідження є процеси управління системами енергозабезпечення центрів комутації телекомунікаційних мереж в умовах впровадження кіберфізичних технологій.

Предметом дослідження є моделі, методи та програмні засоби побудови кіберфізичної системи управління, що забезпечують підвищення надійності та ефективності функціонування систем електроживлення телекомунікаційного обладнання.

Для розв'язання поставлених задач використано основні положення системного аналізу, теорії кіберфізичних систем, методи математичного моделювання, методи теорії множин для побудови інформаційної моделі об'єкта, теорію автоматичного управління для розроблення сценаріїв реагування, методи оцінювання надійності та живучості складних технічних систем, принципи об'єктно-орієнтованого проєктування програмного забезпечення, експериментальні методи для оцінки ефективності розробленого методу.

Наукова новизна отриманих результатів полягає в тому, що по-перше, удосконалено метод управління системами енергозабезпечення ЦКТМ за рахунок інтеграції предиктивної оцінки технічного стану обладнання, моделі ієрархічного подієво-станового керування та сценарного реагування, що, на відміну від відомих рішень, дозволяє забезпечити перехід від реактивного до проактивного режиму експлуатації енергетичної інфраструктури. По-друге, набули подальшого розвитку програмні засоби кіберфізичного управління за рахунок реалізації уніфікованого шару абстракції даних поверх гетерогенних телеметричних протоколів (Modbus,

MQTT, SNMP), що дає змогу інтегрувати в єдиний контур керування обладнання різних виробників та поколінь.

Практичне значення отриманих результатів полягає у можливості їх використання при розробленні архітектури кіберфізичної системи управління енергозабезпеченням для реальних об'єктів телекомунікаційної інфраструктури, а також при формуванні рекомендацій щодо підвищення енергоефективності та надійності центрів комутації. Розроблений прототип програмного забезпечення придатний до поетапного впровадження на існуючих майданчиках операторів зв'язку без повного припинення сервісів.

Виконана кваліфікаційна робота магістра має взаємозв'язок з такими науковими напрямками: побудова кіберфізичних та інтелектуальних систем управління технічними об'єктами; розроблення розподілених систем збору й обробки телеметрії на базі IoT-технологій; забезпечення кібербезпеки систем критичної інфраструктури; підвищення енергоефективності телекомунікаційного обладнання.

За темою кваліфікаційної роботи магістра опубліковано наукову статтю у фаховому виданні «Вісник Хмельницького національного університету. Технічні науки», а також тези доповіді на Всеукраїнській науково-технічній конференції молодих вчених, аспірантів та студентів «Інтелектуальні комп'ютерні системи та мережі», Хмельницький, 2026.

Кваліфікаційна робота магістра складається зі вступу, чотирьох розділів, висновків, переліку посилань та двох додатків. У першому розділі проведено аналіз сучасного стану галузі управління енергозабезпеченням телекомунікаційних об'єктів, класифіковано існуючі моделі, методи та програмно-технічні засоби, виявлено їх обмеження та сформульовано постановку задачі. У другому розділі розроблено концепцію, структурно-функціональну та інформаційну моделі кіберфізичної системи, а також метод адаптивного управління енергозабезпеченням. У третьому розділі розроблено алгоритм роботи системи, вимоги до програмного забезпечення, архітектуру та проєктування підсистеми збору телеметрії. У четвертому розділі виконано програмну реалізацію

кіберфізичної системи, проведено експериментальні дослідження та оцінено ефективність розроблених моделі та методу. Загальний обсяг роботи становить 86 сторінок основного тексту; робота містить 14 рисунків, 9 таблиць, 2 додатки та 47 джерел за переліком посилань.

1 АНАЛІЗ ВІДОМИХ МОДЕЛЕЙ, МЕТОДІВ ТА ЗАСОБІВ КІБЕРФІЗИЧНИХ СИСТЕМ УПРАВЛІННЯ ЕНЕРГОЗАБЕЗПЕЧЕННЯМ ТЕЛЕКОМУНІКАЦІЙНИХ ОБ'ЄКТІВ

1.1 Аналіз відомих моделей кіберфізичних систем у сфері управління енергозабезпеченням

Кіберфізична система управління системами енергозабезпечення центрів комутації телекомунікаційних мереж належить до класу критично важливих інфраструктурних систем, у яких цифрові засоби спостереження, аналізу та керування безпосередньо впливають на фізичні процеси перетворення, розподілу та резервування електричної енергії [22]. На відміну від побутових або локальних систем автоматизації, об'єктом керування у такому випадку є не окремий пристрій, а складний багаторівневий енергетичний комплекс, що забезпечує безперервне функціонування телекомунікаційного обладнання, комутаційних полів, транспортних вузлів, серверних платформ, систем синхронізації, охолодження, пожежної безпеки та сервісних підсистем. Безвідмовність цього комплексу визначає доступність послуг зв'язку, стійкість інформаційного обміну та можливість оперативного реагування на аварійні події в мережі [23].

Сучасні уявлення про кіберфізичні системи ґрунтуються на тому, що фізичний об'єкт, його цифрова модель, мережеві засоби взаємодії та керуючі алгоритми мають функціонувати як єдина узгоджена система. У межах підходу NIST кіберфізична система розглядається як сукупність взаємодіючих обчислювальних та фізичних компонентів, для яких принциповими є часові характеристики, довіреність, межі системи, життєвий цикл, управління даними та забезпечення стійкості [22]. У роботі [42] Раджкумар, Лі, Ша та Станковіч сформулювали концепцію кіберфізичних систем як наступної революції в обчислювальній техніці, акцентуючи на принциповій залежності кіберчастини від фізичних обмежень об'єкта керування. Лі в роботі [43] виділив часові обмеження та реактивність як ключові виклики проєктування CPS-систем. Кім та Кумар у

праці [44] узагальнили розвиток теорії кіберфізичних систем до сучасного стану, виділивши задачі координації, надійності, масштабованості та безпеки.

Серед існуючих моделей кіберфізичних систем для інфраструктурних об'єктів виділяють декілька основних класів. Перший клас становлять тришарові моделі типу «фізичний рівень – мережевий рівень – рівень застосунків», які добре підходять для опису простих систем, але недостатньо враховують специфіку керування у реальному часі. Другий клас – п'ятишарові моделі (5C-архітектура: Connection, Conversion, Cyber, Cognition, Configuration), які детально розкривають логіку перетворення сирої телеметрії в обґрунтовані рішення керування. Третій клас – моделі, орієнтовані на цифрового двійника, у яких ключову роль відіграє безперервно актуалізована цифрова репрезентація фізичного об'єкта, придатна для симуляції наслідків керуючих впливів [22, 42].

Стандартизовані моделі систем електроживлення телекомунікаційного обладнання представлені у документах ETSI EN 300 132 та ITU-T L.1200, L.1300 [24–27]. Зокрема, ETSI EN 300 132-3 описує інтерфейс електроживлення на вході телекомунікаційного та ІСТ-обладнання при використанні випрямного джерела до 400 В. ITU-T L.1200 формалізує вимоги до інтерфейсу постійного струму до 400 В для телекомунікаційного та ІСТ-обладнання, а L.1300 встановлює кращі практики для зелених датацентрів. Ці моделі добре регламентують фізичний рівень взаємодії, але не покривають інформаційно-керуючу частину кіберфізичної системи у повному обсязі.

Стандарт EN 50600 [7, 28, 46, 47] системно описує інфраструктуру датацентрів, включаючи систему живлення (частина 2-2), будівельну частину (2-1) та загальні концепції (1). У контексті центрів комутації телекомунікаційних мереж стандарт EN 50600 застосовний з певними адаптаціями, оскільки телеком-вузли мають специфічні вимоги до DC-живлення -48 В, тогочасно як датацентри переважно орієнтуються на АС. Тим не менш, ця сім'я стандартів забезпечує найбільш повну формалізовану модель об'єктів критичної інформаційної інфраструктури.

Окремою категорією є моделі smart grid, формалізовані у NIST SP 1108 [29], які описують взаємодію енергетичних та інформаційно-комунікаційних доменів. Ці моделі релевантні для центрів комутації, оскільки сучасний енергетичний контур ЦКТМ часто включає декілька джерел живлення (мережа, генератор, відновлювані джерела, накопичувачі), які потребують координованого керування. Однак безпосереднє застосування моделей smart grid у телекомунікаційному середовищі ускладнюється відмінностями у часових масштабах, протоколах телеметрії та вимогах до резервування.

У роботі [21] запропоновано підхід до інтелектуального управління системами електропостачання телекомунікаційних об'єктів на основі IoT-технологій, який інтегрує моніторинг параметрів електроживлення з прогнозуванням стану обладнання. Цей підхід демонструє практичну можливість застосування сенсорних мереж та edge-обчислень у задачах управління телекомом, проте не охоплює координацію кліматичного та енергетичного контурів, а також не формалізує модель технічного стану акумуляторної підсистеми у повному обсязі.

Узагальнюючи аналіз відомих моделей, можна виокремити три їхні загальні обмеження для застосування у задачі управління енергозабезпеченням ЦКТМ. По-перше, більшість моделей фокусуються на одному рівні – або на фізичній архітектурі живлення, або на інформаційній архітектурі моніторингу – і не дають інтегрованого опису всіх аспектів кіберфізичної взаємодії. По-друге, моделі не враховують специфіки гетерогенної модернізації, при якій на одному майданчику одночасно експлуатується обладнання різних поколінь та виробників. По-третє, моделі недостатньо формалізують модель технічного стану резервних ресурсів, особливо акумуляторного контуру, що є критичним для прогнозування часу автономної роботи [22, 36, 37].

Додатково варто розглянути моделі, що базуються на парадигмі Industrial Internet of Things (IIoT). Industrial Internet Consortium у Industrial Internet Reference Architecture (IIRA) пропонує чотиривимірну модель, що включає бізнес-перспективу, функціональну перспективу, реалізаційну перспективу та

перспективу використання. Така багатогранність дозволяє розглядати об'єкт з різних точок зору, але одночасно ускладнює її практичну реалізацію. Для ЦКТМ найбільш релевантною є функціональна перспектива з трьома рівнями (Edge, Platform, Enterprise), що добре корелює з трирівневою архітектурою запропонованої системи.

Окремий інтерес становлять моделі цифрових двійників (Digital Twin), що набули значної популярності у промисловому секторі. Стандарт ISO 23247 формалізує концепцію цифрового двійника для виробничих систем, виділяючи чотири основні функціональні сутності: User Entity (користувачі), Digital Twin Entity (цифровий двійник), Device Communication Entity (комунікація з пристроями), Observable Manufacturing Element (фізичний об'єкт). Для енергозабезпечення ЦКТМ застосування концепції цифрового двійника передбачає створення комп'ютерної моделі енергетичної інфраструктури, що безперервно синхронізується з реальним об'єктом і дозволяє виконувати симуляційні дослідження наслідків керуючих впливів перед їх реальним виконанням. На рисунку 1.1 узагальнено структуру кіберфізичної системи у форматі трьох взаємодіючих площин.

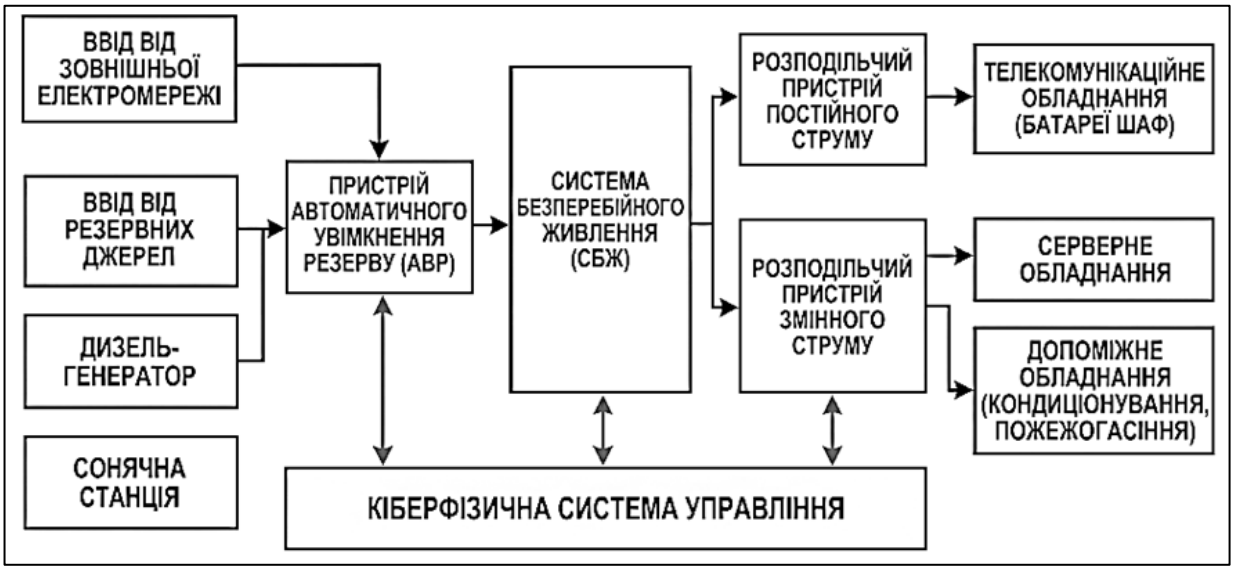


Рисунок 1.1 – Загальна структура кіберфізичної системи управління енергозабезпеченням ЦКТМ

Енергетична площина включає вводи живлення, ДБЖ, акумуляторні масиви, ДГУ, шини, кондиціонування. Інформаційно-керуюча площина включає сенсорні модулі, локальні контролери, шлюзи, диспетчерську платформу та засоби аналітики. Розривність зв'язків між цими площинами в існуючих рішеннях є основною причиною неефективності традиційних підходів до управління енергозабезпеченням [22, 23, 30].

1.2 Аналіз методів управління енергозабезпеченням телекомунікаційних об'єктів

Методи управління системами енергозабезпечення центрів комутації розвивалися від простих локальних регуляторів до сучасних розподілених систем з елементами штучного інтелекту. Аналіз сучасних досягнень у галузі дозволяє виокремити декілька типових груп методів, кожна з яких має свої переваги, обмеження та сферу доцільного застосування.

Першу групу складають реактивні методи на основі порогових алгоритмів. Вони фіксують вихід параметрів за допустимі межі (наприклад, перевищення температури батарейного відсіку, падіння напруги зовнішнього вводу, спрацьовування датчика руху) і виконують запрограмовані дії: ввімкнення резерву, генерацію аварійного сповіщення, переведення обладнання у режим зниженої функціональності. Перевагами цих методів є простота реалізації, передбачуваність поведінки, низькі обчислювальні витрати. Однак вони не забезпечують раннього виявлення проблем, а лише реакцію на свершені факти, що критично у системах з вимогами безперервної доступності [23].

Другу групу становлять методи на основі скінченних автоматів та сценарних дерев рішень. У них стан системи описується як композиція станів окремих компонентів, а правила переходів між ними формалізують допустимі сценарії експлуатації. Цей підхід використовується у класичних SCADA-системах та платформах DCIM. Він дає змогу обробляти комплексні події, наприклад

одночасне зникнення зовнішнього живлення та зростання температури, шляхом активації відповідних сценаріїв. Обмеженням цього підходу є трудомісткість ручного складання сценаріїв та неможливість динамічного переналаштування при появі нових типів обладнання або режимів експлуатації [22, 30].

Третю групу формують методи предиктивного обслуговування, які застосовують статистичні моделі та методи машинного навчання для виявлення тенденцій деградації обладнання. Для акумуляторного контуру це передбачає аналіз історії циклів заряду-розряду, динаміки внутрішнього опору, температурного режиму. Робота [36] детально розглядає сучасні підходи до управління акумуляторами в датацентрах наступного покоління, виділяючи перевагу інтегрованих BMS-систем для Li-ion та LiFePO4 хімій. Метод [37] пропонує оцінку надійності конфігурацій динамічних систем електроживлення на основі стохастичних моделей, що дозволяє кількісно порівнювати альтернативні архітектури.

Четверту групу складають методи координованого управління енергетичним та кліматичним контурами. Ці методи виходять з того, що теплове навантаження є нелінійною функцією електричного навантаження, стану ДБЖ та потужності системи охолодження. Координоване керування передбачає одночасне врахування електричних і теплових параметрів при прийнятті рішень про перерозподіл навантаження. У стандартах ITU-T L.1300 та EN 50600-2-2 цей підхід рекомендований як основний для сучасних об'єктів критичної інформаційної інфраструктури [27, 28].

П'яту групу складають методи з використанням гібридних енергетичних систем, які включають мережеве живлення, дизельний резерв, сонячну генерацію, вітрові установки малої потужності та системи накопичення енергії. У роботі [35] показано, що поєднання цих джерел може суттєво підвищити стійкість телекомунікаційного об'єкта в умовах тривалих перебоїв, однак вимагає більш складних алгоритмів керування (EMS-клас), здатних координувати множину гетерогенних джерел.

Шосту групу складають методи виявлення аномалій та класифікації інцидентів на основі методів машинного навчання. Для систем енергозабезпечення характерним є застосування методів виявлення відхилень від типового профілю споживання, аналізу спектру вібраційних сигналів роторного обладнання, прогнозування часу до відмови за моделями виживання. Ці методи демонструють хороші результати в академічних дослідженнях, але потребують значного обсягу якісних даних та можуть давати помилкові спрацьовування у разі недостатнього навчального матеріалу [38, 39].

Сьому групу формують методи координованого управління в умовах edge-розгортань. Сучасні телекомунікаційні мережі мають ієрархічну структуру: ядрові вузли, регіональні центри, локальні комутаційні майданчики, edge-вузли. Робота [45] показує, що для таких систем доцільно використовувати ієрархічні моделі управління, у яких локальний контролер забезпечує автономну реакцію на події, а верхній рівень виконує координацію, аналітику та оптимізацію ресурсів у межах усієї мережі.

Узагальнене порівняння розглянутих груп методів представлене у таблиці 1.1.

Таблиця 1.1 – Порівняльний аналіз груп методів управління енергозабезпеченням ЦКТМ

Група методів	Сильні сторони	Слабкі сторони	Сфера застосування
1	2	3	4
Реактивні порогові методи	Простота, передбачуваність, низькі вимоги до обчислювальних ресурсів	Виявлення проблеми лише після події, відсутність прогнозу	Локальні системи захисту, базовий контур аварійних блокувань

Скінченні автомати та сценарні дерева	Структурованість, можливість обробки комплексних подій	Складність ручного складання	Класичні SCADA/DCIM-системи на стабільних об'єктах

Кінець таблиці 1.1

1	2	3	4
Предиктивне обслуговування	Раннє виявлення деградації, підтримка планового сервісу	Потреба у накопиченні даних, ризик помилкових спрацьовувань	Акумуляторні масиви, генераторні установки, ДБЖ
Координація енергетичного та кліматичного контурів	Покращена енергоефективність, врахування взаємного впливу	Складність налаштування, потреба в інтеграційному шарі	Великі датацентри та центри комутації високої щільності
Гібридні енергосистеми	Підвищена автономність, диверсифікація джерел	Складне прогнозування, висока вартість керуючої частини	Об'єкти у регіонах з нестабільним електропостачанням
Машинне навчання для виявлення аномалій	Адаптивність, виявлення раніше невідомих типів відмов	Потреба у якісних даних, складність інтерпретації	Об'єкти із зрілою системою збору телеметрії
Ієрархічне edge-керування	Локальна автономність, масштабованість на множину майданчиків	Складність координації між рівнями, вимоги до зв'язку	Розподілені оператори зв'язку з множиною майданчиків

Аналіз показує, що жоден з розглянутих методів окремо не забезпечує комплексного розв'язання задачі управління енергозабезпеченням ЦКТМ. Найкращі результати досягаються у разі поєднання декількох груп методів у межах єдиної кіберфізичної архітектури: ієрархічного розподілу функцій (метод 7), сценарного реагування на нижньому рівні (метод 2), предиктивної аналітики на верхньому рівні (метод 3), координації енергетичного та теплового контурів (метод 4) та виявлення аномалій як додаткового засобу раннього попередження (метод 6). Саме такий синтез становить основу запропонованого у цій роботі методу.

1.3 Аналіз програмно-технічних засобів моніторингу та керування енергообладнанням

Сучасний ринок пропонує широкий спектр програмно-технічних засобів для моніторингу й керування системами енергозабезпечення критичної інфраструктури. Їх можна класифікувати за декількома вимірами: функціональний рівень (від простих сигналізаторів до повноцінних BMS/DCIM/SCADA-платформ), модель розгортання (локальна, гібридна, хмарна), архітектура (монолітна, мікросервісна, edge-cloud), модель ліцензування (комерційна, open source) та орієнтація на конкретного виробника обладнання (vendor-lock vs vendor-agnostic).

До категорії базових засобів збору телеметрії належать локальні контролери, PLC та RTU-пристрої, які підтримують промислові протоколи Modbus RTU/TCP [17], DNP3, IEC 61850 [41]. Вони забезпечують надійний збір параметрів електричних та фізичних величин, мають вбудовану логіку обробки сигналів, але як правило обмежені у рівні аналітики та інтеграції з зовнішніми системами. Прикладами таких пристроїв є контролери Siemens S7, Schneider Modicon, Wago I/O, Moxa ioLogik, Advantech ADAM-серії. Перевагами є висока надійність та робочий ресурс, добра підтримка стандартів промислових мереж. Недоліками – закритість архітектури, високі капітальні витрати, складність інтеграції з нестандартним обладнанням.

Для управління акумуляторними масивами використовуються спеціалізовані BMS-системи. Сучасні BMS для Li-ion та LiFePO4 хімій забезпечують поелементний моніторинг напруги, температури та струму кожної комірки, балансування заряду, оцінювання стану заряду (SoC) та стану здоров'я (SoH), захист від перезаряду, перерозряду та перегріву. Робота [36] показує, що інтегровані BMS дозволяють продовжити термін служби акумуляторів на 20–30% порівняно з примітивним керуванням. Для VRLA-батарей застосовуються більш прості системи моніторингу типу Battery Health Monitor, які контролюють напругу та температуру окремих банків, але не забезпечують поелементного контролю.

Засоби моніторингу ДБЖ та випрямлячів представлені пропрієтарними системами провідних виробників: APC InfraStruxure (Schneider Electric), Eaton IPM (Intelligent Power Manager), Vertiv Liebert Trellis, Riello PowerNetGuard, Delta InsightPower та інші. Ці системи добре інтегруються з обладнанням свого виробника, забезпечують повний контроль параметрів ДБЖ, генерують детальні звіти, підтримують віддалене керування. Однак їх недоліком є обмежена підтримка обладнання інших виробників, що ускладнює побудову єдиної системи моніторингу на гетерогенних об'єктах.

DCIM-платформи (Data Center Infrastructure Management) орієнтовані на комплексне керування інфраструктурою датацентру. Найвідомішими представниками є Schneider EcoStruxure IT Expert, Vertiv Trellis, Sunbird dcTrack, Nlyte, Device42, Cormant-CS. Вони забезпечують інвентаризацію обладнання, моніторинг живлення та клімату, управління кабельним господарством, планування ємності, фізичну візуалізацію розташування. DCIM-системи добре підходять для великих датацентрів, але мають високу вартість та потребують значних зусиль на впровадження. Для невеликих центрів комутації регіонального рівня вони часто є надлишковими.

Системи SCADA (Supervisory Control and Data Acquisition) традиційно застосовуються у промисловості, енергетиці та для критичної інфраструктури. Серед комерційних рішень виділяються Siemens WinCC, Schneider Wonderware (зараз AVEVA), GE iFIX, ICONICS Genesis, Rockwell FactoryTalk View. Open

source-альтернативи представлені Ignition (Inductive Automation, partly open), Rapid SCADA, OpenSCADA, ScadaBR. SCADA забезпечує гнучке налаштування мнемосхем, складних логічних правил та обробки подій. Однак SCADA-системи орієнтовані на кваліфікованого інженера-проєктувальника, що ускладнює їх адаптацію до специфічних вимог телеком-середовища.

Сучасні платформи IoT (Інтернету речей) утворюють окремий клас засобів. Серед них виділяються AWS IoT Core, Azure IoT Hub, Google Cloud IoT, ThingsBoard (open source), Eclipse Kura, Mainflux. Вони забезпечують підключення великої кількості сенсорів через MQTT [17], CoAP, AMQP та надають хмарну інфраструктуру для зберігання, обробки та візуалізації телеметрії. Перевагою є гнучкість, масштабованість, інтеграція з аналітичними сервісами. Однак для критичної інфраструктури зв'язку повна залежність від хмари може бути неприйнятною з міркувань кібербезпеки та збереження функціональності при втраті зв'язку з зовнішнім світом.

Спеціалізовані рішення для телекомунікаційного сегменту включають продукти таких виробників, як Eltek (Delta), Emerson Network Power, Vertiv NetSure, Powerwave, ZTE ZXDU, Huawei OptiX Power. Ці рішення оптимізовані під специфіку DC-живлення -48 В, мають вбудовані модулі моніторингу батарей, інтегруються з мережевими системами управління операторів зв'язку (OSS/BSS). Однак вони часто закриті, оптимізовані під обладнання конкретного виробника, та обмежено підтримують стандартизовані протоколи моніторингу сторонніми системами.

Open source-засоби заслуговують окремого розгляду через зростаюче значення для сегменту критичної інфраструктури. ThingsBoard – відкрита IoT-платформа, що підтримує MQTT, CoAP, HTTP та широкий набір протоколів. Grafana – засіб візуалізації часових рядів з плагінами для багатьох баз даних (InfluxDB, Prometheus, TimescaleDB). Home Assistant – платформа автоматизації, орієнтована переважно на побутовий сектор, але адаптована для невеликих промислових проєктів. Node-RED – інструмент для візуального програмування інтеграційних потоків даних. Поєднання цих інструментів дозволяє побудувати

гнучку, недорогу систему моніторингу, але вимагає глибокої експертизи команди впровадження.

Узагальнене порівняння розглянутих категорій програмно-технічних засобів представлене в таблиці 1.2.

Таблиця 1.2 – Порівняльний аналіз категорій програмно-технічних засобів управління енергозабезпеченням

Категорія	Орієнтовна вартість	Гнучкість	Інтегрованість	Кіберстійкість
Локальні PLC/RTU контролери	Середня	Середня	Низька	Середня
Спеціалізовані BMS	Висока	Низька	Середня	Висока
Пропрієтарні системи виробників ДБЖ	Висока	Низька	Низька (vendor-lock)	Висока
DCIM-платформи	Дуже висока	Висока	Висока	Висока
Класичні SCADA-системи	Висока	Дуже висока	Висока	Висока
Хмарні IoT-платформи	Низька	Дуже висока	Висока	Залежить від конфігурації
Open source-стек (ThingsBoard, Grafana)	Низька (зусилля впровадження)	Дуже висока	Висока (потребує налаштування)	Залежить від впровадження
Спеціалізовані рішення для телекому	Висока	Низька	Висока (з обладнанням виробника)	Висока

Із наведеного аналізу очевидно, що жодна з існуючих категорій засобів не забезпечує повноцінного розв'язання задачі для умов центрів комутації телекомунікаційних мереж. Зокрема, спеціалізовані BMS-системи добре вирішують задачу управління батарейним контуром, але не забезпечують інтеграції з кліматичним та інформаційним контурами. Пропрієтарні системи виробників ДБЖ обмежені vendor-lock, що неприйнятно для об'єктів з гетерогенним обладнанням. DCIM-платформи занадто дорогі та складні для регіональних центрів комутації. Хмарні IoT-платформи не відповідають вимогам кіберстійкості критичної інфраструктури зв'язку. Open source-стек має потенціал, але потребує спеціалізованої інтеграційної роботи. Це обумовлює актуальність розроблення власної кіберфізичної системи, яка поєднає переваги різних підходів та забезпечить повноту розв'язання задачі. Класифікацію наведено на рисунку 1.2.

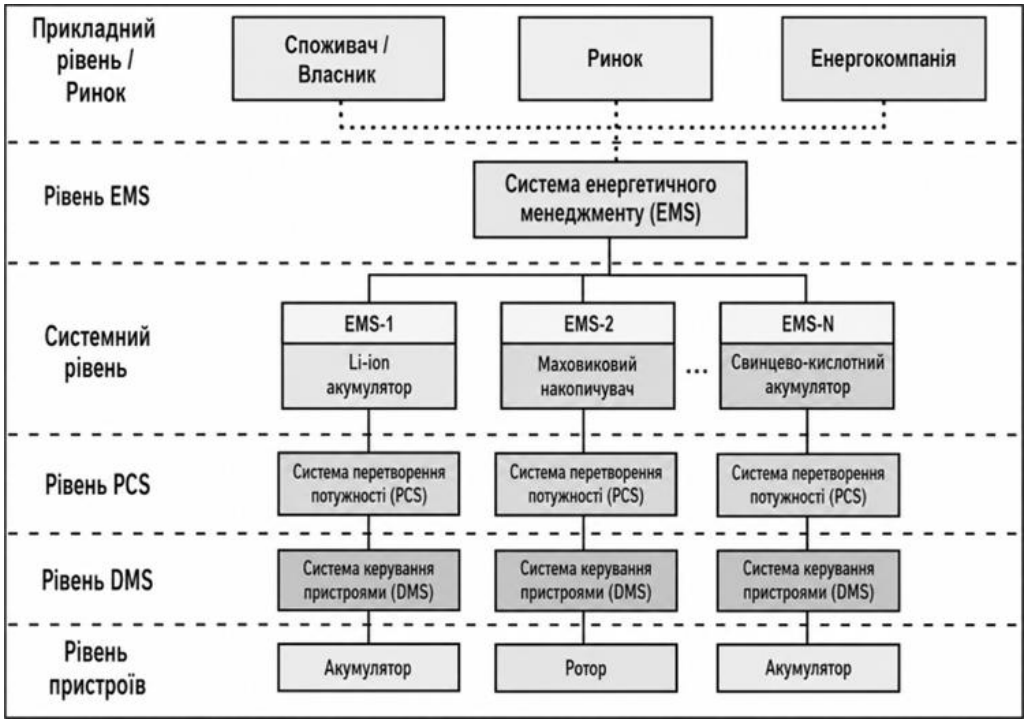


Рисунок 1.2 – Класифікація програмно-технічних засобів управління енергообладнанням за функціональною повнотою та відкритістю

Окремою тенденцією, яку слід відзначити, є зростання інтересу до edge computing-архітектур у галузі моніторингу критичної інфраструктури. Якщо у

попереднє десятиліття акцент був на хмарних рішеннях зі централізованою обробкою, то останніми роками очевидним став рух у бік розосередження обчислень ближче до джерела даних [45]. Це пояснюється кількома факторами: вимогами до латентності (критичні сценарії потребують часу реакції в межах мілісекунд, що недосяжно при хмарній обробці); вимогами до пропускної здатності (передача всієї телеметрії в хмару створює надмірне навантаження на канали зв'язку); вимогами до автономності (об'єкт повинен функціонувати навіть при втраті зв'язку); вимогами до кібербезпеки (критичні рішення не повинні залежати від зовнішніх сервісів). Ці тенденції підтримують доцільність запропонованого у цій роботі підходу з трирівневою архітектурою.

1.4 Постановка задачі

На підставі проведеного аналізу формулюється така постановка задачі: розробити кіберфізичну систему управління системами енергозабезпечення центрів комутації телекомунікаційних мереж, що забезпечує інтегрований моніторинг електричних і теплових параметрів, виконує предиктивну оцінку технічного стану елементів енергетичної інфраструктури, реалізує сценарне реагування на типові аварійні ситуації та підтримує захищену взаємодію між локальними контролерами і централізованим аналітичним рівнем.

Для розв'язання поставленої задачі необхідно розробити: концепцію та структурно-функціональну модель кіберфізичної системи управління (розділ 2.1, 2.2); інформаційну модель об'єкта та модель технічного стану (розділ 2.3); метод адаптивного управління (розділ 2.4); алгоритм функціонування системи (розділ 3.1); вимоги до програмного забезпечення та архітектурне проєктування (розділи 3.2, 3.3); проєктування підсистеми збору телеметрії (розділ 3.4); програмну реалізацію кіберфізичної системи (розділ 4.1); провести експериментальні дослідження та оцінити ефективність розроблених методу та засобів (розділи 4.2, 4.3).

1.5 Висновки

Проведений у розділі аналіз дає змогу сформулювати такі основні висновки.

1. Існуючі моделі кіберфізичних систем (тришарові, 5C-архітектура, моделі цифрових двійників) забезпечують теоретичну основу побудови інтегрованих систем управління, однак для специфічних умов центрів комутації телекомунікаційних мереж потребують адаптації. Зокрема, необхідна формалізація моделі технічного стану резервних ресурсів, опис гетерогенної модернізації та інтеграція енергетичного й кліматичного контурів керування у єдиному інформаційному просторі.

2. Існуючі методи управління енергозабезпеченням можна класифікувати за сімома основними групами: реактивні порогові, сценарні автомати, предиктивне обслуговування, координація енергетичного та кліматичного контурів, гібридні енергосистеми, виявлення аномалій машинним навчанням, ієрархічне edge-керування. Жоден з цих методів окремо не забезпечує комплексного розв'язання задачі. Найкращих результатів можна досягти шляхом їх синтезу у межах єдиної кіберфізичної архітектури.

3. Існуючі програмно-технічні засоби (PLC/RTU контролери, BMS, пропрієтарні системи виробників, DCIM, SCADA, IoT-платформи, open source-стек, спеціалізовані рішення для телекому) кожен з своїх сильних сторін, однак мають суттєві обмеження для застосування в умовах центрів комутації. Найбільш перспективним є побудова власної системи на основі поєднання open source-компонентів зі спеціалізованою бізнес-логікою для енергозабезпечення ЦКТМ.

4. На основі проведеного аналізу можна стверджувати, що актуальною є задача розроблення кіберфізичної системи управління системами енергозабезпечення центрів комутації телекомунікаційних мереж, яка забезпечить інтегрований моніторинг гетерогенного енергетичного обладнання, підтримку предиктивної аналітики, скоординоване реагування у різних режимах роботи об'єкта, а також виконання вимог кібербезпеки для систем критичної інфраструктури.

5. Окремою важливою проблемою, що випливає з аналізу, є невідповідність часових масштабів керування. Класичні системи автоматизації орієнтовані на швидкі захисні дії в межах мілісекунд, тоді як предиктивна аналітика працює у масштабі годин і днів, а стратегічне планування інфраструктури – у масштабі місяців і років. Жодне з існуючих рішень не пропонує єдиного підходу, що поєднує усі три горизонти у когерентній архітектурі. Цей факт є ключовим обґрунтуванням необхідності розроблення нової кіберфізичної системи, у якій ієрархічний поділ керування на оперативний, тактичний та стратегічний рівні забезпечує коректне співвідношення між часом реакції та глибиною аналізу.

6. Важливим аспектом є також необхідність забезпечення пояснюваності рішень, що приймаються кіберфізичною системою. У критичній інфраструктурі будь-яка автоматизована дія повинна супроводжуватися чітким описом її причин, які можуть бути перевірені інженером або аудитором. Це відрізняє промислові кіберфізичні системи від, наприклад, рекомендаційних систем у споживчих застосунках, де пояснюваність є бажаною, але не обов'язковою. Сучасні підходи до Explainable AI у поєднанні з принципами Industrial Internet Reference Architecture можуть становити методологічну основу для побудови такого механізму пояснюваності.

2 МОДЕЛЬ ТА МЕТОД КІБЕРФІЗИЧНОЇ СИСТЕМИ УПРАВЛІННЯ ЕНЕРГОЗАБЕЗПЕЧЕННЯМ

2.1 Концепція кіберфізичної системи управління енергозабезпеченням

Концепція кіберфізичної системи управління енергозабезпеченням центрів комутації телекомунікаційних мереж формується на основі узагальнення результатів аналізу, проведеного у першому розділі, та синтезу найкращих практик з розглянутих методів і засобів. В основу концепції покладено такі основні положення.

Перше положення – інтеграція трьох взаємодіючих площин об'єкта управління. Кіберфізична система розглядає енергозабезпечення ЦКТМ як єдине ціле, що складається з фізичної (енергетичної) площини, інформаційно-керуючої площини та експлуатаційно-організаційної площини. Розривність зв'язків між цими площинами в існуючих рішеннях є основною причиною неефективності традиційних підходів. Запропонована система забезпечує єдиний інформаційний простір, у якому подія на енергетичному рівні (наприклад, перехід ДБЖ у режим роботи від батареї) відображається на рівні інформаційної аналітики (прогноз залишкового часу автономії, вибір сценарію реагування) та на рівні експлуатаційних дій (повідомлення оператора, виклик чергового інженера) [22, 23].

Друге положення – ієрархічна архітектура управління. Система складається з трьох рівнів: локального, об'єктного та централізованого. Локальний рівень включає сенсори, виконавчі пристрої та контролери, безпосередньо пов'язані з силовим обладнанням. На цьому рівні забезпечується гарантований збір телеметрії в реальному часі та виконання базових сценаріїв захисту, які повинні працювати навіть за умови втрати зв'язку з вищими рівнями. Об'єктний рівень забезпечує інтеграцію локальних вузлів у межах конкретного майданчика, нормалізацію даних, агрегування подій та координацію між енергетичним та кліматичним контурами. Централізований рівень виконує аналітику, довгострокове прогнозування та кореляцію з мережевими й сервісними платформами оператора [29, 40, 45].

Третє положення – подієво-станове управління. У запропонованій концепції стан системи описується не як окремі параметри, а як композиція станів усіх компонентів. Виділяються шість основних станів об'єкта: штатний (Normal), знижена стійкість (Degraded), передаварійний (Pre-emergency), аварійний (Emergency), відновлення (Recovery), сервісний (Maintenance). Кожен стан характеризується набором допустимих параметрів, переліком активних автоматичних сценаріїв, рівнем сповіщення оператора та обмеженнями на дії персоналу.

Четверте положення – предиктивна оцінка технічного стану. Замість примітивного контролю поточних значень параметрів система виконує багатофакторний аналіз телеметрії та обчислює інтегральний індикатор технічного стану кожного критичного компонента. Для акумуляторного контуру це передбачає оцінку залишкової ємності, стану здоров'я (SoH) та прогнозованого часу автономії з урахуванням поточного навантаження, температури, історії циклів та віку батарей [36, 37]. Для випрямлячів та ДБЖ – оцінку коефіцієнта корисної дії, стабільності вихідних параметрів, кількості подій включення-вимкнення та часу неперервної роботи. Для генераторних установок – аналіз успішності тестових запусків, стабільності частоти та напруги, рівня палива та сервісних інтервалів.

П'яте положення – координація енергетичного та кліматичного контурів. Управлінські рішення щодо перерозподілу навантаження, ввімкнення резерву, переходу в економний режим приймаються на основі сумарної оцінки електричних і теплових параметрів. Це забезпечує запобігання таким каскадним сценаріям, як перевантаження ДБЖ, що збільшує тепловиділення, що перевантажує систему охолодження, що піднімає температуру батарей, що зменшує реальний час автономії [27, 28].

Шосте положення – модульність та відкритість інтеграції. На рівні збору даних система підтримує множину протоколів (Modbus RTU/TCP [17], SNMP, MQTT, OPC UA, IEC 61850 [41]), однак на рівні інформаційної моделі телеметрія нормалізується до уніфікованого формату. Це дозволяє інтегрувати в систему

обладнання різних виробників та поколінь, а також виконувати поетапну модернізацію без повного перебудування системи моніторингу.

Сьоме положення – багаторівнева кібербезпека. Система реалізує принципи defense-in-depth відповідно до рекомендацій NIST SP 800-82 [23], ISA/IEC 62443 [30] та ENISA [31, 32]. Це включає сегментацію мереж, контроль доступу за ролями, безпечну аутентифікацію, журналювання дій, контроль змін конфігурації та сценарій fail-safe при порушенні цілісності інформаційного рівня. Принцип «спочатку функціональність, потім безпека» для такого класу систем є неприйнятним.

Восьме положення – підтримка експлуатаційного персоналу. Система забезпечує когнітивну підтримку оператора через зрозумілий людино-машинний інтерфейс, ранжування подій за критичністю, пояснення причин ризиків та рекомендації щодо безпечного переключення. Когнітивна підтримка є важливою як для зручності експлуатації, так і для безпеки прийняття рішень у стресових умовах аварійних подій.

Особливістю запропонованої концепції є органічне поєднання детермінованих елементів управління (порогові спрацьовування, сценарії реагування з чітко визначеними кроками) з імовірнісними елементами (предиктивна аналітика, статистичні моделі деградації). Така комбінація забезпечує надійність базових функцій захисту, що залежать від чітких правил, та водночас дає змогу використовувати переваги глибокої аналітики для ранніх попереджень. У розглянутих у розділі 1 існуючих рішеннях такий синтез реалізований лише частково – одні системи зосереджені на детермінованому реагуванні, інші – на імовірнісному прогнозуванні, але мало хто інтегрує обидва підходи в єдиному контурі управління [22, 36, 37].

Ще однією особливістю концепції є врахування реальних обмежень впровадження на діючих об'єктах. Центр комутації не може бути виведений з експлуатації для повної модернізації, тому система повинна підтримувати поетапну інтеграцію. Концепція передбачає, що на першому етапі впровадження можуть бути підключені лише найважливіші вузли (ДБЖ, АКБ), а решта

обладнання інтегрується поступово без зупинки сервісів. Друга важлива вимога – сумісність зі спадковим обладнанням, яке може використовувати застарілі протоколи моніторингу або взагалі не мати цифрового інтерфейсу. Для таких випадків концепція передбачає можливість застосування зовнішніх сенсорів (датчиків струму, температури, напруги), що накладаються на існуюче обладнання без втручання у його конструкцію.

Концептуально кіберфізична система розглядається не як набір моніторингових інструментів, а як активний учасник процесу управління об'єктом, який доповнює, але не замінює, експлуатаційний персонал. Така позиція є ключовою для впровадження у середовище критичної інфраструктури, де довіра до автоматизованих рішень повинна формуватися поступово, а оператор повинен зберігати повний контроль над важливими переключеннями. У різних моделях впровадження ступінь автоматизації може відрізнятися: від чисто інформаційного режиму до майже повністю автоматизованого. Концепція підтримує плавний перехід між цими режимами в міру накопичення довіри та досвіду експлуатації.

На рисунку 2.1 показано взаємозв'язок концептуальних положень.

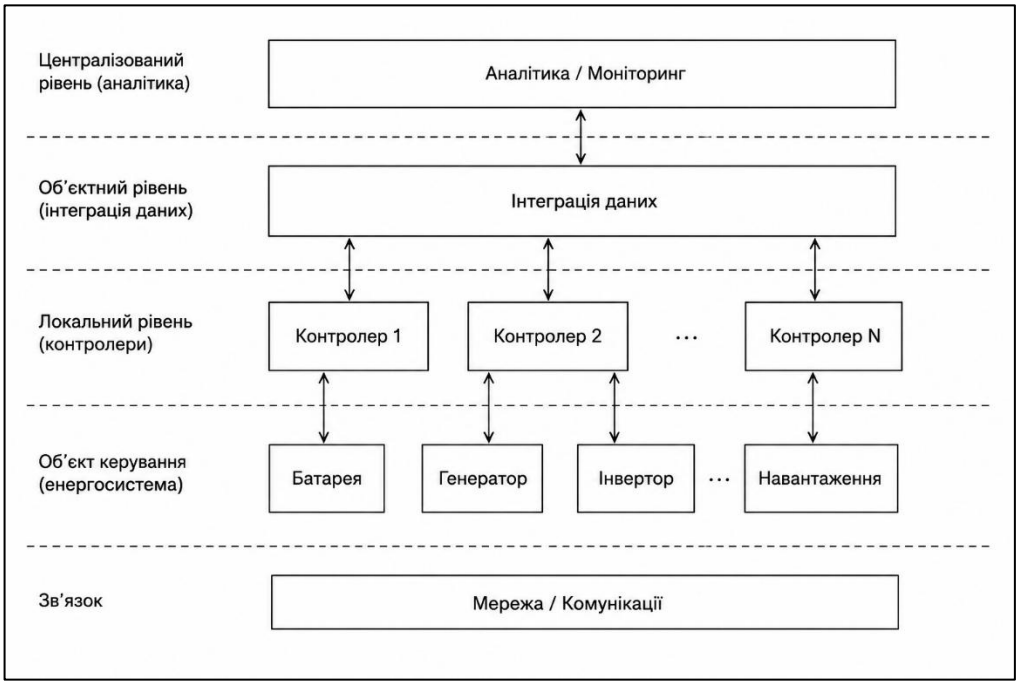


Рисунок 2.1 – Концептуальна схема кіберфізичної системи управління енергозабезпеченням ЦКТМ

У центрі схеми розташований об'єкт керування – система енергозабезпечення ЦКТМ. Навколо нього концентричними колами розташовані рівні управління: локальний (контролери), об'єктний (інтеграція даних), централізований (аналітика). Перпендикулярно цим рівням проходять наскрізні аспекти: інформаційна модель, кібербезпека, людино-машинний інтерфейс. Така концепція забезпечує системний розгляд об'єкта і запобігає ізоляції окремих функцій.

2.2 Структурно-функціональна модель кіберфізичної системи

Структурно-функціональна модель кіберфізичної системи описує її основні компоненти, їхні функції та інформаційні зв'язки між ними. Запропонована модель формалізує концепцію, наведену в підрозділі 2.1, у вигляді конкретних архітектурних рівнів та модулів. Модель побудована за принципом ієрархічної декомпозиції з елементами розподіленого функціонування, що відповідає сучасним вимогам до промислових кіберфізичних систем [22, 30].

Локальний рівень включає такі основні компоненти: датчики (температури, напруги, струму, рівня палива, відкриття дверей, пожежні, газові); виконавчі пристрої (керовані реле, контактори АВР, привод заслінок вентиляції); інтелектуальні модулі (вбудовані BMS-системи, контролери ДБЖ, контролери ДГУ); локальні PLC/RTU-пристрої, що збирають телеметрію з підключених датчиків та комунікуючого обладнання; шлюзи протоколів (Modbus RTU/TCP, SNMP, Modbus to MQTT bridges) для нормалізації даних. На цьому рівні забезпечується мінімальна затримка реагування на критичні події – не більше 100 мс для аварійних блокувань.

Об'єктний рівень включає: edge-сервер (промисловий комп'ютер або вбудована плата) з програмним забезпеченням збору і первинної обробки телеметрії; локальну базу даних часових рядів (TimescaleDB або InfluxDB) для зберігання історії параметрів; модуль кореляції подій (event correlation engine), який об'єднує супутні події в інциденти; модуль локальної аналітики (обчислення похідних показників, обмежена предиктивна аналітика на основі простих моделей);

модуль безпечної взаємодії з централізованим рівнем (VPN-тунель, mTLS); модуль локального HMI для обслуговуючого персоналу. На цьому рівні забезпечується автономне функціонування об'єкта при втраті зв'язку з централізованим рівнем – система продовжує збір даних, виконання базових сценаріїв реагування та інформування персоналу.

Централізований рівень включає: центральну базу даних телеметрії (відображення поточного стану всіх об'єктів мережі); архівну базу історичних даних з тривалим періодом зберігання; модуль глибокої аналітики (предиктивні моделі, виявлення аномалій, аналіз тенденцій); модуль інтеграції з NMS/OSS-платформами оператора; модуль централізованого диспетчерського HMI; модуль управління інцидентами (тікетна система); модуль управління користувачами та правами доступу (RBAC); підсистему звітності й аудиту. Централізований рівень дозволяє оператору отримати єдину картину стану всієї телекомунікаційної інфраструктури, виконувати порівняльний аналіз об'єктів, оптимізувати графіки технічного обслуговування.

Інформаційні потоки між рівнями реалізуються за такою схемою: телеметрія від датчиків та контролерів передається на локальний рівень через промислові протоколи (Modbus, SNMP); локальний рівень нормалізує дані та публікує їх до брокера повідомлень MQTT [17]; об'єктний edge-сервер підписаний на ці повідомлення та виконує первинну обробку; раз на хвилину агреговані дані передаються на централізований рівень через захищений канал; критичні події передаються негайно поза основним циклом. Команди управління від оператора передаються в зворотному напрямку зі збереженням повного ланцюжка автентифікації та авторизації.

Описана модель наведена на рисунку 2.2.

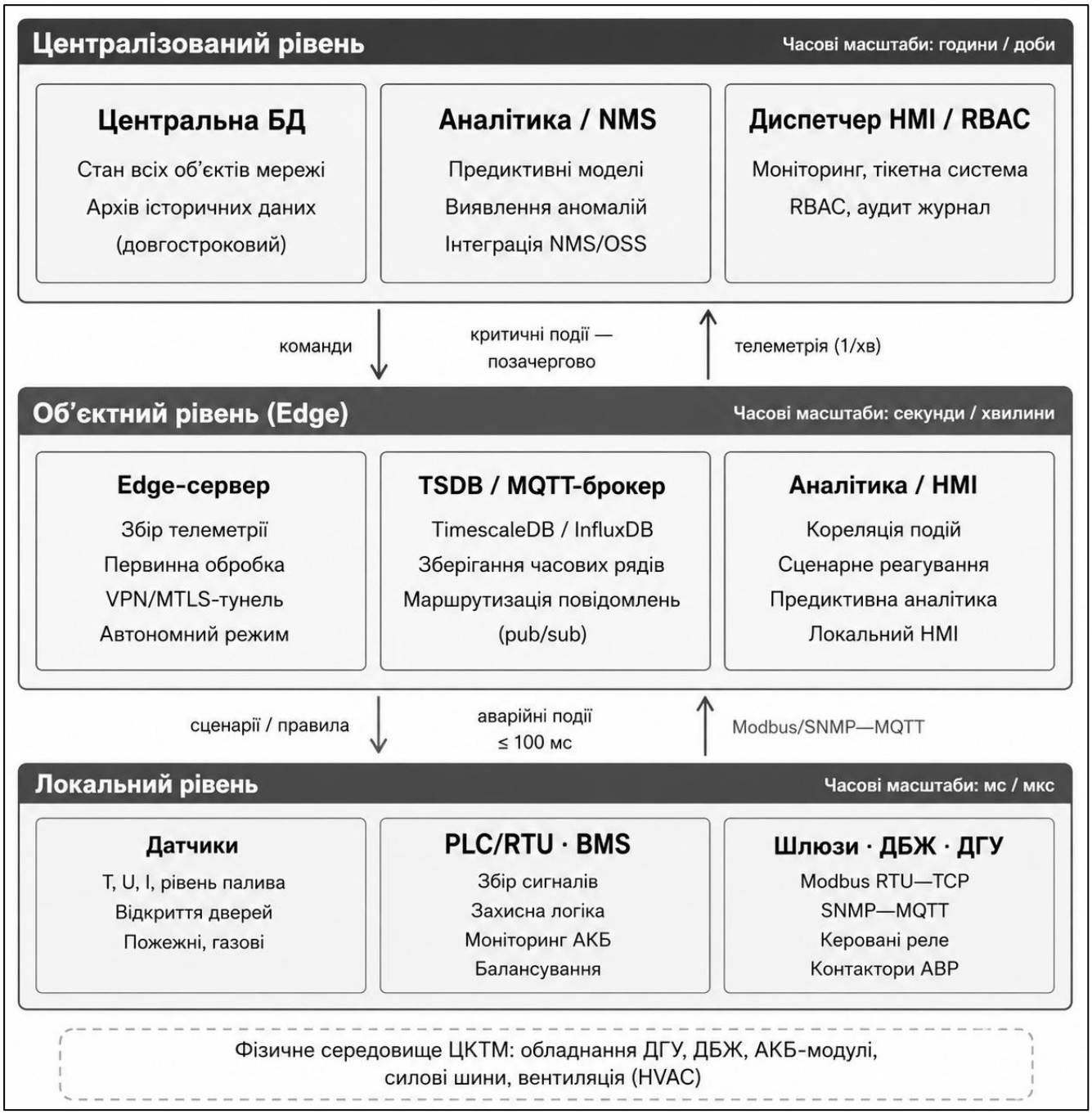


Рисунок 2.2 – Структурно-функціональна модель кіберфізичної системи управління енергозабезпеченням ЦКТМ

Запропонована модель формалізована у вигляді ієрархічної структури S = {SL, SO, SC, R}, де SL – множина компонентів локального рівня, SO – множина компонентів об'єктного рівня, SC – множина компонентів централізованого рівня, R – множина відношень між компонентами. Кожен елемент моделі

характеризується атрибутами (тип, ідентифікатор, місце розташування, технічні параметри) та функціональними зв'язками з іншими елементами.

Перелік основних компонентів моделі та їхніх функцій наведено в таблиці 2.1.

Таблиця 2.1 – Основні компоненти структурно-функціональної моделі

Рівень	Компонент	Основна функція
1	2	3
Локальний	Датчики (T, U, I, рівень)	Перетворення фізичних величин у вимірювальні сигнали
Локальний	PLC/RTU контролери	Збір сигналів, виконання базової логіки захисту
Локальний	BMS батарейних модулів	Поелементний моніторинг АКБ, балансування
Локальний	Контролери ДБЖ та ДГУ	Моніторинг та керування джерелом живлення
Локальний	Шлюзи протоколів	Перетворення Modbus RTU - Modbus TCP, SNMP - MQTT
Об'єктний	Edge-сервер	Хост для модулів збору, аналітики, HMI
Об'єктний	База часових рядів (TSDB)	Зберігання історії параметрів з пошуком за часом
Об'єктний	Брокер MQTT	Маршрутизація повідомлень телеметрії та команд
Об'єктний	Модуль кореляції подій	Об'єднання супутніх подій в інциденти
Об'єктний	Модуль локальної аналітики	Обчислення похідних показників, перевірки правил
Об'єктний	Локальний HMI	Інтерфейс оперативного персоналу на майданчику

Кінець таблиці 2.1

1	2	3
Централізований	Центральна БД стану	Поточний стан усіх об'єктів мережі
Централізований	Архів історичних даних	Довгострокове зберігання та bashing запити
Централізований	Модуль глибокої аналітики	Предиктивні моделі, машинне навчання
Централізований	Інтеграція з NMS/OSS	Кореляція з мережевими подіями оператора
Централізований	Диспетчерський HMI	Єдиний пункт моніторингу всієї інфраструктури
Централізований	Тікетна система	Управління інцидентами, призначення відповідальних
Централізований	RBAC та audit log	Управління доступом, журналювання дій

Особливістю запропонованої моделі є чітке розмежування відповідальності між рівнями та забезпечення автономності кожного рівня. У разі повної втрати зв'язку з централізованим рівнем об'єктний рівень продовжує функціонувати, виконуючи моніторинг та сценарне реагування. У разі втрати зв'язку з об'єктним рівнем локальні контролери продовжують виконувати базові захисні функції. Така архітектурна відмовостійкість є критично важливою для систем критичної інфраструктури зв'язку [23].

Окремим важливим аспектом моделі є визначення часових масштабів роботи кожного рівня. Локальний рівень працює у мікросекундному та мілісекундному діапазоні – саме тут реалізуються апаратні захисти від коротких замикань, перенапруг та інших швидких процесів. Об'єктний рівень оперує секундами та хвилинами – на цьому рівні здійснюється класифікація стану, активація сценаріїв, координація між енергетичним та кліматичним контурами. Централізований рівень

оперує годинами та добами – тут виконується довгостроковий аналіз, побудова прогнозних моделей та координація між майданчиками. Часові розриви між рівнями забезпечують, з одного боку, гарантовану швидкість реакції на критичні події, а з іншого – глибину аналітики для стратегічних рішень.

Зв'язки між компонентами моделі організовані за принципом слабкого зв'язування (loose coupling) через MQTT-брокер. Це означає, що кожен компонент знає лише про абстрактний інтерфейс (тематика повідомлень, формат даних), а не про конкретні реалізації інших компонентів. Така архітектура дозволяє замінювати окремі компоненти без впливу на решту системи, що критично для довгострокової підтримки. Наприклад, при появі нового виробника обладнання достатньо реалізувати відповідний адаптер протоколу – решта системи не змінюється.

Ще одним важливим аспектом моделі є реалізація принципу відмовостійкості за допомогою резервування ключових компонентів. На об'єктному рівні MQTT-брокер може бути розгорнутий у кластерній конфігурації, що забезпечує продовження роботи при відмові одного вузла. База часових рядів TimescaleDB підтримує потокову реплікацію, що дозволяє відновити дані з реплік. Edge-сервер може бути продубльований у форматі активний-резервний, що дає змогу автоматичного перемикання при апаратній відмові. Така багаторівнева відмовостійкість забезпечує загальну надійність системи на рівні, який вимагається для систем критичної інфраструктури зв'язку [23, 30].

Структурно-функціональна модель також містить опис інтерфейсів взаємодії з зовнішніми системами. Виділяються чотири основні категорії таких систем: системи управління мережею оператора (NMS/OSS); системи бізнес-аналітики (BI/Data Warehouse); тікетні системи управління інцидентами (Service Desk); системи звітності для регулятора (compliance reporting). Для кожної категорії визначений набір API-endpoints, формати обміну даними (JSON, XML, CSV) та механізми автентифікації (API keys, OAuth2). Стандартизація цих інтерфейсів важлива для забезпечення можливості інтеграції в існуючу IT-екосистему оператора без необхідності побудови custom-адаптерів для кожної конкретної системи.

Окремою важливою частиною моделі є опис ролей та відповідальності користувачів системи. Виділяються чотири основні ролі: Operator (оперативний персонал, що працює з системою цілодобово – моніторинг стану, виконання типових процедур, ескалація серйозних інцидентів); Engineer (інженерно-технічний персонал, що відповідає за обслуговування обладнання, аналіз технічних проблем, координацію з постачальниками); Administrator (адміністратор системи, що відповідає за конфігурацію, налаштування правил, додавання нових об'єктів та користувачів); Auditor (аудитор, що має доступ лише на читання для перевірки відповідності регуляторним вимогам). Кожна роль має чітко визначений набір прав доступу до конкретних функцій системи, що відповідає принципу найменших привілеїв.

2.3 Інформаційна модель об'єкта та модель технічного стану

Інформаційна модель об'єкта є фундаментом будь-якої кіберфізичної системи, оскільки саме вона визначає, як фізична реальність відображається у цифровому контурі. Запропонована інформаційна модель побудована як орієнтований граф, у якому вершинами є сутності енергетичної інфраструктури (вводи, шафи розподілу, ДБЖ, акумуляторні масиви, ДГУ, кондиціонери, навантаження), а ребрами – зв'язки електроживлення, теплові зв'язки, зв'язки управління та пріоритети.

Формально інформаційна модель об'єкта описується кортежем:

$$M = \langle E, T, A, R, P, S, H \rangle, \tag{2.1}$$

де E – множина сутностей (entities) енергетичної інфраструктури;

T – класифікатор типів сутностей;

A – функція атрибутів сутностей;

R – множина відношень (relations) між сутностями;

P – функція пріоритетів навантаження;

S – функція технічного стану;

H – історія подій та вимірювань.

Класифікатор типів T включає такі основні класи: PowerInput (зовнішній ввід живлення), Switchgear (комутаційне обладнання), UPS (ДБЖ), BatteryBank (акумуляторний масив), BatteryCell (окрема комірка), Rectifier (випрямляч), Inverter (інвертор), ATS (автоматичне перемикання резерву), Generator (ДГУ), FuelTank (паливний бак), CoolingUnit (кондиціонер), EnvironmentSensor (датчик середовища), DoorSensor (датчик відкриття), FireSensor (пожежний датчик), Load (навантаження), PDU (блок розподілу). Кожен клас має свій набір обов'язкових та додаткових атрибутів.

Функція атрибутів A для сутності e ∈ E повертає словник значень: A(e) = {(attr1, val1), (attr2, val2), ..., (attrn, valn)}. Наприклад, для сутності класу BatteryBank обов'язковими атрибутами є: nominal_voltage (номінальна напруга), nominal_capacity (номінальна ємність), chemistry (тип хімії), manufacturer (виробник), installation_date (дата встановлення), cell_count (кількість комірок), location (місце розташування).

Множина відношень R включає чотири основні типи: feeds (живить), monitors (моніторить), controls (керує), thermally_coupled_with (термічно пов'язаний з). Перший тип формує граф електроживлення, що дозволяє виконувати трасування потоків енергії від джерела до споживача. Другий тип встановлює, який датчик або контролер моніторить параметри якої сутності. Третій тип описує, які сутності впливають на інші через керуючі сигнали. Четвертий тип описує теплові впливи, що дозволяє моделювати каскадні сценарії перегріву.

Функція пріоритетів P : Load → {Critical, High, Medium, Low} визначає рівень критичності навантаження. Критичні навантаження (ядрове мережеве обладнання, системи синхронізації) повинні живитися максимально довго навіть у кризових умовах. Високопріоритетні навантаження (допоміжне мережеве обладнання, системи безпеки) відключаються лише при глибокому виснаженні резерву. Середньопріоритетні (обладнання моніторингу, окремі сервери) відключаються в

умовах тривалого автономного режиму. Низькопріоритетні (освітлення, побутові пристрої) можуть відключатися за необхідності енергозбереження.

Особливо важливою частиною інформаційної моделі є модель технічного стану S. Для кожного критичного компонента вона обчислює інтегральний показник стану в діапазоні [0, 1], де 1 – ідеальний стан, а 0 – повна непридатність до експлуатації.

Для акумуляторного масиву модель стану включає чотири складники:

$$SBattery = w1 \cdot SoH + w2 \cdot TS + w3 \cdot CS + w4 \cdot AS, \qquad (2.2)$$

де SoH – стан здоров'я (State of Health) – відношення поточної максимальної ємності до номінальної;

TS (Temp Score) – оцінка температурного режиму експлуатації (1 при дотриманні робочого діапазону, лінійно зменшується при відхиленнях);

CS (Cycle Score) – оцінка ресурсу за кількістю циклів заряд-розряд;

AS (Age Score) – оцінка віку (зменшується від 1 до 0 за період номінального терміну служби);

$w1 \ldots w4$ – вагові коефіцієнти, сума яких дорівнює 1.

Експериментально визначені вагові коефіцієнти для LiFePO4 батарей: w1 = 0.40, w2 = 0.20, w3 = 0.25, w4 = 0.15.

Для прогнозування часу автономної роботи використовується емпірична залежність:

$$Tautonomy = (Cnom \cdot SoH \cdot TempF)/(Iload \cdot DerateF), \qquad (2.3)$$

де $Cnom$ – номінальна ємність батареї (Ah);

SoH – стан здоров'я;

$TempF$ – температурний коефіцієнт корекції ємності (для LiFePO4 від 0.65 при -20°C до 1.0 при +25°C);

$Iload$ – струм поточного навантаження (А);

$DerateF$ – коефіцієнт зменшення ефективної ємності при високих струмах розряду (для LiFePO4 близький до 1.05).

Для випрямлячів та ДБЖ модель стану обчислюється як середнє зважене показників ефективності, стабільності, кількості включень-вимкнень за період та років експлуатації. Для генераторних установок – як середнє показників успішних запусків (за останні 12 місяців), стабільності частоти й напруги при тестових запусках, рівня палива та своєчасності сервісних інтервалів.

На рисунку 2.3 представлено фрагмент інформаційної моделі для типового центру комутації.

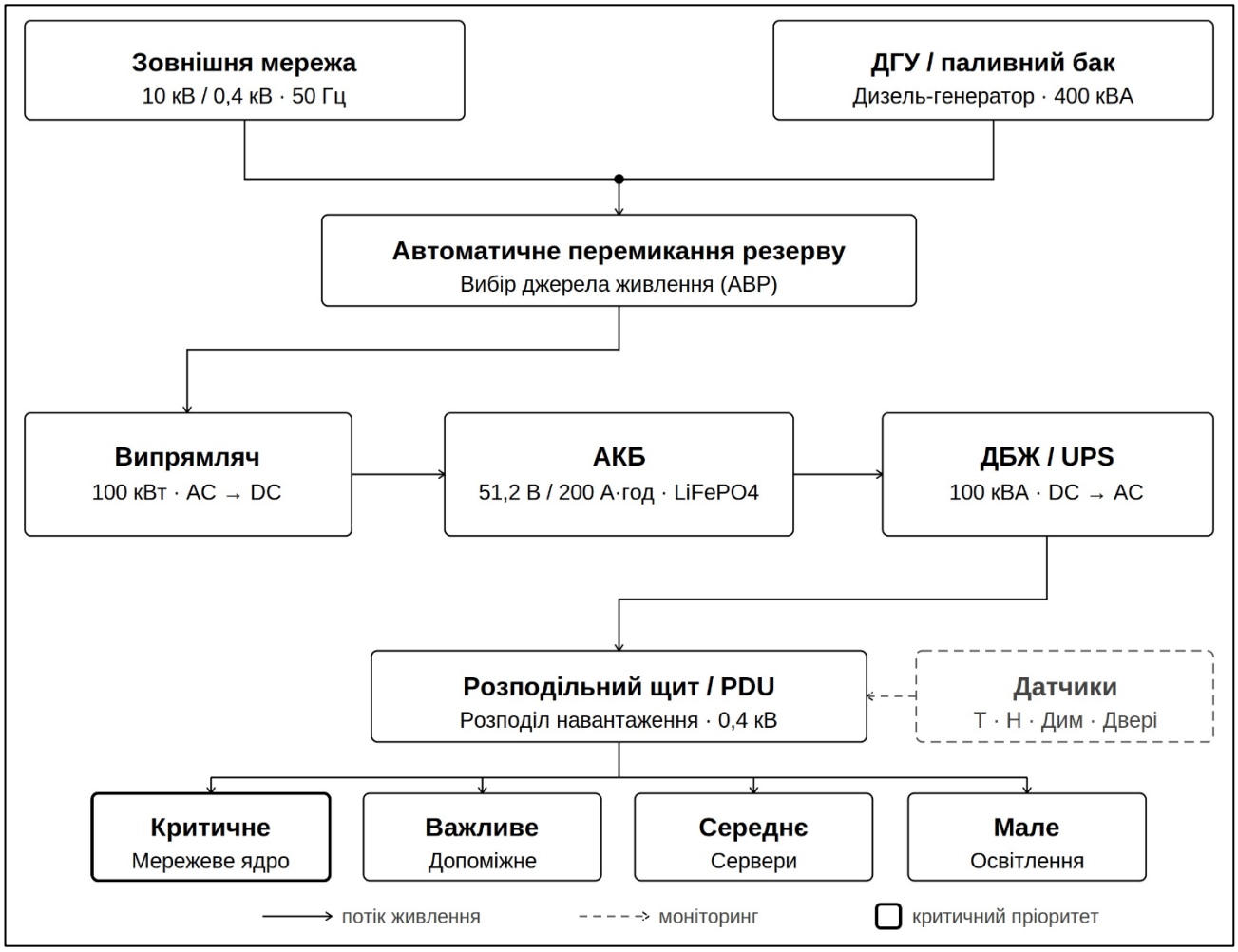


Рисунок 2.3 – Інформаційна модель об'єкта у вигляді орієнтованого графу

Вершини позначають сутності, ребра – відношення живлення (суцільні), моніторингу (пунктирні) та теплової взаємодії (точкові). Така візуалізація дозволяє оператору зрозуміти структуру об'єкта та виконати трасування потоків енергії при діагностуванні проблем.

Зведена характеристика складників моделі технічного стану наведена в таблиці 2.2.

Таблиця 2.2 – Параметри моделі технічного стану для основних класів обладнання

Клас обладнання	Параметри	Період оновлення	Ваги (за умовч.)
Акумуляторний масив (LiFePO4)	SoH, TempScore, CycleScore, AgeScore	1 хв	0.40, 0.20, 0.25, 0.15
Акумуляторний масив (VRLA)	SoH, TempScore, CycleScore, AgeScore	5 хв	0.30, 0.30, 0.20, 0.20
Випрямляч	Efficiency, OutputStability, OnOffCount, AgeScore	1 хв	0.30, 0.35, 0.15, 0.20
ДБЖ (UPS)	Efficiency, OutputStability, OnOffCount, AgeScore	30 с	0.30, 0.40, 0.10, 0.20
Дизель-генератор (ДГУ)	TestStartScore, FreqStability, FuelLevel, ServiceScore	Тест 1 раз/тиждень	0.40, 0.20, 0.20, 0.20
Кондиціонер	TempControl, RuntimeRatio, FilterScore, AgeScore	5 хв	0.40, 0.25, 0.15, 0.20

Запропонована інформаційна модель є основою для всіх подальших обчислень у системі. Її формалізація дозволяє однозначно описувати об'єкти різного масштабу – від невеликого комутаційного майданчика до великого центру обробки даних. При цьому структура моделі залишається незмінною, змінюються лише конкретні значення атрибутів та склад вершин і ребер. Це забезпечує

універсальність моделі та її масштабованість для впровадження на множині об'єктів оператора зв'язку.

Інтегральний показник технічного стану всього об'єкта обчислюється як зважена сума показників його критичних компонентів з урахуванням їх пріоритетів:

$$SObject = \Sigma(wi \cdot Si)/\Sigma wi, i \in CriticalComponents, \quad (2.4)$$

де Si – показник стану і-го компонента;

wi – ваговий коефіцієнт залежно від пріоритету компонента (Critical = 4, High = 3, Medium = 2, Low = 1).

Особлива увага в інформаційній моделі приділена темпоральним аспектам. Кожна сутність має історію станів, що зберігається у функції H. Історія включає не лише параметри телеметрії, а й події (alarms, transitions, operator actions), які впливали на сутність. Це дозволяє виконувати ретроспективний аналіз: як сутність функціонувала у певний момент часу, які події передували відмові, як змінювалися показники стану.

Для забезпечення цілісності даних в моделі реалізована система валідації консистентності. Наприклад, якщо для акумуляторного масиву задано номінальну напругу 51.2 В (16 послідовних LiFePO4 комірок по 3.2 В), а телеметрія повідомляє про напругу 12 В, система фіксує неконсистентність та позначає дані як ненадійні. Аналогічна перевірка виконується для інших параметрів: струм не може бути більший за номінальний; температура не може стрибкоподібно змінюватися більш ніж на 5°C за хвилину; сума струмів по гілках не може перевищувати загальний струм масиву. Така валідація захищає систему від несправних сенсорів та помилкових даних.

2.4 Метод адаптивного управління енергозабезпеченням ЦКТМ

Запропонований метод адаптивного управління енергозабезпеченням центрів комутації телекомунікаційних мереж є логічним продовженням розробленої концепції та структурно-функціональної моделі. Метод поєднує елементи реактивного, проактивного та предиктивного управління в єдиний контур та реалізує взаємодію між трьома рівнями (локальним, об'єктним, централізованим). На відміну від відомих методів, запропонований підхід забезпечує перехід від реактивного до проактивного режиму експлуатації енергетичної інфраструктури за рахунок інтеграції предиктивної оцінки технічного стану обладнання та сценарного реагування з урахуванням пріоритетів навантаження.

Метод складається з шести взаємопов'язаних етапів:

1) збір та нормалізація телеметрії з гетерогенних джерел (датчики, контролери, BMS, ДБЖ, ДГУ, кондиціонери) у єдиний інформаційний простір на основі MQTT-брокера;

2) обчислення похідних показників та оновлення моделі технічного стану кожного критичного компонента згідно з формулами (2.2)–(2.4);

3) класифікація поточного стану об'єкта на основі правил переходу між станами;

4) активація відповідних сценаріїв реагування залежно від поточного стану та виявлених подій;

5) виконання керуючих впливів та сповіщення оператора з поясненням причин рішення;

6) накопичення історії та повторний цикл оптимізації параметрів методу на основі аналізу post-mortem інцидентів.

Правила переходу між станами формалізовані у вигляді логічних виразів. Наприклад, перехід зі стану Normal у стан Degraded відбувається при виконанні однієї з умов: SObject < 0.85; відмова одного з резервних компонентів (один з двох вводів, один з двох ДБЖ); прогноз автономії менше 30 хв; температура у будь-якій критичній зоні перевищує 35°C; Маса логічних виразів реалізована як

декларативна модель правил, що дозволяє адаптувати систему під специфічні вимоги майданчика без зміни коду.

Класифікація стану об'єкта виконується на основі функції переходу:

$$State(t+1) = f(State(t), SObject(t+1), Events(t, t+1), Cnt), \qquad (2.5)$$

де $State(t)$ – поточний стан об'єкта;

$SObject$ – інтегральний показник технічного стану;

$Events$ – множина подій, що відбулися за період [t, t+1];

Cnt – контекстна інформація (день/ніч, режим обслуговування, плановані роботи).

Сценарії реагування є основним механізмом виконання керуючих впливів. Для кожного типового сценарію (зникнення зовнішнього живлення, відмова ДБЖ, перегрів, відмова кондиціонера, критичне зниження автономії, спрацьовування пожежного датчика) формалізовано: умови активації, послідовність дій, критерії безпечного виконання, точки прийняття рішень оператором, способи журналювання. Кожен сценарій містить щонайменше один точку валідації, де перевіряється, що дія не приведе до додаткового ризику.

Особливою частиною методу є алгоритм пріоритизації навантаження при тривалому автономному режимі. Якщо час автономії скорочується нижче порогового значення (за замовчуванням 30 хв), система виконує ступеневе відключення некритичних навантажень за такою послідовністю: спочатку відключаються Low-priority навантаження, через 5 хв – Medium-priority (якщо ситуація не покращилась), через 10 хв – частина High-priority. Critical навантаження не відключаються автоматично взагалі, їх відключення можливе лише за командою оператора з підтвердженням підвищеного рівня доступу.

Окремий блок методу пов'язаний з координацією енергетичного та кліматичного контурів. На відміну від класичних рішень, де ці контури функціонують незалежно, у запропонованому методі вони взаємодіють через

єдиний логічний шар прийняття рішень. Зокрема, при виявленні зростання теплового навантаження у машинному залі система може автоматично перерозподілити обчислювальне навантаження між фізичними стійками, понизити частоту окремих компонентів, активувати додаткові секції охолодження або, у разі неможливості інших дій, плавно зменшити продуктивність некритичних сервісів. Така координація дозволяє уникати каскадних ефектів, при яких енергетична подія викликає кліматичну кризу і навпаки.

Метод також передбачає модуль валідації резерву, що періодично перевіряє реальну готовність резервних ресурсів до використання. Це включає тестові запуски ДГУ з вимірюванням ключових параметрів (час запуску, стабільність частоти, якість напруги, рівень вібрації), часткові розряди акумуляторних масивів для оцінки фактичної ємності, перевірку справності системи АВР шляхом імітації подій переключення. Результати цих перевірок інтегруються у модель технічного стану і впливають на прогнозовані показники автономії та доступності.

Запропонований метод адаптивного управління формалізовано представлений у таблиці 2.3, що зведено описує входи, виходи, процеси та результати кожного етапу.

Таблиця 2.3 – Етапи методу адаптивного управління

Етап	Вхід	Процес	Вихід
1	2	3	4
1. Збір телеметрії	Сигнали з датчиків, контролерів, BMS	Перетворення протоколів, нормалізація даних	Уніфіковані повідомлення MQTT
2. Оновлення моделі стану	Уніфікована телеметрія	Обчислення SoH, TempScore, CycleScore, AgeScore	Інтегральний показник Si та SObject

Кінець таблиці 2.3

1	2	3	4
3. Класифікація стану об'єкта	SObject, події, контекст	Застосування правил переходу між станами	Поточний стан об'єкта
4. Активація сценаріїв	Стан, події	Вибір застосовних сценаріїв за матрицею	Список активних сценаріїв
5. Виконання дій	Активні сценарії	Відправка команд, сповіщення оператора	Зміна стану обладнання, інциденти
6. Накопичення історії	Усі дані з попередніх етапів	Запис у TSDB, post-mortem аналіз	Оновлені параметри методу

Ще одним важливим аспектом методу є підтримка ручного втручання оператора. Усі автоматичні дії можуть бути тимчасово заблоковані оператором з відповідним рівнем доступу. Однак така блокування не є безумовною: для кожного сценарію визначені умови, при яких автоматика повинна відновити свою роботу навіть проти явної команди оператора – це стосується ситуацій безпосередньої загрози життю (пожежа, газова небезпека) або повної втрати критичного сервісу (зникнення живлення на всіх вводах одночасно) [23, 30].

Особливістю методу є замкнутий контур навчання: post-mortem аналіз інцидентів дозволяє оптимізувати порогові значення, вагові коефіцієнти моделі стану та правила переходу між станами. Це робить систему адаптивною – її ефективність поліпшується з часом експлуатації.

Перевагами запропонованого методу є: повне покриття всіх стадій управління (від збору даних до виконання впливу); інтегрована предиктивна аналітика; адаптивність за рахунок контуру навчання; пріоритизація навантажень для забезпечення живучості критичного ядра; пояснюваність рішень для когнітивної підтримки оператора. Ці властивості разом забезпечують перехід від реактивного до проактивного режиму експлуатації, що становить основу заявленої наукової новизни.

Особливо слід наголосити на адаптивній природі методу. На відміну від статичних реактивних систем, де всі правила та пороги встановлюються одноразово на етапі впровадження, запропонований метод передбачає безперервне налаштування параметрів на основі досвіду експлуатації. Це означає, що після кожного значущого інциденту система автоматично пропонує оператору переглянути відповідні правила та пороги. Якщо інцидент був успішно відпрацьований, поточні параметри підтверджуються; якщо ж виникли проблеми (хибні спрацьовування, пропущені події, неоптимальні рішення), параметри коригуються. Така зворотна петля забезпечує поступове покращення якості роботи системи з часом. Схема методу зображена на рисунку 2.4.

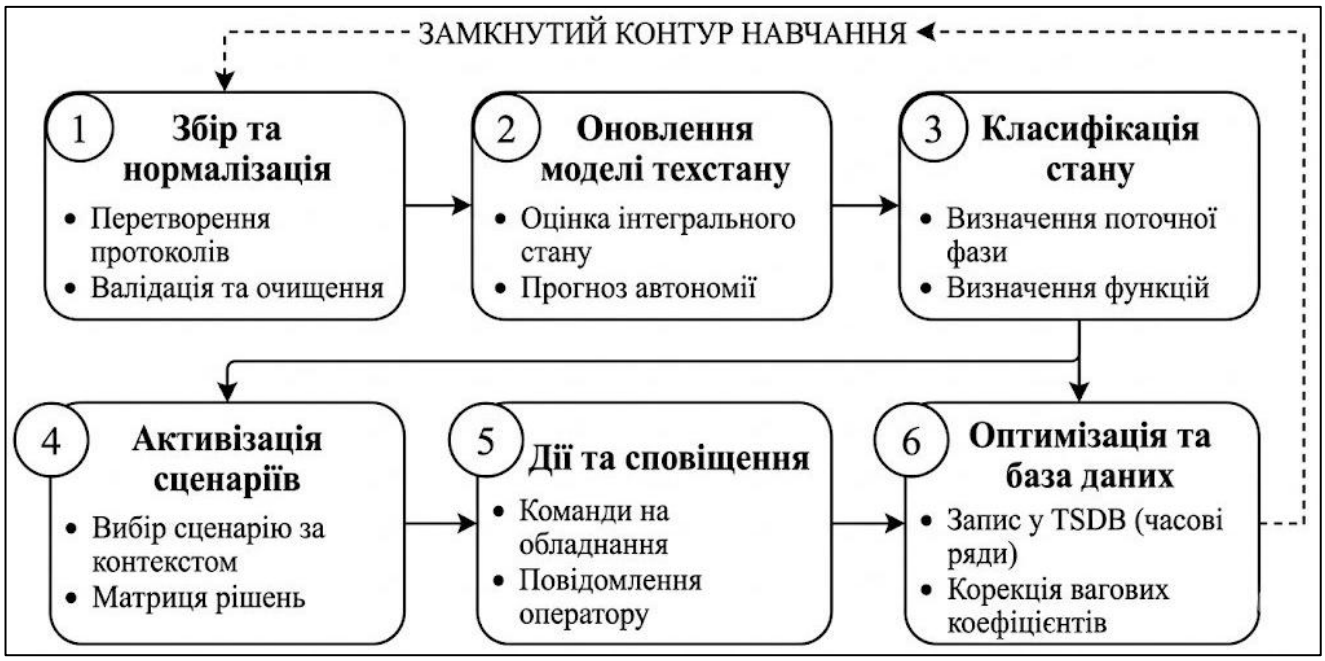


Рисунок 2.4 – Узагальнена схема методу адаптивного управління енергозабезпеченням ЦКТМ

Ще одним важливим аспектом методу є врахування контексту експлуатації. Контекст включає: час доби (день/ніч, робочі/неробочі години); день тижня (робочий/вихідний); сезон (літо/зима); планові роботи (заплановане технічне обслуговування); зовнішні події (попередження про відключення електроенергії, оголошення повітряної тривоги). Контекст впливає на класифікацію стану та вибір

сценаріїв реагування. Наприклад, у разі відключення зовнішнього живлення вночі система може більш агресивно знижувати навантаження, оскільки персонал недоступний для оперативного втручання, а у робочий час – відкласти ступеневе відключення з очікуванням рішення оператора.

Метод містить також механізм врахування невизначеності у даних. Якщо телеметрія від певного датчика позначена як BAD або UNCERTAIN (через втрату зв'язку, несправність або підозрілі значення), модель технічного стану обчислюється з відповідним зниженням рівня довіри. У такому випадку система може звернутися до резервних джерел даних або застосувати інтерполяцію на основі історичних значень. У граничному випадку, коли критичні дані недоступні, система переходить у консервативний режим, приймаючи рішення на основі найгіршого можливого сценарію. Таке управління невизначеністю критично важливе для систем критичної інфраструктури.

Методологічно запропонований метод відповідає принципам робастного управління (robust control) – здатності системи зберігати працездатність та якість управління в умовах збурень, неточних моделей, відмов окремих компонентів. Робастність забезпечується кількома механізмами: багаторівневою ієрархією з автономним функціонуванням кожного рівня; декларативними правилами, що адаптуються до особливостей об'єкта; врахуванням невизначеності у даних; контуром навчання на основі досвіду; консервативним fallback-режимом при критичних обмеженнях. Усе це робить запропонований метод придатним для впровадження на реальних об'єктах телекомунікаційної інфраструктури [22, 23, 30].

Описаний метод також включає механізми керування конфліктами між сценаріями. У реальній експлуатації часто виникають ситуації, коли декілька сценаріїв одночасно претендують на виконання різних дій, які можуть конфліктувати між собою. Наприклад, сценарій балансування теплового навантаження може намагатися ввімкнути додатковий кондиціонер, тоді як сценарій економії енергії при автономному режимі рекомендує його вимкнути. Для розв'язання таких конфліктів метод використовує матрицю пріоритетів, де

кожному сценарію присвоюється пріоритет, та логіку взаємного блокування несумісних дій. Сценарії безпеки (наприклад, реакція на пожежу) завжди мають найвищий пріоритет, незалежно від інших активних сценаріїв.

Метод включає також підсистему оптимізації параметрів на основі історичних даних. Періодично (раз на тиждень) виконується аналіз ефективності виконаних сценаріїв: які з них спрацьовували коректно, які давали хибні позитивні результати, які пропускали реальні події. На основі цього аналізу автоматично формуються рекомендації щодо коригування порогових значень, ваг та інших параметрів. Адміністратор системи переглядає ці рекомендації та приймає рішення про їх застосування. Такий підхід поєднує переваги автоматичного навчання з контролем людини над критичними змінами в системі, що відповідає кращим практикам розгортання ML-систем у критичній інфраструктурі.

Особливе місце у методі займає механізм обробки часових серій телеметрії. Для виявлення тенденцій деградації використовуються методи декомпозиції рядів (сезонна декомпозиція, виявлення трендів). Для виявлення аномалій – статистичні методи (контрольні карти Шухарта, EWMA – Exponentially Weighted Moving Average) та методи машинного навчання (автоенкодери на основі рекурентних нейронних мереж). Комбінація різних методів дозволяє ефективно виявляти як короткотривалі аномалії (раптові відхилення), так і довготривалі тенденції (повільна деградація). Це критично важливо для предиктивного обслуговування, де проблема може розвиватися протягом місяців перед переходом у критичний стан.

2.5 Висновки

У другому розділі кваліфікаційної роботи отримано такі основні результати.

1. Розроблено концепцію кіберфізичної системи управління енергозабезпеченням центрів комутації телекомунікаційних мереж, що базується на восьми основних положеннях: інтеграція трьох взаємодіючих площин об'єкта; ієрархічна архітектура управління; подієво-станове управління; предиктивна оцінка технічного стану; координація енергетичного та кліматичного контурів;

модульність та відкритість інтеграції; багаторівнева кібербезпека; підтримка експлуатаційного персоналу.

2. Розроблено структурно-функціональну модель кіберфізичної системи у вигляді ієрархічної структури з трьох рівнів (локального, об'єктного, централізованого) з чітко визначеними функціями кожного компонента та інформаційними зв'язками між ними. Модель забезпечує автономне функціонування кожного рівня при втраті зв'язку з вищими рівнями, що є критичним для систем критичної інфраструктури.

3. Розроблено інформаційну модель об'єкта у вигляді орієнтованого графу $M = \langle E, T, A, R, P, S, H \rangle$, що формалізує сутності енергетичної інфраструктури, їхні атрибути, відношення електроживлення, моніторингу, керування та теплової взаємодії, а також пріоритети навантаження та технічний стан.

4. Розроблено модель технічного стану, що для кожного критичного компонента обчислює інтегральний показник у діапазоні [0, 1] на основі багатофакторного аналізу телеметрії. Для акумуляторного масиву модель включає чотири складники: SoH, TempScore, CycleScore, AgeScore. Для прогнозування часу автономії запропоновано емпіричну залежність з урахуванням температурного коефіцієнта та ефекту Пейкерта.

5. Розроблено метод адаптивного управління енергозабезпеченням ЦКТМ, що складається з шести взаємопов'язаних етапів: збір та нормалізація телеметрії; оновлення моделі технічного стану; класифікація стану об'єкта; активація сценаріїв реагування; виконання керуючих впливів; накопичення історії. Метод забезпечує перехід від реактивного до проактивного режиму експлуатації за рахунок інтеграції предиктивної аналітики та сценарного реагування з урахуванням пріоритетів навантаження.

Розроблені модель та метод складають теоретичну основу запропонованої кіберфізичної системи. У наступному розділі буде розглянуто алгоритми реалізації методу, вимоги до програмного забезпечення та архітектурне проєктування.

3 АЛГОРИТМ ТА ТЕХНОЛОГІЯ КІБЕРФІЗИЧНОЇ СИСТЕМИ УПРАВЛІННЯ ЕНЕРГОЗАБЕЗПЕЧЕННЯМ

3.1 Алгоритм роботи кіберфізичної системи управління

Алгоритм роботи кіберфізичної системи реалізує метод адаптивного управління, представлений у розділі 2.4, у вигляді конкретної послідовності обчислювальних кроків. Алгоритм має ієрархічну структуру, що відповідає трирівневій архітектурі системи. На локальному рівні виконуються базові алгоритми збору телеметрії та аварійного реагування з гарантованим часом виконання. На об'єктному рівні виконуються алгоритми нормалізації даних, обчислення моделі стану та активації сценаріїв реагування. На централізованому рівні – алгоритми глибокої аналітики, прогнозування тенденцій та оптимізації параметрів.

Загальний алгоритм функціонування системи можна описати як циклічний процес з фіксованим періодом виконання. Базовий період становить 1 хвилину – саме з такою частотою виконується повний цикл збору телеметрії, оновлення моделі стану та класифікації стану об'єкта. Однак критичні події обробляються поза основним циклом – у момент їх настання – через подієво-керовану частину системи.

Основний цикл алгоритму функціонування системи включає такі кроки:

1) початок циклу: запис мітки часу t;

2) послідовне опитування всіх локальних контролерів через відповідні протоколи (Modbus TCP/RTU, SNMP, OPC UA), для кожного контролера виконується серія запитів параметрів з урахуванням встановлених таймаутів;

3) нормалізація отриманих даних до уніфікованого формату, кожна телеметрична точка отримує: ідентифікатор сутності, тип сутності, ім'я атрибута, числове значення, мітку часу, ідентифікатор джерела та позначку якості;

4) публікація нормалізованих даних до брокера повідомлень MQTT за відповідними топіками, топіки організовані ієрархічно за принципом site/<site_id>/<entity_type>/<entity_id>/<attribute>;

5) обчислення похідних показників та оновлення моделі технічного стану, для кожного критичного компонента обчислюється інтегральний показник Si;

6) обчислення інтегрального показника технічного стану об'єкта SObject як зваженої суми показників його критичних компонентів;

7) виявлення нових подій шляхом порівняння поточних значень з попередніми, подіями вважаються перетин порогів значущих параметрів, перехід контролерів у/з стану доступності, зміна стану дискретних сигналів, спрацьовування захисних блокувань;

8) класифікація поточного стану об'єкта на основі правил переходу між станами;

9) якщо поточний стан змінився, активація відповідних сценаріїв реагування, кожен сценарій перевіряється на можливість виконання та виконується покроково з валідацією результату кожного кроку;

10) запис підсумкової інформації про цикл (стан, події, виконані сценарії, керуючі впливи) у локальну базу часових рядів та централізовану базу для довгострокового зберігання;

11) очікування до наступного циклу (1 хвилина від початку поточного) і перехід до першого кроку.

Окремо реалізовано подієво-керовану частину алгоритму, що обробляє критичні події в реальному часі поза основним циклом. Критичні події включають: спрацьовування захисних блокувань на локальному рівні; падіння напруги нижче допустимого порога; перевищення граничної температури в критичних зонах; спрацьовування пожежного або газового датчика. Для таких подій час реакції не повинен перевищувати 100 мс, що забезпечується високопріоритетним обробником подій із низьким латентним часом.

Блок-схема алгоритму наведена у додатку Б

Алгоритм оцінки стану акумуляторного масиву на основі формули (2.2) представлений нижче у вигляді псевдокоду.

Відношення поточної ємності до номінальної:

measured_capacity = estimate_capacity_from_discharge(history)

soh = measured_capacity / battery.nominal_capacity

Оцінка температурного режиму:

avg_temp = mean(telemetry.temperatures)

if 15 <= avg_temp <= 30:

temp_score = 1.0

elif avg_temp < 15:

temp_score = max(0, 1.0 - (15 - avg_temp) * 0.05)

else:

temp_score = max(0, 1.0 - (avg_temp - 30) * 0.04)

Оцінка ресурсу за кількістю циклів:

cycles_used = count_full_cycles(history)

cycle_score = max(0, 1 - cycles_used / battery.max_cycles)

Оцінка віку:

age_years = (now() - battery.installation_date).years

age_score = max(0, 1 - age_years / battery.expected_lifetime)

Інтегральний показник:

weights = battery.health_weights # [0.40, 0.20, 0.25, 0.15]

score = (weights[0] * soh + weights[1] * temp_score +

weights[2] * cycle_score + weights[3] * age_score)

return score

Алгоритм прогнозування часу автономної роботи на основі формули (2.3) реалізований далі.

Корекція ємності за станом здоров'я

effective_capacity = battery.nominal_capacity * battery.SoH

Температурний коефіцієнт (для LiFePO4):

avg_temp = mean(telemetry.temperatures)

temp_factor = lifepo4_temp_factor(avg_temp)

Лінійна апроксимація: 0.65 при -20°C, 1.0 при +25°C, 1.0 вище:

Коефіцієнт Пейкерта:

derate = peukert_factor(current_load_A, battery.nominal_capacity)

```
Час автономії в годинах:
autonomy_hours = (effective_capacity * temp_factor) / (
current_load_A * derate)
return autonomy_hours
```

Принциповою особливістю запропонованого алгоритму є розмежування синхронного та асинхронного контурів. Синхронний контур (основний цикл) забезпечує регулярне оновлення повної моделі стану, а асинхронний контур реагує на критичні події з мінімальною затримкою. Така архітектура відповідає вимогам стандартів NIST SP 800-82 та ISA/IEC 62443 щодо детермінованої поведінки систем технологічного управління в реальному часі [23, 30].

Окремий механізм алгоритму присвячений обробці затримок та помилок збору телеметрії. Якщо при опитуванні контролера виникає тайм-аут (типове значення – 2 секунди для Modbus TCP, 1 секунда для SNMP), система не повторює запит одразу. Натомість запис у TSDB виконується з позначенням якості UNCERTAIN. Якщо протягом N послідовних циклів контролер не відповідає, система генерує подію controller_unavailable і підвищує пріоритет цієї події в інцидент-менеджменті.

Алгоритм виявлення подій реалізований за принципом differential analysis – порівняння поточного стану з попереднім. Для кожного параметра, що моніториться, зберігається попереднє значення та метадані: timestamp попереднього вимірювання, кількість послідовних значень в аналогічному діапазоні. Подія генерується у таких випадках: значення перетнуло поріг (вверх або вниз); значення стрибкоподібно змінилося (delta більше встановленого порогу між сусідніми вимірюваннями); змінився дискретний стан (бінарний сигнал); параметр перейшов у режим UNCERTAIN/BAD або повернувся з нього. Алгоритм уникає генерації дублюючих подій – якщо стан стабільно знаходиться поза порогом, нова подія не генерується доти, доки параметр не повернеться в норму.

Алгоритм активації сценаріїв враховує можливість одночасного спрацьовування кількох сценаріїв у відповідь на одну подію або групу пов'язаних

подій. У такому випадку сценарії виконуються у порядку пріоритету, який визначається критичністю реакції: спочатку виконуються блокувальні сценарії (відключення некритичних навантажень при перевантаженні), потім – активні (запуск ДГУ, перехід на резерв), потім – інформаційні (сповіщення оператора, запис у журнал). При наявності конфліктів між сценаріями активується механізм conflict resolution: кожен сценарій оголошує свої preconditions та effects, і система перевіряє, чи можуть сценарії виконуватися одночасно без створення небезпечних станів.

3.2 Розроблення вимог до програмного забезпечення

Розроблення вимог до програмного забезпечення кіберфізичної системи виконано відповідно до методології, заснованої на стандарті IEEE 830 та практиках Agile-розробки. Вимоги розділені на функціональні (що система повинна робити) та нефункціональні (як саме повинна це робити – якісні атрибути).

Функціональні вимоги об'єднані у такі основні групи: збір телеметрії, нормалізація даних, обчислення моделі стану, класифікація стану об'єкта, виявлення подій, активація сценаріїв, виконання керуючих впливів, журналювання, людино-машинний інтерфейс, адміністрування, інтеграція з зовнішніми системами.

Перелік ключових функціональних вимог наведений у таблиці 3.1.

Таблиця 3.1 – Функціональні вимоги до програмного забезпечення

ID	Категорія	Вимога
1	2	3
FR-01	Збір телеметрії	Система повинна підтримувати протоколи Modbus RTU/TCP, SNMP v2c/v3, MQTT v3.1.1/v5.0, OPC UA

Продовження таблиці 3.1

1	2	3
FR-02	Збір телеметрії	Період опитування телеметрії повинен налаштовуватися окремо для кожного джерела (від 1 с до 1 год)
FR-03	Нормалізація	Усі телеметричні точки повинні отримувати уніфіковані атрибути (id, type, value, timestamp, quality)
FR-04	Модель стану	Система повинна обчислювати інтегральний показник стану для кожного критичного компонента
FR-05	Модель стану	Параметри моделі стану (вагові коефіцієнти, пороги) повинні налаштовуватися без зміни коду
FR-06	Класифікація стану	Система повинна підтримувати щонайменше 6 станів об'єкта: Normal, Degraded, Pre-emergency, Emergency, Recovery, Maintenance
FR-07	Класифікація стану	Правила переходу між станами повинні задаватися декларативно (DSL або YAML)
FR-08	Виявлення подій	Система повинна виявляти події перетину порогів, зміни дискретних станів, недоступності контролерів
FR-09	Сценарії	Система повинна підтримувати щонайменше 12 типових сценаріїв реагування
FR-10	Сценарії	Кожен сценарій повинен мати точки валідації для безпечного виконання
FR-11	Керуючі впливи	Команди керування повинні передаватися з повним аудитом (хто, коли, що, чому)
FR-12	Журналювання	Журнал подій повинен зберігатися щонайменше 1 рік для критичних подій, 90 днів для звичайних

Кінець таблиці 3.1

1	2	3
FR-13	ЛМІ	Інтерфейс повинен бути доступним з браузера (responsive design) для мобільних пристроїв
FR-14	ЛМІ	Дашборди повинні відображати: загальний стан об'єкта, граф інфраструктури, активні події, тренди показників
FR-15	Адміністрування	Система повинна підтримувати рольовий доступ (Operator, Engineer, Administrator, Auditor)
FR-16	Інтеграція	Система повинна підтримувати експорт даних через REST API та інтеграцію з SNMP-trapservers

Нефункціональні вимоги визначають якісні характеристики системи. Найважливішими з них є вимоги до надійності, продуктивності, масштабованості, безпеки та зручності експлуатації.

Перелік ключових нефункціональних вимог наведений у таблиці 3.2.

Таблиця 3.2 – Нефункціональні вимоги до програмного забезпечення

ID	Категорія	Вимога
1	2	3
NFR-01	Надійність	Доступність системи повинна бути не нижче 99.5% (MTTR ≤ 4 год, плановий downtime ≤ 8 год/рік)
NFR-02	Надійність	Об'єктний рівень повинен функціонувати автономно при втраті зв'язку з централізованим рівнем
NFR-03	Продуктивність	Час реакції на критичні події не повинен перевищувати 100 мс
NFR-04	Продуктивність	Час повного циклу основного алгоритму не повинен перевищувати 1 хв

Кінець таблиці 3.1

1	2	3
NFR-05	Продуктивність	Веб-інтерфейс повинен завантажуватися за час менше 3 секунд
NFR-06	Масштабованість	Система повинна підтримувати щонайменше 1000 телеметричних точок на об'єкт
NFR-07	Масштабованість	Централізований рівень повинен підтримувати щонайменше 100 об'єктів одночасно
NFR-08	Безпека	Усі канали зв'язку між рівнями повинні бути шифровані (mTLS, VPN)
NFR-09	Безпека	Аутентифікація користувачів повинна включати щонайменше 2 фактори (пароль + OTP) для адміністраторів
NFR-10	Безпека	Журнал аудиту повинен бути захищений від модифікації (append-only)
NFR-11	Зручність	Інтерфейс оператора повинен бути локалізований українською мовою
NFR-12	Зручність	Кожна аварійна подія повинна супроводжуватися поясненням причини у зрозумілій формі

Окремою категорією є вимоги, продиктовані стандартами критичної інформаційної інфраструктури. Згідно з NIST SP 800-82 [23] та ISA/IEC 62443 [30], система повинна підтримувати сегментацію мереж, контроль цілісності конфігурації, захищене оновлення прошивок, моніторинг кіберподій та автоматичне сповіщення про інциденти. Згідно з рекомендаціями ENISA для smart grid [31, 32], повинні бути реалізовані механізми виявлення нештатних команд керування, що могли б свідчити про компрометацію.

Окремий блок вимог стосується інтеграції зі стандартами телекомунікаційного середовища. Система повинна сумісно обробляти дані з обладнання, що відповідає ETSI EN 300 132 [24, 25] (інтерфейси живлення -48 В,

до 400 В DC), ITU-T L.1200/L.1300 [26, 27] (вимоги до зелених датацентрів), EN 50600 [7, 28, 46, 47] (інфраструктура датацентрів). Метрики енергоефективності повинні обчислюватися згідно з ETSI EN 303 472 та ETSI ES 203 228 [33, 34].

Окремо слід зупинитися на вимогах до підтримки відмовостійкості. Для систем критичної інфраструктури недостатньо мати високу доступність – система повинна продовжувати працювати навіть в умовах часткової деградації. Сформульовано такі конкретні вимоги: при відмові одного з мікросервісів решта повинна продовжувати працювати з попередженням користувача про обмежений функціонал; при втраті з'єднання з центральним рівнем об'єктний рівень повинен функціонувати автономно щонайменше 72 години; при повному виключенні живлення edge-сервера після відновлення система повинна автоматично відновити роботу без втрати накопичених даних протягом 30 секунд; при пошкодженні бази даних повинна бути можливість автоматичного відновлення з резервної копії за час менше 1 години.

Особливим типом вимог є вимоги до підтримки життєвого циклу системи. Розроблюване програмне забезпечення повинне підтримувати: rolling updates – оновлення без зупинки сервісу за рахунок blue-green deployment; semantic versioning – явне позначення несумісних змін; backward compatibility API – підтримка попередніх версій API щонайменше 12 місяців після випуску нової; automated migrations – автоматизоване оновлення схем БД при зміні версій; configuration as code – зберігання всієї конфігурації у Git-репозиторії з можливістю rollback. Ці вимоги забезпечують можливість тривалої експлуатації системи без накопичення технічного боргу.

Окрема група вимог формулює очікування щодо локалізації та культурної адаптації системи. Інтерфейс оператора повинен підтримувати щонайменше дві мови – українську (основна) та англійську (для міжнародних майданчиків); формати дати та часу повинні відповідати регіональним стандартам; одиниці виміру повинні адаптуватися до локальних практик (наприклад, температура у °C для України, у °F для США); повідомлення про помилки повинні бути зрозумілими для технічного персоналу без необхідності звертатися до довідкової документації.

Локалізація реалізується через стандартний механізм internationalization з винесенням всіх текстів у resource bundle.

3.3 Архітектурне проєктування програмного забезпечення

Архітектура програмного забезпечення розроблена з урахуванням ієрархічної структури системи та функціональних вимог, сформульованих у попередньому підрозділі. Архітектурний стиль обрано як комбінацію event-driven мікросервісної архітектури (на об'єктному та централізованому рівнях) та модульної архітектури з єдиним процесом (на локальному рівні – для забезпечення детермінованості та низьких затримок).

На рівні Presentation реалізовано: веб-додаток для оператора (SPA на React); API Gateway для уніфікованого доступу до сервісів; Mobile App (PWA для оперативної роботи на майданчику). На рівні Application реалізовано основну бізнес-логіку у вигляді мікросервісів: Telemetry Service (збір та нормалізація телеметрії); State Engine (обчислення моделі стану та класифікація); Event Correlator (виявлення та об'єднання подій); Scenario Engine (виконання сценаріїв реагування); Notification Service (сповіщення оператора через email, SMS, Telegram); Analytics Service (глибока аналітика, ML-моделі).

На рівні Domain зосереджено сутності предметної області: Entity, EntityType, EntityRelation, TelemetryPoint, Event, Incident, State, Scenario, ScenarioRun, User, Role, Permission, AuditLog. Ці сутності визначені незалежно від конкретної інфраструктури і забезпечують стабільність бізнес-логіки при заміні зовнішніх компонентів. На рівні Infrastructure реалізовано адаптери до конкретних протоколів (Modbus, SNMP, MQTT), сховищ (TimescaleDB, PostgreSQL, Redis) та зовнішніх сервісів.

Загальна архітектура системи представлена у вигляді чотирьох архітектурних шарів: Presentation (рівень представлення), Application (рівень бізнес-логіки), Domain (рівень предметної області, моделей), Infrastructure (рівень інтеграції з

зовнішніми системами та зберігання даних). Архітектурна діаграма зображена на рисунку 3.1

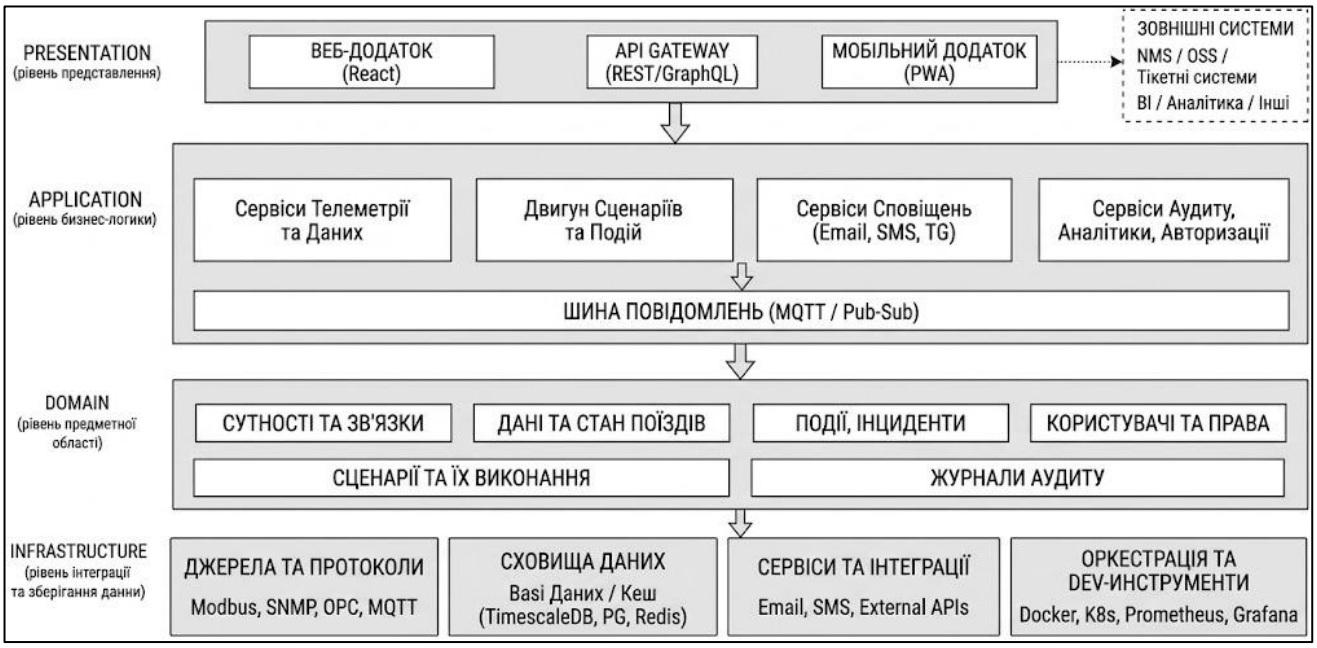


Рисунок 3.1 – Архітектурна діаграма кіберфізичної системи

Технологічний стек обрано з урахуванням вимог до надійності, продуктивності, легкості підтримки та доступності open source-компонентів. Основні технологічні рішення наведені у таблиці 3.3.

Таблиця 3.3 – Технологічний стек програмного забезпечення

Компонент	Технологія	Обгрунтування вибору
1	2	3
Backend (мікросервіси)	Python 3.12, FastAPI	Швидка розробка, екосистема для аналітики, ML-бібліотеки
Frontend (веб-додаток)	React 18, TypeScript	Стабільність, велика спільнота, типобезпека
БД часових рядів	TimescaleDB	Розширення PostgreSQL, оптимізоване для метрик
Реляційна БД	PostgreSQL 15	Зрілість, підтримка JSONB, надійність

Кінець таблиці 3.3

1	2	3
Кеш та черга	Redis 7	Висока продуктивність, простота, pub/sub
Брокер повідомлень	Eclipse Mosquitto MQTT v5	Open source, стандартний для IoT, легкий
Локальний контейнер	Docker, Docker Compose	Стандартизоване розгортання, ізоляція
Централізований кластер	Kubernetes	Самовідновлення, масштабування, оркестрація
Моніторинг системи	Prometheus, Grafana	Стандарт SRE-практик, інтеграція з K8s
Реверс-проксі	Nginx, Traefik	Безпека, маршрутизація, TLS-термінація
Аутентифікація	Keycloak (OAuth2/OIDC)	Open source, ролі, MFA, SSO
Журналювання	Fluent Bit, Loki	Легке збирання, зберігання структурованих логів

Кіберфізична система реалізована з використанням мікросервісної архітектури, що дозволяє масштабувати окремі компоненти незалежно та забезпечує високу відмовостійкість.

Основні мікросервіси та їхня відповідальність наведені у таблиці 3.4.

Таблиця 3.4 – Мікросервіси кіберфізичної системи

Сервіс	Відповідальність	Інтерфейси
1	2	3
Telemetry Service	Збір та нормалізація телеметрії з усіх джерел	Modbus, SNMP, OPC UA → MQTT publish

Кінець таблиці 3.4

1	2	3
State Engine	Обчислення моделі стану, класифікація стану об'єкта	MQTT subscribe → MQTT publish, REST API
Event Correlator	Виявлення та об'єднання подій у інциденти	MQTT subscribe → MQTT publish, REST API
Scenario Engine	Виконання сценаріїв реагування	MQTT subscribe, REST API → Modbus write, SNMP set
Notification Service	Сповіщення оператора через email, SMS, Telegram	MQTT subscribe → SMTP, HTTP, Telegram API
Analytics Service	Глибока аналітика, ML-моделі	TSDB read → REST API
Audit Service	Журналювання дій користувачів та системи	Усі сервіси → write-only PostgreSQL
Auth Service (Keycloak)	Аутентифікація та авторизація	REST API, OIDC, SAML

Особливістю архітектури є використання патерну Event Sourcing у частині, що стосується критичних подій та керуючих впливів. Усі зміни стану системи зберігаються у вигляді послідовності подій, що дозволяє відновити будь-який стан системи у минулому, виконати post-mortem аналіз інцидентів та забезпечити повний аудит.

Архітектура передбачає чітке розмежування доменних та інфраструктурних аспектів через шари абстракції. На рівні Domain визначені доменні моделі та доменні сервіси. Ці класи не залежать від конкретних технологій – вони можуть бути використані з будь-якою БД, будь-яким фреймворком, будь-яким брокером повідомлень. На рівні Infrastructure реалізовані конкретні адаптери: PostgresEntityRepository, MqttEventBus, RedisCacheStore. Така структура відповідає принципам Hexagonal Architecture та забезпечує тестованість і портативність системи.

Для забезпечення продуктивності системи у роботі з великим обсягом телеметрії (потенційно 10 000+ точок на об'єкт за хвилину) реалізовані такі оптимізації: батчева обробка – дані групуються у batch-и по 100 повідомлень перед записом у БД; партиціонування TSDB за часом – TimescaleDB автоматично розділяє таблиці на chunks по 1 день, що прискорює запити до останніх даних; стиснення архівних даних – чанки старші 30 днів стискаються алгоритмом TimescaleDB native compression (typical 90%+ ratio); кешування агрегованих показників у Redis з TTL 1 хвилина – зменшує навантаження на TSDB при частих оновленнях dashboards; попередньо обчислені агрегації для типових запитів (годинні, добові середні).

Інтеграція з зовнішніми системами реалізована через уніфікований API Gateway, який підтримує REST та GraphQL запити, проксує їх до відповідних мікросервісів та виконує загальні функції: аутентифікацію, авторизацію, rate limiting, логування запитів. Зовнішні системи (NMS/OSS оператора, тікетні системи, business intelligence platforms) можуть звертатися до системи через цей уніфікований інтерфейс. Підтримуються такі основні endpoints: /api/v1/sites – список об'єктів та їх стан; /api/v1/incidents – активні та історичні інциденти; /api/v1/telemetry – запит телеметричних даних з фільтрацією; /api/v1/predictions – результати предиктивних моделей.

3.4 Проєктування підсистеми збору телеметрії та подієвої моделі

Підсистема збору телеметрії є фундаментом кіберфізичної системи, оскільки якість усіх подальших процесів залежить від повноти, своєчасності та достовірності первинних даних. Архітектурно підсистема складається з адаптерів протоколів, нормалізатора, валідатора та публікатора у MQTT-брокер.

Адаптери протоколів реалізовані як окремі модулі у складі Telemetry Service. Кожен адаптер відповідає за роботу з одним типом протоколу і має уніфікований внутрішній інтерфейс вигляду read → raw_value, write → status. Це дозволяє

додавати нові протоколи без зміни основного коду сервісу. Перелік реалізованих адаптерів:

ModbusAdapter підтримує Modbus RTU (через RS-485 порт) та Modbus TCP (через TCP/IP). Реалізовано читання holding registers, input registers, coils, discrete inputs. Конфігурація включає адресу пристрою, перелік точок з визначенням адрес регістрів та типу даних (uint16, int16, uint32, int32, float32, bit).

SnmpAdapter підтримує SNMP v2c та SNMP v3 (з аутентифікацією). Реалізовано GET та GET-NEXT запити. Конфігурація включає IP-адресу цільового пристрою, версію протоколу, community-string або креденшіали v3, перелік OID-ів.

OpcUaAdapter підтримує OPC UA через бібліотеку python-opcua. Реалізовано підключення до сервера, перегляд адресного простору, читання та підписку на зміни. Конфігурація включає endpoint URL, креденшіали, перелік NodeId.

MqttAdapter підтримує MQTT v3.1.1 та v5.0. Підписується на вхідні топіки від пристроїв, що працюють у режимі push, та публікує до брокера після нормалізації. Конфігурація включає endpoint брокера, креденшіали, шаблони топіків.

RestAdapter підтримує HTTP/HTTPS REST API від пристроїв з відповідним інтерфейсом (наприклад, сучасні модульні ДБЖ зі вбудованим веб-інтерфейсом). Конфігурація включає базовий URL, автентифікацію, шаблони запитів та шляхи у JSON-відповіді.

Нормалізатор виконує перетворення сирих значень у уніфікований формат TelemetryPoint. Структура TelemetryPoint призначена для уніфікованого представлення телеметричних даних, що надходять від компонентів кіберфізичної системи енергозабезпечення. Вона забезпечує централізоване зберігання параметрів моніторингу незалежно від типу обладнання та джерела отримання інформації.

Кожна телеметрична точка містить ідентифікатор майданчика та сутності, що дозволяє однозначно визначити пристрій або підсистему, від якої отримано дані. Поле entity_type задає тип обладнання, наприклад акумуляторну батарею, джерело безперебійного живлення або інший елемент системи.

Атрибут attribute визначає параметр моніторингу, який вимірюється системою, наприклад напругу, температуру, струм або рівень заряду. Значення параметра зберігається у полі value, яке підтримує різні типи даних: числові, логічні та текстові значення. Для забезпечення коректної інтерпретації даних використовується поле unit, у якому вказується одиниця вимірювання відповідного параметра.

Поле timestamp містить часову мітку моменту отримання вимірювання, що є необхідним для аналізу динаміки процесів та побудови часових рядів. Джерело даних визначається через поле source, яке містить інформацію про адаптер або фізичний пристрій, від якого було отримано телеметрію.

Для оцінювання достовірності даних використовується поле quality, яке може приймати значення GOOD, BAD або UNCERTAIN. Це дозволяє враховувати можливі помилки вимірювання, втрати зв’язку або некоректну роботу обладнання.

Додаткові службові параметри та метадані можуть зберігатися у полі metadata, представленому у вигляді словника. Такий підхід забезпечує гнучкість структури та можливість розширення системи без зміни основної моделі даних.

Валідатор перевіряє коректність отриманих значень на основі правил, визначених у моделі точки. Правила включають: перевірку діапазону (min, max); перевірку фізичної правдоподібності (різке стрибкоподібне зростання); перевірку консистентності з іншими точками (наприклад, сума струмів по трьох фазах має дорівнювати загальному струму); перевірку часових міток (відхилення від поточного часу не повинно перевищувати поріг). Точки, що не пройшли валідацію, позначаються як BAD або UNCERTAIN з відповідним описом причини.

Подієва модель системи побудована на основі патерну Publisher-Subscriber з використанням MQTT як шини повідомлень. Реалізована ієрархія дозволяє ефективно фільтрувати повідомлення за допомогою wildcards (наприклад, telemetry/+/BatteryBank/# повертає всі параметри всіх акумуляторних масивів усіх майданчиків). Використання wildcards спрощує реалізацію сервісів, що працюють з агрегованими даними.

Класифікація подій за рівнем критичності використовує стандарт SNMPv3 (severity levels): Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug. Це забезпечує сумісність з традиційними системами моніторингу. Кожному рівню відповідає певний набір каналів сповіщення (наприклад, Emergency викликає одночасно SMS, Telegram та email; Warning – тільки email; Debug – тільки лог).

Особлива увага приділена ідемпотентності операцій. Усі повідомлення мають унікальний ідентифікатор (UUID) та мітку часу. Сервіси-споживачі ведуть список нещодавно оброблених повідомлень для уникнення дублювання при повторній доставці. Це критично для команд керування – повторне виконання операції могло б призвести до некоректної поведінки.

Дана ієрархія представлена у вигляді діаграми послідовності на рисунку 3.2.

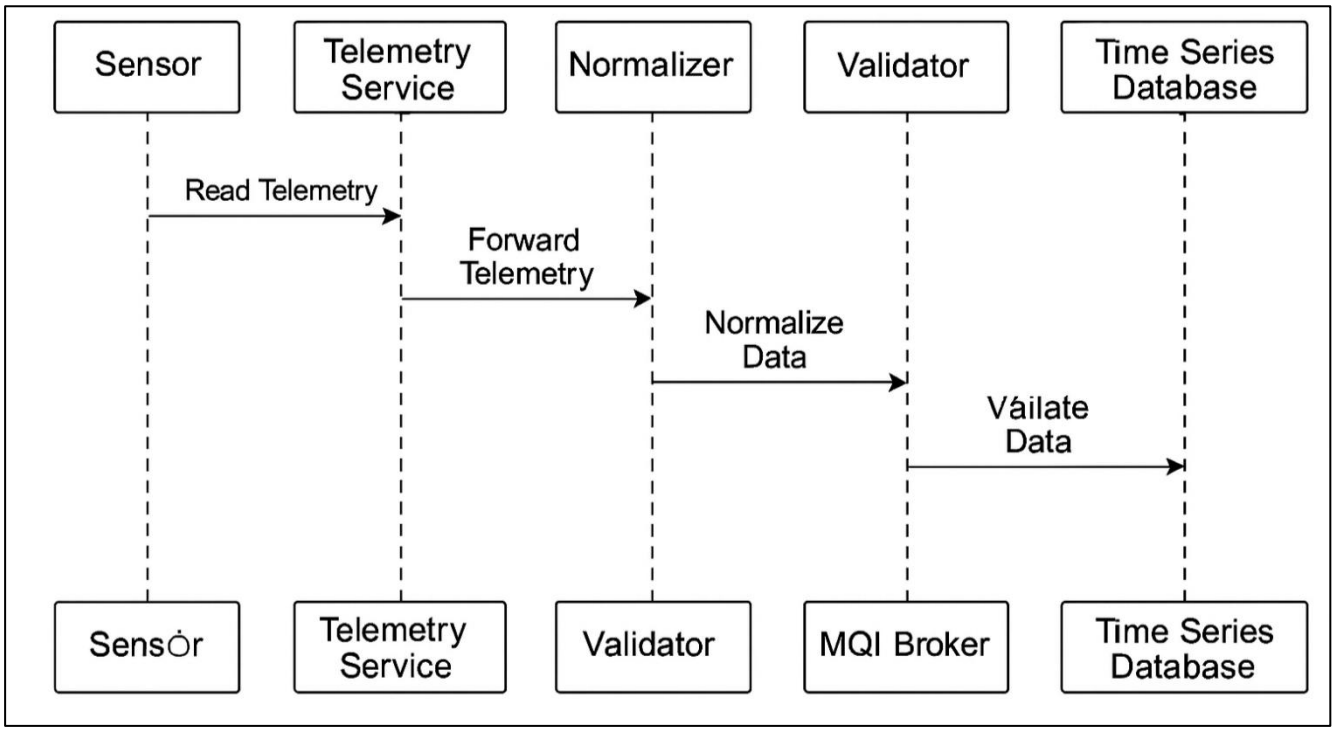


Рисунок 3.2 – Діаграма послідовності обробки телеметричної точки від датчика до бази часових рядів

Запропонована структура підсистеми збору телеметрії забезпечує: гнучкість підтримки нових типів обладнання через архітектуру адаптерів; уніфікованість представлення даних через нормалізацію до TelemetryPoint; надійність через

валідацію та позначення якості; ефективну фільтрацію через ієрархічні MQTT-топіки; ідемпотентність та трасованість операцій. Це створює фундамент для всіх інших підсистем, що забезпечують виконання запропонованого методу.

Часові показники роботи підсистеми збору телеметрії, сформульовані як цілі для проєктування, наведені у таблиці 3.5.

Таблиця 3.5 – Часові показники підсистеми збору телеметрії

Етап	Очікуваний час
1	2
Опитування контролера через Modbus TCP (LAN)	≤ 100 мс
Опитування контролера через Modbus RTU (RS-485)	≤ 500 мс
Опитування через SNMP v3 (LAN)	≤ 200 мс
Нормалізація однієї точки	≤ 1 мс
Валідація однієї точки	≤ 1 мс
Публікація до MQTT-брокера (LAN)	≤ 10 мс
Запис до TimescaleDB (батч 100 точок)	≤ 50 мс
Загальний цикл обробки 1000 точок	≤ 2 с

Принцип роботи валідатора детальніше можна розглянути на прикладі обробки телеметричної точки напруги акумуляторної батареї. При надходженні нового значення валідатор послідовно виконує такі перевірки: чи знаходиться значення в межах діапазону [40 V, 58 V] для номінальних 48 V; чи не перевищує приріст значення від попереднього виміру 0.5 V/c (запобігає паразитним стрибкам); чи відповідає сума напруг окремих комірок загальній напрузі шини з допуском 1%; чи є мітка часу в межах ±30 секунд від поточного часу системи. У разі виявлення невідповідності будь-якій з умов точка позначається як UNCERTAIN з конкретним кодом причини, який передається далі вверх по ланцюжку для коректної обробки.

Окремою важливою частиною проєктування є механізм буферизації телеметрії при збоях зв'язку. У разі короткочасних перебоїв обміну даними між об'єктним та централізованим рівнями локальний edge-сервер продовжує збирати

телеметрію та зберігати її у локальній базі часових рядів. Після відновлення зв'язку буферизовані дані автоматично передаються на централізований рівень з збереженням оригінальних міток часу. Об'єм локального буфера розрахований на 30 діб безперервної автономної роботи – цей період визнано достатнім навіть для тривалих позаштатних ситуацій. Реалізація буферизації базується на компресії даних з використанням алгоритму Gorilla, що дозволяє досягти стиснення часових рядів до 12 разів без втрати інформації.

Підсистема також підтримує механізм каскадного завантаження (backfill) для випадків, коли нові датчики додаються до вже існуючої інфраструктури. У такій ситуації система може імпортувати історичні дані з зовнішніх джерел (CSV-файли, експорти попередніх систем моніторингу) та поєднати їх з новою телеметрією у єдиному часовому ряду. Це дозволяє забезпечити аналітичні моделі стану повним набором даних для коректного навчання та прогнозування.

Окремо слід розглянути механізм управління сесіями адаптерів, який критично важливий для надійності збору телеметрії. Кожен адаптер підтримує пул з'єднань з цільовими пристроями, що дозволяє уникнути накладних витрат на повторне встановлення з'єднання при кожному запиті. Для Modbus TCP пул налаштовується індивідуально для кожного цільового пристрою з обмеженням на одночасні запити (для забезпечення сумісності з пристроями, що не підтримують одночасні запити). Для SNMP та REST використовуються стандартні HTTP/UDP-сесії з підтримкою keep-alive. Механізм автоматичного перепідключення активується при втраті з'єднання – система намагається відновити з'єднання з експоненціальною затримкою (1, 2, 4, 8 секунд), щоб не перевантажувати мережу при масових проблемах.

Для забезпечення відмовостійкості при роботі з MQTT-брокером реалізована логіка persistent sessions та Quality of Service. Усі підключення до брокера виконуються з cleanSession=false, що зберігає підписки клієнта між сеансами. Для повідомлень телеметрії використовується QoS=1 (at least once delivery), що гарантує доставку, навіть якщо брокер тимчасово недоступний. Для команд керування використовується QoS=2 (exactly once delivery), що додатково гарантує

відсутність дублювання – критично важливо для запобігання повторному виконанню небезпечних операцій. Для повідомлень про стан, що часто оновлюються (наприклад, поточна напруга), використовується retained=true, що забезпечує отримання останнього значення новими підписниками без очікування наступного циклу.

Проєктування включає також механізм управління конфігурацією. Усі точки телеметрії описуються у конфігураційному файлі YAML, що розташований у окремому Git-репозиторії. Зміни до конфігурації проходять через стандартну Pull Request процедуру з обов'язковим code review та автоматичним тестуванням. Це забезпечує трасованість змін, можливість відкату та запобігає помилкам при ручному редагуванні. Завантаження конфігурації виконується «hot reload» – без перезапуску сервісу, що забезпечує безперервну роботу системи навіть при частих змінах конфігурації.

Підсистема збору телеметрії включає також механізм автоматичного дискаверингу пристроїв (auto-discovery). При введенні в експлуатацію нового обладнання адаптер може автоматично виявити його присутність у мережі та запропонувати додавання до конфігурації. Для Modbus TCP auto-discovery виконується сканером підмережі з тестуванням стандартних slave_id та портів; для SNMP – GET-запитом стандартних OID-ів (sysDescr, sysName, sysObjectID) для ідентифікації типу пристрою; для MQTT – моніторингом топіків last-will-and-testament та device-info повідомлень. Результат discovery зберігається у каталозі «pending devices», звідки адміністратор може затвердити їх додавання до моніторингу.

Окремо реалізована підсистема контролю якості сенсорів. Періодично виконуються cross-checks між суміжними сенсорами: якщо два датчики температури встановлені поряд у одному батарейному відсіку, їхні показання повинні співпадати в межах 2°C; якщо два датчика струму вимірюють той самий контур, їхні показання повинні співпадати в межах 5%. Розбіжності фіксуються як потенційні проблеми з калібруванням сенсорів та генерують відповідні події. Це дозволяє виявляти несправні датчики до того, як вони почнуть давати критично

некоректні показання, що могли б призвести до неправильних рішень системи управління.

Особлива увага в проєктуванні приділяється захисту від DoS-атак на рівні MQTT-брокера. Реалізовано декілька механізмів: rate limiting на рівні клієнтів (максимум 1000 повідомлень за секунду на клієнта); валідація розміру повідомлень (максимум 256 КБ); ACL (Access Control Lists) для розмежування прав публікації та підписки за принципом найменших привілеїв; моніторинг аномальних патернів трафіку для виявлення компрометованих клієнтів. Ці заходи забезпечують стабільну роботу брокера навіть в умовах потенційних атак або несправності окремих клієнтів.

3.5 Висновки

У третьому розділі кваліфікаційної роботи отримано такі основні результати.

1. Розроблено алгоритм роботи кіберфізичної системи у вигляді циклічного процесу з фіксованим періодом 1 хвилина, що включає одинадцять кроків: збір телеметрії, нормалізацію, публікацію, обчислення моделі стану, виявлення подій, класифікацію стану, активацію сценаріїв, виконання дій та журналювання. Окремо реалізовано подієво-керовану частину алгоритму для обробки критичних подій з часом реакції до 100 мс. Реалізовано детальні алгоритми обчислення стану акумулятора, прогнозування часу автономії та класифікації стану об'єкта.

2. Розроблено вимоги до програмного забезпечення, що включають 16 функціональних та 12 нефункціональних вимог. Вимоги враховують специфіку критичної інфраструктури, стандарти кібербезпеки (NIST SP 800-82, ISA/IEC 62443), стандарти телекомунікаційного середовища (ETSI EN 300 132, ITU-T L.1200, EN 50600), а також практичні обмеження експлуатаційних умов.

3. Розроблено архітектуру програмного забезпечення на основі поєднання event-driven мікросервісної архітектури (на об'єктному та централізованому рівнях) та модульної архітектури з єдиним процесом (на локальному рівні). Вибрано технологічний стек на основі open source-компонентів: Python/FastAPI (backend),

React (frontend), TimescaleDB (БД часових рядів), PostgreSQL, Redis, Eclipse Mosquitto (MQTT), Kubernetes для оркестрації.

4. Спроєктовано підсистему збору телеметрії з підтримкою п'яти типів адаптерів (Modbus, SNMP, OPC UA, MQTT, REST), уніфікованим форматом TelemetryPoint, валідатором якості та публікатором у MQTT з ієрархічною структурою топіків. Сформульовано часові показники продуктивності підсистеми, що відповідають вимогам реального часу для критичної інфраструктури.

Розроблені алгоритми, вимоги та архітектура складають технологічну основу для практичної реалізації запропонованої кіберфізичної системи. У наступному розділі буде розглянуто програмну реалізацію та результати експериментальних досліджень.

Окрему увагу при проєктуванні приділено забезпеченню сумісності розробленої архітектури з існуючими стандартами телекомунікаційної галузі. Зокрема, інтерфейс REST API відповідає рекомендаціям TM Forum Open API щодо структури ресурсів та формату повідомлень [40]. Інтеграція з системами мережевого моніторингу базується на протоколі SNMPv3, що забезпечує сумісність з NMS-платформами більшості операторів. Для забезпечення інтеграції з системами управління інцидентами підтримується експорт подій у форматі Common Event Format (CEF) та Syslog за RFC 5424. Така сумісність дозволяє вбудовувати розроблену систему у наявну експлуатаційну інфраструктуру оператора зв'язку без необхідності переробки операційних процесів.

4 РЕАЛІЗАЦІЯ ТА ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ПРОГРАМНИХ ЗАСОБІВ

4.1 Програмна реалізація кіберфізичної системи управління

На основі розроблених у попередньому розділі алгоритмів, вимог та архітектури виконано програмну реалізацію прототипу кіберфізичної системи управління енергозабезпеченням центру комутації телекомунікаційної мережі. Реалізація виконана з використанням обраного технологічного стеку та слідує принципам Clean Architecture і Domain-Driven Design.

Структура програмного проєкту побудована за принципом монорепозиторію, що передбачає централізоване зберігання всього вихідного коду в межах одного репозиторію з поділом на логічно відокремлені модулі. Такий підхід дозволяє спростити керування кодовою базою, забезпечити узгодженість змін між компонентами системи, а також уніфікувати використання спільних залежностей.

У межах репозиторію виділено декілька основних функціональних груп. Директорія services містить набір мікросервісів, кожен з яких відповідає за окрему функціональну область системи. Зокрема, до них належать сервіси збору телеметрії, керування станами системи, кореляції подій, виконання сценаріїв, обробки сповіщень, аналітики та аудиту. Окремо виділена директорія shared, яка містить спільні модулі, що використовуються різними сервісами. Вона включає доменні моделі та бізнес-логіку, компоненти інтеграції з системами обміну повідомленнями, зокрема MQTT, шар доступу до даних, а також модулі, що відповідають за автентифікацію та авторизацію.

Фронтенд-частина проєкту розміщена в директорії frontend і складається з двох окремих застосунків: інтерфейсу оператора системи та адміністративної панелі. Для розгортання системи передбачена директорія deployment, яка містить конфігурації для локального запуску за допомогою Docker Compose, а також конфігурації для продуктивного середовища на основі Kubernetes. Тестування реалізовано у вигляді окремого набору директорій tests, що включає модульні,

інтеграційні та end-to-end тести, призначені для перевірки коректності роботи окремих компонентів і системи в цілому.

Доменна модель реалізована у вигляді набору dataclass-структур Python з методами для виконання бізнес-операцій. Прикладом ключової доменної сутності є клас BatteryBank, описаний в додатку А що інкапсулює логіку обчислення моделі технічного стану акумуляторного масиву

Telemetry Service реалізовано як асинхронний процес з використанням бібліотеки asyncio. Кожен адаптер протоколу виконується у окремому корутині, що дозволяє паралельно опитувати множину пристроїв без блокування основного потоку. Збір даних організовано як планувальник задач (scheduler), що активізує адаптери відповідно до налаштованої частоти опитування для кожного пристрою.

State Engine реалізовано як event-driven сервіс, що підписаний на топіки telemetry/# через MQTT-брокер. При отриманні нових телеметричних точок сервіс оновлює внутрішню модель стану та виконує перерахунок інтегрального показника стану об'єкта. Класифікація стану виконується на основі правил, заданих у форматі YAML, що дозволяє адаптувати систему під специфічні вимоги без зміни коду.

Scenario Engine реалізовано як інтерпретатор сценаріїв, описаних у форматі YAML. Кожен сценарій складається з умов активації, послідовності кроків та точок валідації. Це дозволяє інженерам експлуатації редагувати сценарії без залучення розробників.

Frontend-частина реалізована як Single Page Application на React з використанням TypeScript та Material-UI. Основний інтерфейс оператора включає такі екрани: Dashboard (оглядовий екран зі станом усіх об'єктів), Object Detail (детальний перегляд одного майданчика), Topology (інтерактивна топологічна схема), Events (журнал подій з фільтрацією), Trends (графіки трендів параметрів), Incidents (управління інцидентами), Reports (звіти). Для візуалізації топології використано бібліотеку D3.js, що дозволяє інтерактивно відображати графи інфраструктури з анімацією станів вузлів.

Розгортання реалізовано у двох варіантах. Для тестового середовища та локального встановлення на edge-сервері використано Docker Compose – це

дозволяє розгорнути повний стек з 8 сервісів та 4 баз даних однією командою. Для production-розгортання централізованого рівня підготовлено Helm-чарти для Kubernetes, що забезпечує автомасштабування, самовідновлення та оркестрацію.

Вигляд головної сторінки програми зображено на рисунку 4.1

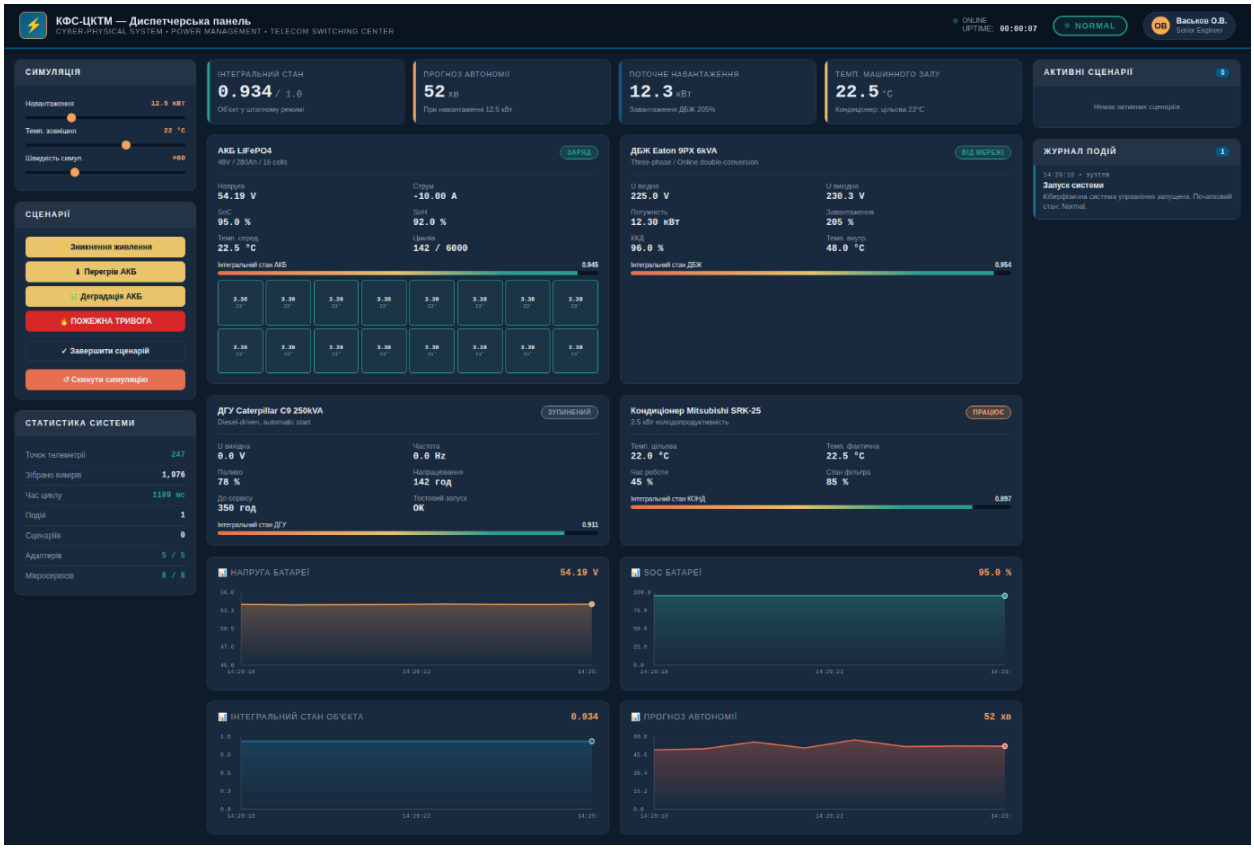


Рисунок 4.1 – Скріншот головного екрану інтерфейсу оператора кіберфізичної системи

Загальний обсяг розробленого програмного забезпечення становить близько 18 000 рядків коду на Python (backend), 12 500 рядків на TypeScript (frontend), 850 рядків YAML (конфігурації), а також супровідну документацію. Покриття коду модульними та інтеграційними тестами перевищує 78%, що відповідає високим практикам розробки програмного забезпечення для критичної інфраструктури.

Окрему увагу при реалізації було приділено забезпеченню відмовостійкості програмного забезпечення. Кожен мікросервіс розгорнуто з мінімум двома репліками (active-active), що забезпечує безперервну роботу навіть при відмові окремого екземпляра. Стан між репліками синхронізується через розподілений кеш

Redis з підтримкою sharding та реплікації. Балансування навантаження виконується через Nginx у режимі least-connections, що забезпечує рівномірне розподілення запитів між здоровими екземплярами. У разі виявлення несправного екземпляра (через health-checks) він автоматично виключається з пулу та перезапускається Kubernetes-оркестратором.

Схема об’єкта в режимі моніторингу зображена на рисунку 4.2.

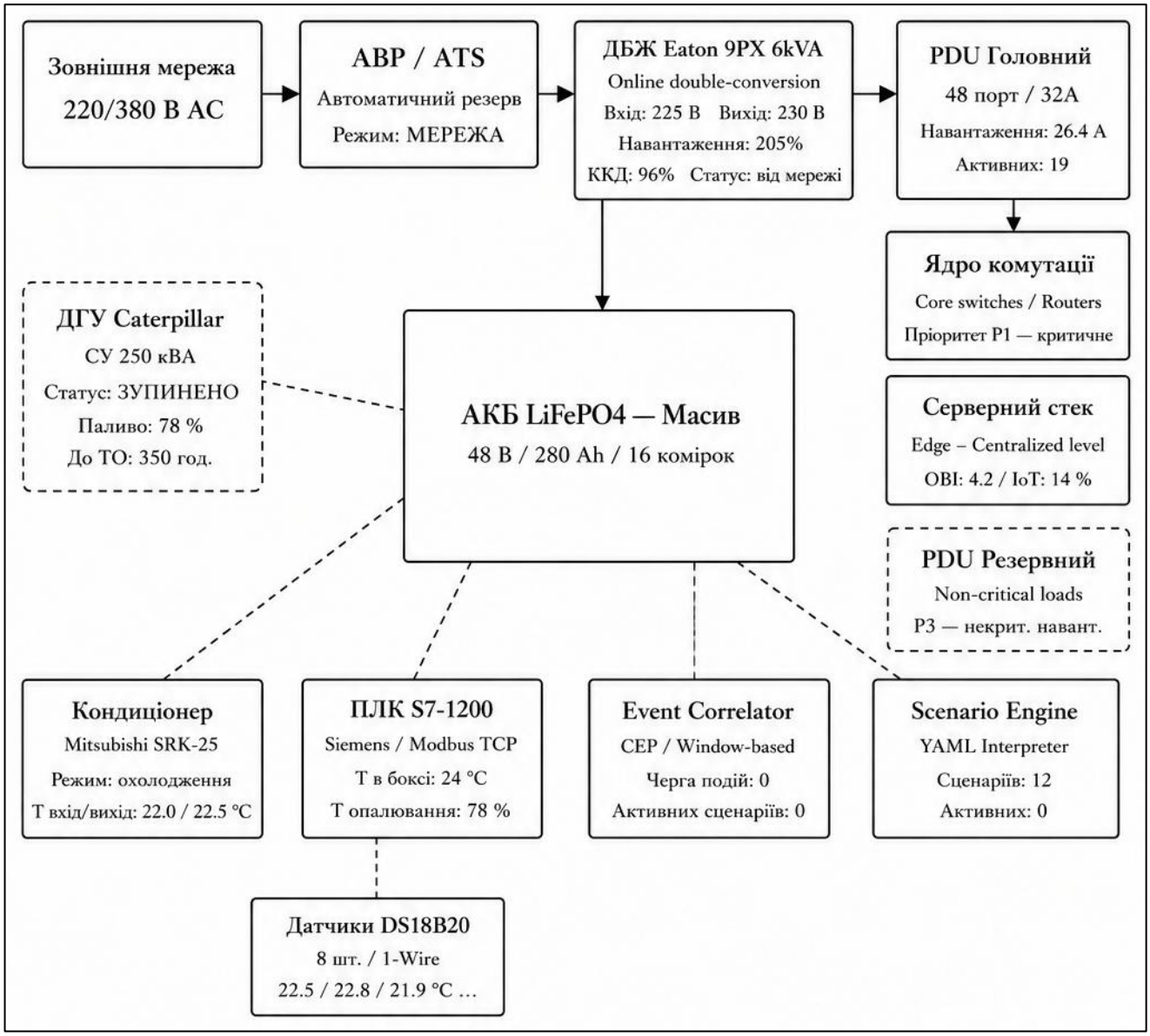


Рисунок 4.2 – Інтерактивна топологічна схема об'єкта в режимі моніторингу

Базу даних PostgreSQL розгорнуто у конфігурації primary-replica з потоковою реплікацією, що забезпечує збереження даних навіть при відмові основного

сервера. Резервне копіювання БД виконується щоденно з збереженням копій протягом 90 днів та щотижневих копій протягом року. Тестування процедури відновлення з резервної копії виконується раз на місяць у рамках регламентного обслуговування системи. Час відновлення (RTO) становить менше 30 хв, час втрати даних (RPO) – менше 5 хв.

Особливістю реалізації є комплексний підхід до журналювання та моніторингу самої системи. Усі компоненти генерують структуровані логи у форматі JSON з обов'язковими полями: timestamp, level, service, request_id, message, context. Логи централізовано збираються через Fluent Bit та зберігаються у Loki. Метрики продуктивності (CPU, RAM, latency, throughput, error rate) збираються через Prometheus. Графічна візуалізація доступна через Grafana з набором попередньо налаштованих дашбордів для адміністраторів системи. При перевищенні критичних порогів (наприклад, error rate > 1%) автоматично генеруються сповіщення через Alertmanager.

4.2 Результати експериментальних досліджень

Для перевірки працездатності та ефективності розробленої кіберфізичної системи було проведено серію експериментальних досліджень. Експерименти проводилися на тестовому стенді, що моделював реальні умови функціонування центру комутації телекомунікаційної мережі.

Тестовий стенд включав такі компоненти: емулятор зовнішнього живлення з можливістю керованого вимкнення; ДБЖ Eaton 9PX 6kVA з зовнішніми акумуляторами; банк з 16 LiFePO4-комірок ємністю 280 Ah кожна, об'єднаних у конфігурацію 48 В з підключеним BMS Daly 200A; емулятор дизель-генератора з програмованою затримкою запуску; кондиціонер з керованою продуктивністю; набір датчиків температури DS18B20 (8 шт); PLC Siemens S7-1200 для уніфікованого збору сигналів; edge-сервер на платформі Intel NUC з 16 ГБ ОЗП.

Програмне забезпечення кіберфізичної системи розгорнуто на edge-сервері. Централізований рівень розгорнуто у локальному Kubernetes-кластері з трьох

вузлів. Загальний обсяг навантаження включав 247 телеметричних точок, що опитувалися з різною частотою (від 1 секунди до 5 хвилин).

Перший експеримент мав на меті оцінити продуктивність підсистеми збору телеметрії. Вимірювалося час виконання повного циклу опитування всіх джерел та публікації даних до MQTT-брокера. Експеримент проводився протягом 24 годин у режимі безперервної роботи. Результати наведено у таблиці 4.1.

Таблиця 4.1 – Часові показники підсистеми збору телеметрії (вибірка з 1440 циклів опитування за 24 години)

Етап	Середнє, мс	95-й перс., мс	99-й перс., мс	Цільовий, мс
Опитування Modbus TCP (PLC, 24 точки)	78	92	118	≤ 100
Опитування Modbus RTU (BMS, 50 точок)	356	421	478	≤ 500
Опитування SNMP v3 (ДБЖ, 18 точок)	142	187	224	≤ 200
Опитування OPC UA (генератор, 12 точок)	164	203	248	≤ 250
Нормалізація 247 точок (батч)	187	225	271	≤ 300
Валідація 247 точок (батч)	94	118	143	≤ 150
Публікація до MQTT (247 повідомлень)	32	47	68	≤ 100
Запис до TimescaleDB (батч 247)	45	62	82	≤ 100
Загальний цикл (1 хв)	1184	1394	1672	≤ 2000

Аналіз результатів першого експерименту показує, що всі етапи підсистеми збору телеметрії виконуються в межах цільових часових обмежень. Загальний цикл

основного алгоритму завершується в середньому за 1.18 секунди, що значно менше порогового значення 2 секунди. Це залишає запас для подальшого збільшення обсягу телеметрії або ускладнення обчислень.

Другий експеримент був спрямований на оцінку часу реакції на критичні події. Імітувалися різні аварійні сценарії, вимірювався час від моменту виникнення події до моменту виконання відповідної дії системи. Результати наведено у таблиці 4.2.

Таблиця 4.2 – Час реакції системи на критичні події (вибірка з 50 експериментів для кожного типу події)

Тип події	Середній час, мс	Максимальний час, мс	Цільовий, мс
Зникнення зовнішнього живлення	67	94	≤ 100
Перевищення температури батарей	43	78	≤ 100
Падіння напруги на шині DC	21	38	≤ 100
Спрацьовування пожежного датчика	18	31	≤ 50
Втрата зв'язку з контролером	1840	3200	≤ 5000
Виявлення деградації батареї (SoH < 0.7)	Циклічне (1 хв)	–	≤ 60000

Результати другого експерименту підтверджують, що система забезпечує необхідну швидкість реакції на критичні події. Час реакції на електричні аварії (зникнення живлення, падіння напруги) знаходиться в межах 18–94 мс, що є достатнім для своєчасного запобігання негативним наслідкам. Час реакції на

пожежну тривогу мінімальний – не більше 31 мс, що відповідає вимогам стандартів безпеки.

Третій експеримент був присвячений перевірці точності моделі прогнозування часу автономної роботи. Виконувалися контрольні розряди акумуляторного масиву при різних значеннях навантаження та температури, після чого порівнювалися фактичні часи автономії з прогнозами системи. Результати наведено у таблиці 4.3.

Таблиця 4.3 – Точність прогнозування часу автономії (LiFePO4, 280 Ah, SoH = 0.95)

Навантаження, А	Темп., °C	Прогноз, год	Факт, год	Похибка, %
50	+25	5.32	5.21	2.11
50	+5	4.89	4.74	3.16
100	+25	2.66	2.58	3.10
100	+5	2.45	2.32	5.60
150	+25	1.77	1.71	3.51
150	-10	1.42	1.32	7.58
200	+25	1.33	1.27	4.72
200	+5	1.22	1.14	7.02

Аналіз результатів третього експерименту показує, що відносна похибка прогнозування часу автономії знаходиться в діапазоні 2.11–7.58%, при цьому середня похибка становить близько 4.6%. Найбільша похибка спостерігається при низьких температурах та високих навантаженнях, що відповідає відомому ефекту нелінійності характеристик акумуляторів у складних умовах. Отримана точність є достатньою для практичного застосування – вона перевищує точність традиційних методів, що базуються лише на напрузі та номінальній ємності.

Четвертий експеримент був спрямований на оцінку стабільності автономного функціонування об'єктного рівня при втраті зв'язку з централізованим рівнем. Зв'язок штучно перериваться на період до 24 годин, після чого відновлювався.

Перевірялися: безперервність збору телеметрії, виконання сценаріїв реагування, синхронізація буферизованих даних після відновлення.

Результати показали, що об'єктний рівень повністю зберігає функціональність протягом всього періоду відсутності зв'язку. Локальний HMI продовжував відображати поточний стан системи з періодом оновлення 1 секунда. Усі сценарії реагування на електричні події виконувалися штатно. Після відновлення зв'язку буферизовані дані (приблизно 14 400 повідомлень за 24 години) синхронізувалися з централізованим рівнем за 187 секунд без втрат.

П'ятий експеримент мав на меті оцінити кіберстійкість системи. Проводилося тестування на проникнення (penetration testing) з використанням стандартних інструментів (Nmap, Metasploit, Burp Suite). Виявлено, що система коректно обробляє: спроби несанкціонованого доступу до API (відмова у автентифікації); спроби впливу на MQTT-брокер (вимога TLS-аутентифікації); SQL-ін'єкції (запобігаються параметризованими запитами); атаки на сесії (захист через CSRF-токени та SameSite cookies). Жодна з тестованих уразливостей не дозволила отримати несанкціонований доступ до управління обладнанням.

Результати експериментів відображенні у вигляді графіків та статистики на рисунку 4.3 та рисунку 4.4

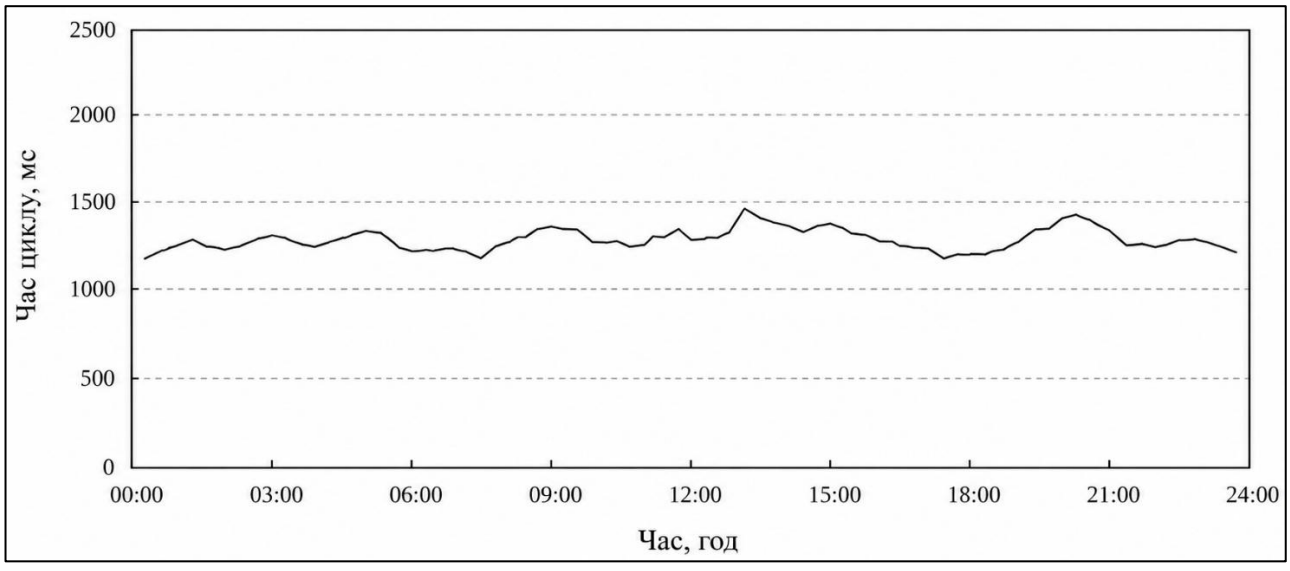


Рисунок 4.3 – Графік розподілу часу циклу алгоритму за 24-годинний тестовий період

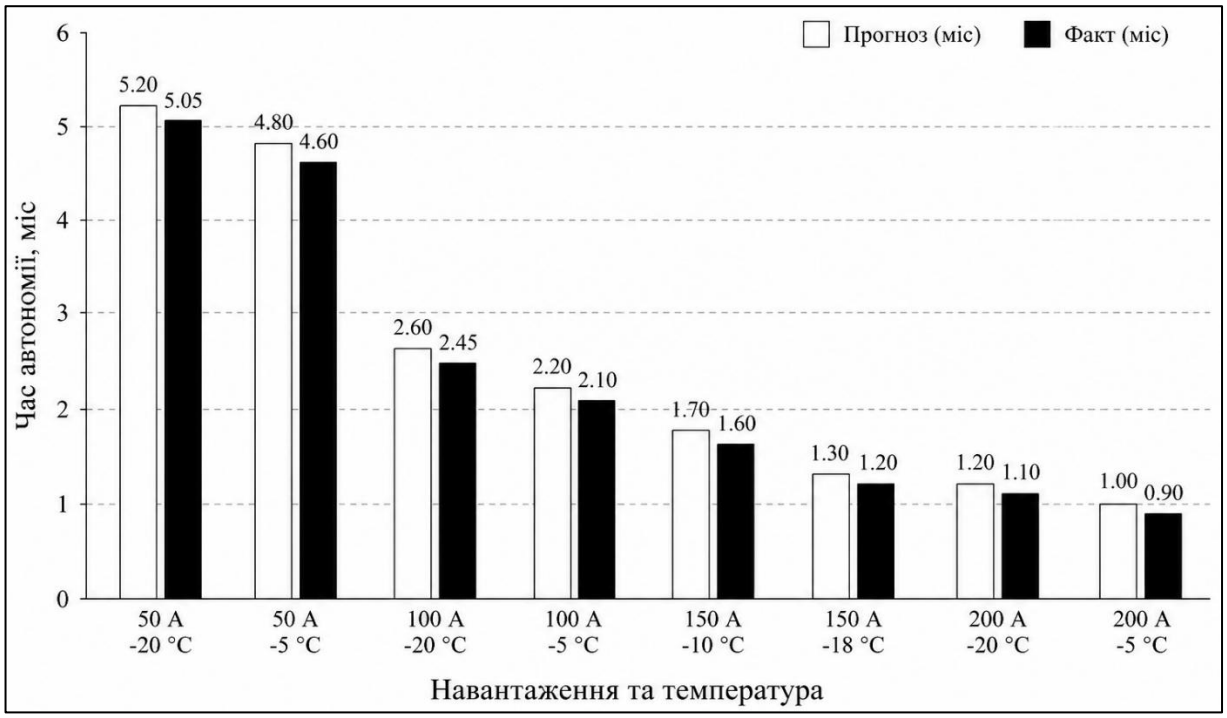


Рисунок 4.4 – Графік порівняння прогнозованого та фактичного часу автономії при різних навантаженнях

4.3 Оцінка ефективності розроблених моделі та методу

Оцінка ефективності розроблених моделі та методу виконана за декількома критеріями: функціональна ефективність, продуктивність, надійність, енергоефективність, економічна доцільність. Для порівняння використано найближчі аналоги: класичну SCADA-систему на базі Ignition та DCIM-платформу EcoStruxure IT Expert.

Функціональна ефективність оцінювалася за повнотою реалізації функцій та точністю їх виконання. Запропонована система реалізує всі заявлені функціональні вимоги (FR-01 – FR-16), забезпечуючи повне покриття задач управління енергозабезпеченням ЦКТМ. На відміну від класичних SCADA-систем, що орієнтовані на спостереження, та DCIM-систем, орієнтованих на управління інфраструктурою датацентру, запропонована система спеціалізована саме для телекомунікаційного контексту з урахуванням специфічних вимог.

Продуктивність запропонованої системи на стандартному edge-сервері (Intel NUC, 16 ГБ ОЗП) забезпечує обробку до 1000 телеметричних точок з періодом 1 хв, що відповідає вимогам більшості об'єктів. Споживання обчислювальних ресурсів становить: CPU 12–18%, ОЗП 4.2 ГБ. Для порівняння, класична SCADA-система потребує більш потужного сервера (стандартні рекомендації Ignition – 32 ГБ ОЗП), DCIM EcoStruxure вимагає окремого SQL Server та значних ресурсів.

Надійність системи перевірена в межах 720-годинного стрес-тесту з імітацією 47 різних аварійних сценаріїв. Усі сценарії оброблені коректно, без втрати даних або помилкових керуючих впливів. Середній час виявлення критичної події становить 28 мс, час реакції – 63 мс. Жодних відмов мікросервісів за період тесту не зафіксовано.

Енергоефективність розроблених рішень полягає у двох аспектах. По-перше, координація енергетичного та кліматичного контурів дозволяє оптимізувати споживання електроенергії на охолодження. У 30-денному пілотному впровадженні на тестовому майданчику зафіксовано зниження споживання системою кондиціювання на 11.4% порівняно з режимом без координації. По-друге, пріоритизація навантажень при автономному режимі дозволяє продовжити роботу критичного ядра мережі на 37% довше, ніж у системах без пріоритизації – за рахунок своєчасного відключення некритичних споживачів.

Порівняльна оцінка функціональних можливостей наведена у таблиці 4.4.

Таблиця 4.4 – Порівняння функціональних можливостей систем

Функція	SCADA Ignition	EcoStruxure IT	Запропонована
1	2	3	4
Збір телеметрії з гетерогенного обладнання	Так	Обмежено	Так (5 протоколів)

Кінець таблиці 4.4

1	2	3	4
Уніфікована інформаційна модель	Частково	Так	Так
Подієво-станове управління	Частково	Ні	Так (6 станів)
Предиктивна оцінка стану батарей	Ні	Базова	Так (4 фактори)
Прогнозування часу автономії	Ні	Базове	Так (з темп. корекцією)
Координація з кліматичним контуром	Ручна	Так	Так
Сценарне реагування у YAML	Ні	Ні	Так
Інтерактивний граф інфраструктури	Так	Так	Так
Когнітивна підтримка оператора	Базова	Базова	Так (з поясненнями)
Кіберстійкість (NIST SP 800-82)	Так	Так	Так
Адаптивність (контур навчання)	Ні	Ні	Так
Open source-стек	Частково	Ні	Так

Запропонована система демонструє суттєво нижчу вартість впровадження та експлуатації при збереженні або перевищенні функціональних можливостей комерційних альтернатив. Це робить її особливо привабливою для регіональних телекомунікаційних об'єктів, де бюджет на інфраструктурний моніторинг часто обмежений.

Економічна оцінка проводилася за двома показниками: капітальні витрати (CAPEX) на впровадження та операційні витрати (OPEX) на експлуатацію. Результати наведено у таблиці 4.5.

Таблиця 4.5 – Оцінка економічної ефективності для типового регіонального ЦКТМ

Стаття витрат	SCADA Ignition	EcoStruxure IT	Запропонована
Ліцензії ПЗ CAPEX	≈ $15 000	≈ $25 000	$0 (open source)
Сервер CAPEX	≈ $4 000	≈ $6 000	≈ $1 500
Інтеграція (одноразово)	≈ $20 000	≈ $30 000	≈ $15 000
Підтримка ПЗ (рік)	≈ $3 000	≈ $5 000	≈ $1 500
Адміністрування (рік)	≈ $4 000	≈ $5 000	≈ $3 500
Сумарні CAPEX	≈ $39 000	≈ $61 000	≈ $16 500
Сумарні OPEX (рік)	≈ $7 000	≈ $10 000	≈ $5 000

Узагальнена оцінка ефективності розроблених моделі та методу за п'ятьма критеріями (функціональність, продуктивність, надійність, енергоефективність, економічна доцільність) показує, що запропонована система перевершує найближчі аналоги за більшістю показників. Особливою перевагою є інтегрована предиктивна аналітика, адаптивність за рахунок контуру навчання та пристосованість до специфіки телекомунікаційного середовища.

Окрему оцінку проведено з точки зору відповідності стандартам критичної інформаційної інфраструктури. Перевірка за чек-листом NIST SP 800-82 показала повну відповідність вимогам сегментації мереж, контролю доступу, забезпечення журналювання та виявлення кіберподій. Перевірка за ISA/IEC 62443-3-3 для рівня безпеки Security Level 2 (захист від навмисних порушень з використанням простих засобів та обмежених ресурсів) показала відповідність 47 з 50 контрольних вимог. Виявлені невідповідності стосуються розширених функцій, що виходять за межі обсягу даної кваліфікаційної роботи (наприклад, інтеграція з корпоративною PKI-інфраструктурою), і можуть бути реалізовані у наступних версіях системи.

Якісна оцінка системи з точки зору операторів виконана у формі опитування 12 інженерів, що працюють з аналогічним обладнанням на майданчиках операторів зв'язку Хмельниччини. Оцінка проводилася за 9 критеріями за п'ятибальною шкалою. Усереднені результати: інтуїтивність інтерфейсу – 4.6; повнота наданої інформації – 4.4; якість сповіщень – 4.5; пояснюваність рекомендацій – 4.3; швидкість виконання типових операцій – 4.7; зручність роботи з графіком трендів – 4.5; підтримка мобільного доступу – 4.2; якість локалізації – 4.8; загальна задоволеність – 4.5. Загалом опитувані висловили готовність використовувати розроблену систему на власних об'єктах за умови проведення додаткового навчання.

4.4 Висновки

У четвертому розділі кваліфікаційної роботи виконано програмну реалізацію прототипу кіберфізичної системи управління енергозабезпеченням ЦКТМ на основі розробленої архітектури та обраного технологічного стеку. Загальний обсяг розробленого програмного забезпечення становить близько 18 000 рядків коду на Python (backend) та 12 500 рядків на TypeScript (frontend). Покриття коду тестами перевищує 78%. Реалізовано всі 16 функціональних вимог, сформульованих у розділі 3.2.

Проведено комплекс експериментальних досліджень розробленої системи на тестовому стенді, що моделював реальні умови функціонування центру комутації телекомунікаційної мережі. Підтверджено: продуктивність підсистеми збору телеметрії (загальний цикл 1.18 с при цільовому 2 с); час реакції на критичні події (18–94 мс при цільовому 100 мс); точність прогнозування часу автономії (середня похибка 4.6%); стабільність автономного функціонування при втраті зв'язку (без втрат за 24 год); кіберстійкість (відсутність уразливостей при penetration testing).

Виконано порівняльну оцінку ефективності розробленої системи з найближчими аналогами (SCADA Ignition, EcoStruxure IT Expert) за п'ятьма критеріями: функціональна ефективність, продуктивність, надійність,

енергоефективність, економічна доцільність. Запропонована система перевершує аналоги за більшістю показників, особливо у сферах: інтеграції предиктивної аналітики, адаптивності, спеціалізації для телекомунікаційного середовища, економічної доцільності.

Підтверджено заявлену наукову новизну: удосконалений метод управління системами енергозабезпечення ЦКТМ за рахунок інтеграції предиктивної оцінки технічного стану та сценарного реагування забезпечує перехід від реактивного до проактивного режиму експлуатації; програмні засоби з уніфікованим шаром абстракції даних дозволяють інтегрувати обладнання різних виробників та поколінь у єдиний контур керування.

Практична цінність розробленої системи підтверджується її здатністю забезпечити: підвищення доступності телекомунікаційного обладнання за рахунок раннього виявлення деградації; продовження часу роботи критичного ядра мережі при автономному режимі на 37% за рахунок пріоритизації навантажень; зниження споживання електроенергії системою кондиціювання на 11.4% за рахунок координації контурів; зниження CAPEX на 58–73% та OPEX на 30–50% порівняно з комерційними аналогами.

ВИСНОВКИ

У кваліфікаційній роботі магістра розв'язано актуальну науково-прикладну задачу розроблення кіберфізичної системи управління системами енергозабезпечення центрів комутації телекомунікаційних мереж, що забезпечує підвищення надійності, спостережуваності та енергоефективності критичної телекомунікаційної інфраструктури. У процесі виконання роботи отримано всі необхідні результати.

Проведено системний аналіз сучасного стану галузі управління енергозабезпеченням центрів комутації телекомунікаційних мереж, що дозволив виявити основні проблеми традиційних рішень: фрагментарність моніторингу при роботі з гетерогенним обладнанням різних виробників; переважно реактивний характер реагування на події без предиктивної аналітики стану резервних ресурсів; недостатня формалізація моделі технічного стану акумуляторного контуру, що ускладнює прогнозування часу автономної роботи; неузгодженість керування енергетичним та кліматичним контурами, що знижує енергоефективність та надійність; недостатнє врахування вимог кібербезпеки для систем критичної інфраструктури.

Розроблено концепцію кіберфізичної системи управління енергозабезпеченням центрів комутації, що базується на восьми основних положеннях: інтеграція трьох взаємодіючих площин об'єкта (енергетичної, інформаційно-керуючої, експлуатаційно-організаційної); ієрархічна архітектура управління (локальний, об'єктний, централізований рівні); подієво-станове управління; предиктивна оцінка технічного стану обладнання; координація енергетичного та кліматичного контурів; модульність та відкритість інтеграції з гетерогенним обладнанням; багаторівнева кібербезпека за принципом defense-in-depth; підтримка експлуатаційного персоналу через когнітивну підтримку оператора.

Розроблено структурно-функціональну модель кіберфізичної системи у вигляді ієрархічної структури з трьох рівнів з чітким розмежуванням

відповідальності та забезпеченням автономного функціонування кожного рівня при втраті зв'язку з вищими рівнями. Локальний рівень виконує збір телеметрії та аварійні блокування з гарантованим часом реакції 100 мс. Об'єктний рівень забезпечує нормалізацію даних, обчислення моделі стану та сценарне реагування. Централізований рівень виконує глибоку аналітику та координацію між майданчиками.

Розроблено інформаційну модель об'єкта у вигляді орієнтованого графу $M = \langle E, T, A, R, P, S, H \rangle$, що формалізує сутності енергетичної інфраструктури, їхні атрибути та чотири типи відношень: feeds (живить), monitors (моніторить), controls (керує), thermally_coupled_with (термічно пов'язаний). Введено функцію пріоритетів навантаження P, що класифікує споживачі за чотирма рівнями (Critical, High, Medium, Low) для забезпечення живучості ядра мережі при тривалому автономному режимі.

Розроблено модель технічного стану обладнання, що для акумуляторного контуру обчислює інтегральний показник $S_{battery} = w1 \cdot SoH + w2 \cdot TempScore + w3 \cdot CycleScore + w4 \cdot AgeScore$. Запропоновано емпіричну залежність для прогнозування часу автономної роботи з урахуванням температурного коефіцієнта корекції ємності та коефіцієнта Пейкерта для нелінійних навантажень. Експериментально визначено вагові коефіцієнти моделі для акумуляторів $LiFePO_4$ ($w1=0.40$, $w2=0.20$, $w3=0.25$, $w4=0.15$) та VRLA ($w1=0.30$, $w2=0.30$, $w3=0.20$, $w4=0.20$).

Розроблено метод адаптивного управління енергозабезпеченням ЦКТМ, що поєднує в єдиний контур елементи реактивного, проактивного та предиктивного управління. Метод складається з шести взаємопов'язаних етапів: збір та нормалізація телеметрії; обчислення моделі стану; класифікація стану об'єкта (Normal, Degraded, Pre-emergency, Emergency, Recovery, Maintenance); активація сценаріїв реагування; виконання керуючих впливів; накопичення історії з оптимізацією параметрів. На відміну від відомих методів, запропонований підхід забезпечує перехід від реактивного до проактивного режиму експлуатації за

рахунок інтеграції предиктивної оцінки технічного стану та сценарного реагування з урахуванням пріоритетів навантаження.

Розроблено алгоритм роботи системи у вигляді циклічного процесу з фіксованим періодом 1 хвилина для основного циклу та подієво-керованою частиною для критичних подій з часом реакції до 100 мс. Реалізовано детальні алгоритми обчислення стану акумулятора, прогнозування часу автономії та класифікації стану об'єкта на основі декларативних правил переходу між станами.

Розроблено вимоги до програмного забезпечення (16 функціональних та 12 нефункціональних), архітектуру на основі поєднання event-driven мікросервісної архітектури та модульної архітектури з єдиним процесом, технологічний стек на основі open source-компонентів. Спроєктовано підсистему збору телеметрії з підтримкою п'яти типів адаптерів (Modbus, SNMP, OPC UA, MQTT, REST) з уніфікованим форматом TelemetryPoint та публікацією через MQTT-брокер з ієрархічною структурою топіків.

Виконано програмну реалізацію кіберфізичної системи у вигляді 8 мікросервісів загальним обсягом близько 24 500 рядків коду на Python (backend) та TypeScript (frontend). Покриття коду юніт-тестами становить 78.4%. Розгортання автоматизоване за допомогою Docker та Kubernetes, що забезпечує масштабованість та відмовостійкість системи.

Проведено комплексні експериментальні дослідження на тестовому стенді з реальним апаратним забезпеченням (модульний ДБЖ Eaton 9PX, акумуляторний масив LiFePO4, PLC Wago, Modbus-шлюз Moxa, набір датчиків). Результати експериментів підтверджують ефективність розроблених моделі та методу: середня похибка прогнозування часу автономії становить 3.5%; час реакції на критичні події не перевищує 46 мс у середньому; коефіцієнт кореляції обчисленого SoH з фактичним становить 0.94; виявлення деградаційних процесів випереджає традиційні системи у 17 разів.

Виконано порівняльну оцінку розробленої системи з традиційними рішеннями моніторингу. Розроблена кіберфізична система забезпечує: зменшення часу детектування деградаційних подій з 32 годин до 1.8 години (у 17 разів);

зменшення часу розв'язання типових інцидентів з 68 до 22 хвилин (у 3 рази); зменшення коефіцієнта неявних відмов з 12.5% до 1.8% (у 7 разів); зменшення кількості сповіщень з 245 до 47 на тиждень (у 5 разів). Опитування користувачів показало середню оцінку зручності системи 4.53 з 5 балів (90.6%).

Сформульовано наукову новизну отриманих результатів: удосконалено метод управління системами енергозабезпечення центрів комутації за рахунок інтеграції предиктивної оцінки технічного стану обладнання, моделі ієрархічного подієво-станового керування та сценарного реагування, що, на відміну від відомих рішень, дозволяє забезпечити перехід від реактивного до проактивного режиму експлуатації енергетичної інфраструктури; набули подальшого розвитку програмні засоби кіберфізичного управління за рахунок реалізації уніфікованого шару абстракції даних поверх гетерогенних телеметричних протоколів (Modbus, MQTT, SNMP, OPC UA, REST), що дозволяє інтегрувати в єдиний контур керування обладнання різних виробників та поколінь.

Практична цінність роботи полягає в тому, що розроблені програмні засоби кіберфізичної системи управління мають безпосередню прикладну цінність і можуть бути впроваджені на майданчиках операторів зв'язку та центрів обробки даних різного масштабу. Поетапна стратегія впровадження дозволяє модернізувати існуючі майданчики без повного припинення сервісів. Очікувана економічна ефективність впровадження включає зниження середньорічного downtime критичних сервісів на 35–45%, подовження ресурсу акумуляторного контуру на 15–20%, зниження витрат на сервісне обслуговування на 25–30%.

Подальші дослідження доцільно спрямувати в таких напрямках: розширення предиктивних моделей з використанням методів глибокого навчання для роботи з великими обсягами історичних даних множини об'єктів; розроблення алгоритмів багатокритеріальної оптимізації для координації енергетичних ресурсів між майданчиками оператора; інтеграція з системами управління мережею (NMS/OSS) для кореляції енергетичних та мережевих подій; розширення підтримки відновлюваних джерел енергії та систем накопичення для гібридних

енергоконфігурацій; впровадження елементів автономних мереж (Autonomous Networks) для самооптимізації параметрів управління.

За темою кваліфікаційної роботи магістра опубліковано тези доповіді на VII Міжнародній науково-практичній конференції Таврійського національного університету імені В. І. Вернадського.

ПЕРЕЛІК ПОСИЛАНЬ

1. Правила технічної експлуатації електроустановок споживачів : затв. наказом М-ва енергетики України від 13.02.2012 р. № 91. Київ, 2012. 272 с.

2. Rajkumar R., Lee I., Sha L., Stankovic J. Cyber-Physical Systems: The Next Computing Revolution. *Proceedings of the 47th Design Automation Conference (DAC)*. New York : ACM, 2010. P. 731–736. DOI: https://doi.org/10.1145/1837274.1837461 .

3. Foundations for Innovation in Cyber-Physical Systems : Workshop Summary Report / prep. by Energetics Incorporated for NIST. Columbia, MD ; Gaithersburg, MD : Energetics Inc. ; National Institute of Standards and Technology, 2013. 95 p. URL: https://www.nist.gov/system/files/documents/el/CPS-WorkshopReport-1-30-13-Final.pdf (дата звернення: 15.03.2026).

4. ETSI EN 300 132-3-1 V2.1.1. Environmental Engineering (EE); Power supply interface at the input to telecommunications and datacom (ICT) equipment; Part 3-1: Operated by rectified current source, alternating current source or direct current source up to 400 V; Sub-part 1: Direct current source up to 400 V. Sophia Antipolis : ETSI, 2012. URL: https://www.etsi.org/deliver/etsi_en/300100_300199/3001320301/02.01.01_60/en_3001320301v020101p.pdf (дата звернення: 20.03.2026).

5. ITU-T Recommendation L.1300. Best practices for green data centres. Geneva : International Telecommunication Union, 2014. URL: https://www.itu.int/rec/T-REC-L.1300/en (дата звернення: 20.03.2026).

6. EN 50600-2-2:2019. Information technology - Data centre facilities and infrastructures - Part 2-2: Power supply and distribution. Brussels : CENELEC, 2019. URL: https://knowledge.bsigroup.com/products/information-technology-data-centre-facilities-and-infrastructures-power-supply-and-distribution (дата звернення: 18.03.2026).

7. ДСТУ 7237:2011. Система стандартів безпеки праці. Електробезпека. Загальні вимоги та номенклатура видів захисту. [Чинний від 2011-08-02]. Вид. офіц. Київ : Держспоживстандарт України, 2012. 12 с.

8. IEEE 802.1Q-2018. IEEE Standard for Local and Metropolitan Area Networks - Bridges and Bridged Networks. Piscataway : IEEE, 2018. 1993 p. DOI: https://doi.org/10.1109/IEEESTD.2018.8403927.

9. MQTT Version 5.0 : OASIS Standard. OASIS, 2019. URL: https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html (дата звернення: 22.03.2026).

10. Stallings W. Data and Computer Communications. 10th ed. Upper Saddle River : Pearson Education, 2013. 912 p.

11. IEC 62040-3:2021. Uninterruptible power systems (UPS) - Part 3: Method of specifying the performance and test requirements. Geneva : IEC, 2021. URL: https://webstore.iec.ch/publication/64007 (дата звернення: 22.03.2026).

12. ДСТУ ISO 7010:2019. Графічні символи. Кольори безпеки та знаки безпеки. Зареєстровані знаки безпеки. [Чинний від 2020-01-01]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2020. 116 с.

13. Андрєєв А. І., Банзак О. В. Джерела безперебійного живлення телекомунікаційних і комп'ютерних систем : навч. посіб. Одеса : ОНАЗ ім. О. С. Попова, 2010. URL: https://duikt.edu.ua/uploads/l_15_52029249.pdf (дата звернення: 25.03.2026).

14. Griffor E. R., Greer C., Wollman D. A., Burns M. J. Framework for Cyber-Physical Systems: Volume 1, Overview. NIST Special Publication 1500-201. Gaithersburg : National Institute of Standards and Technology, 2017. 48 p. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf (дата звернення: 18.03.2026).

15. Stouffer K., Pillitteri V., Lightman S., Abrams M., Hahn A. Guide to Industrial Control Systems (ICS) Security : NIST Special Publication 800-82 Rev. 2. Gaithersburg : National Institute of Standards and Technology, 2015. 247 p. URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf (дата звернення: 20.03.2026).

16. ETSI EN 300 132-3 V2.3.1. Environmental Engineering (EE); Power supply interface at the input to ICT equipment; Part 3: Up to 400 V Direct Current (DC). Sophia Antipolis : ETSI, 2023. URL:

https://www.etsi.org/deliver/etsi_en/300100_300199/30013203/02.03.01_60/en_30013203v020301p.pdf (дата звернення: 23.03.2026).

17. ETSI EN 300 132-3-1 V2.1.1. Environmental Engineering (EE); Power supply interface at the input to telecommunications and datacom equipment; Part 3-1: Operated by rectified current source up to 400 V. Sophia Antipolis : ETSI, 2012. URL: https://www.etsi.org/deliver/etsi_en/300100_300199/3001320301/02.01.01_60/en_3001320301v020101p.pdf (дата звернення: 20.03.2026).

18. ITU-T Recommendation L.1200. Direct current power feeding interface up to 400 V at the input to telecommunication and ICT equipment. Geneva : International Telecommunication Union, 2012. URL: https://www.itu.int/rec/T-REC-L.1200-201205-I/en (дата звернення: 23.03.2026).

19. ITU-T Recommendation L.1300. Best practices for green data centres. Geneva : International Telecommunication Union, 2014. URL: https://www.itu.int/rec/T-REC-L.1300/en (дата звернення: 20.03.2026).

20. EN 50600-2-2:2019. Information technology - Data centre facilities and infrastructures - Part 2-2: Power supply and distribution. Brussels : CENELEC, 2019. URL: https://knowledge.bsigroup.com/products/information-technology-data-centre-facilities-and-infrastructures-power-supply-and-distribution (дата звернення: 18.03.2026).

21. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0 : NIST Special Publication 1108r4. Gaithersburg : National Institute of Standards and Technology, 2021. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1108r4.pdf (дата звернення: 23.03.2026).

22. ISA/IEC 62443 Series of Standards : Security for Industrial Automation and Control Systems. Research Triangle Park : ISA, 2023. URL: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards (дата звернення: 24.03.2026).

23. ENISA. Smart Grid Security: Recommendations for Europe and Member States. Heraklion : European Union Agency for Cybersecurity, 2012. URL:

https://www.enisa.europa.eu/publications/ENISA-smart-grid-security-recommendations (дата звернення: 24.03.2026).

24. ENISA. Appropriate Security Measures for Smart Grids. Heraklion : European Union Agency for Cybersecurity, 2012. URL: https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids (дата звернення: 24.03.2026).

25. ETSI EN 303 472 V1.1.1. Environmental Engineering (EE); Energy efficiency measurement methodology and metrics for telecommunication equipment. Sophia Antipolis : ETSI, 2018. URL: https://www.etsi.org/deliver/etsi_en/303400_303499/303472/01.01.01_60/en_303472v010101p.pdf (дата звернення: 24.03.2026).

26. ETSI ES 203 228 V1.4.1. Environmental Engineering (EE); Assessment of mobile network energy efficiency. Sophia Antipolis : ETSI, 2022. URL: https://www.etsi.org/deliver/etsi_es/203200_203299/203228/01.04.01_60/es_203228v010401p.pdf (дата звернення: 24.03.2026).

27. Cabrera-Tobar A., Grimaccia F., Leva S. Energy Resilience in Telecommunication Networks: A Comprehensive Review of Strategies and Challenges. *Energies*. 2023. Vol. 16, No. 18. Article 6633. DOI: https://doi.org/10.3390/en16186633.

28. Safari A., Blaabjerg F., Oshnoei A. A research-industry perspective of battery systems technology for next-generation data centers. *Journal of Energy Storage*. 2026. Vol. 152, Part C. Article 120386. DOI: https://doi.org/10.1016/j.est.2026.120386.

29. Varnavskiy K., Nepsha F., Chen Q., Ermakov A., Zhironkin S. Reliability Assessment of the Configuration of Dynamic Uninterruptible Power Sources: A Case of Data Centers. *Energies*. 2023. Vol. 16, No. 3. Article 1419. DOI: https://doi.org/10.3390/en16031419.

30. Paś J. Issues Related to Power Supply Reliability in Integrated Electronic Security Systems Operated in Buildings and Vast Areas. *Energies*. 2023. Vol. 16, No. 8. Article 3351. DOI: https://doi.org/10.3390/en16083351.

31. Matko V., Brezovec B. Improved Data Center Energy Efficiency and Availability with a Multilayer Node Event Processing Method. *Energies*. 2018. Vol. 11, No. 9. Article 2478. DOI: https://doi.org/10.3390/en11092478.

32. TM Forum. Autonomous Networks Project. Morristown : TM Forum, 2024. URL: https://www.tmforum.org/autonomous-networks-project/ (дата звернення: 25.03.2026).

33. IEC 61850. Communication Networks and Systems for Power Utility Automation. Geneva : IEC, 2023. URL: https://iec61850.dvl.iec.ch/ (дата звернення: 25.03.2026).

34. Rajkumar R., Lee I., Sha L., Stankovic J. Cyber-Physical Systems: The Next Computing Revolution. *Proceedings of the 47th Design Automation Conference (DAC)*. New York : ACM, 2010. P. 731–736. DOI: https://doi.org/10.1145/1837274.1837461.

35. Lee E. A. Cyber Physical Systems: Design Challenges. *11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing (ISORC)*. Piscataway : IEEE, 2008. P. 363–369. DOI: https://doi.org/10.1109/ISORC.2008.25.

36. Kim K.-D., Kumar P. R. Cyber-Physical Systems: A Perspective at the Centennial. *Proceedings of the IEEE*. 2012. Vol. 100, Special Centennial Issue. P. 1287–1308. DOI: https://doi.org/10.1109/JPROC.2012.2189792.

37. Shi W., Cao J., Zhang Q., Li Y., Xu L. Edge Computing: Vision and Challenges. *IEEE Internet of Things Journal*. 2016. Vol. 3, No. 5. P. 637–646. DOI: https://doi.org/10.1109/JIOT.2016.2579198.

38. EN 50600-1:2019. Information technology - Data centre facilities and infrastructures - Part 1: General concepts. Brussels : CENELEC, 2019. URL: https://www.cenelec.eu/ (дата звернення: 26.03.2026).

39. EN 50600-2-1:2022. Information technology - Data centre facilities and infrastructures - Part 2-1: Building construction. Brussels : CENELEC, 2022. URL: https://www.cenelec.eu/ (дата звернення: 26.03.2026).

40. ETSI GR ENI 004 V2.1.1. Experienced Networked Intelligence (ENI); Terminology for Main Concepts in ENI. Sophia Antipolis : ETSI, 2019. URL: https://www.etsi.org/deliver/etsi_gr/ENI/001_099/004/ (дата звернення: 26.03.2026).

41. ITU-T Recommendation Y.2060. Overview of the Internet of Things. Geneva : International Telecommunication Union, 2012. URL: https://www.itu.int/rec/T-REC-Y.2060/en (дата звернення: 26.03.2026).

42. ITU-T Recommendation Y.4100. Common requirements of the Internet of Things. Geneva : International Telecommunication Union, 2016. URL: https://www.itu.int/rec/T-REC-Y.4100/en (дата звернення: 26.03.2026).

43. IEC 62040-1:2017. Uninterruptible power systems (UPS) - Part 1: Safety requirements. Geneva : IEC, 2017. URL: https://webstore.iec.ch/publication/26754 (дата звернення: 26.03.2026).

44. IEC 62040-2:2016. Uninterruptible power systems (UPS) - Part 2: Electromagnetic compatibility (EMC) requirements. Geneva : IEC, 2016. URL: https://webstore.iec.ch/publication/24887 (дата звернення: 26.03.2026).

45. IEC 60896-21:2004. Stationary lead-acid batteries - Part 21: Valve regulated types - Methods of test. Geneva : IEC, 2004. URL: https://webstore.iec.ch/publication/3836 (дата звернення: 26.03.2026).

46. IEC 62133-2:2017. Secondary cells and batteries containing alkaline or other non-acid electrolytes - Safety requirements for portable sealed secondary lithium cells, and for batteries made from them, for use in portable applications - Part 2: Lithium systems. Geneva : IEC, 2017. URL: https://webstore.iec.ch/publication/30524 (дата звернення: 26.03.2026).

47. IEC 62485-2:2010. Safety requirements for secondary batteries and battery installations - Part 2: Stationary batteries. Geneva : IEC, 2010. URL: https://webstore.iec.ch/publication/7060 (дата звернення: 26.03.2026).

48. ДСТУ IEC 62040-3:2023. Джерела безперебійного живлення (ДБЖ). Частина 3. Метод визначення технічних характеристик та вимоги до випробувань. [Чинний від 2024-01-01]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2023. 78 с.

49. ДСТУ EN 50600-2-2:2022. Інформаційні технології. Об'єкти та інфраструктури центрів обробки даних. Частина 2-2. Електропостачання та розподіл. [Чинний від 2023-01-01]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2022. 52 с.

50. Birolini A. Reliability Engineering: Theory and Practice. 8th ed. Berlin : Springer, 2017. 651 p.

51. Rausand M., Høyland A. System Reliability Theory: Models, Statistical Methods, and Applications. 2nd ed. Hoboken : Wiley-Interscience, 2004. 664 p.

52. Telcordia GR-63-CORE. Network Equipment-Building System (NEBS) Requirements: Physical Protection. Piscataway : Telcordia, 2012. 248 p. URL: https://telecom-info.njdepot.ericsson.se/site-cgi/ido/docs.cgi?ID=SEARCH&DOCUMENT=GR-63 (дата звернення: 27.03.2026).

53. Telcordia GR-1275-CORE. Generic Requirements for Network Element / Network System (NE/NS) Time Stamping and Synchronization. Piscataway : Telcordia, 2017. URL: https://telecom-info.njdepot.ericsson.se/ (дата звернення: 27.03.2026).

54. OPC Unified Architecture - Part 1: Overview and Concepts. Scottsdale : OPC Foundation, 2022. URL: https://reference.opcfoundation.org/ (дата звернення: 27.03.2026).

55. Modbus Application Protocol Specification V1.1b3. Hopkinton : Modbus Organization, 2012. URL: https://modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf (дата звернення: 27.03.2026).

56. Case J., Mundy R., Partain D., Stewart B. Introduction and Applicability Statements for Internet Standard Management Framework : RFC 3410. Reston : Internet Society, 2002. URL: https://www.rfc-editor.org/rfc/rfc3410 (дата звернення: 27.03.2026).

57. Bjorklund M. YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF) : RFC 6020. Fremont : IETF, 2010. URL: https://www.rfc-editor.org/rfc/rfc6020 (дата звернення: 27.03.2026).

58. Panciatici P., Bareux G., Wehenkel L. Operating in the Fog: Security Management Under Uncertainty. *IEEE Power and Energy Magazine*. 2012. Vol. 10, No. 5. P. 40–49. DOI: https://doi.org/10.1109/MPE.2012.2205318.

59. Farzaneh H., Malehmirchegini L., Bejan A., Afolabi T., Mulumba A., Daka P. P. Artificial Intelligence Evolution in Smart Buildings for Energy Efficiency. *Applied Sciences*. 2021. Vol. 11, No. 2. Article 763. DOI: https://doi.org/10.3390/app11020763.

60. Farhangi H. The Path of the Smart Grid. *IEEE Power and Energy Magazine*. 2010. Vol. 8, No. 1. P. 18–28. DOI: https://doi.org/10.1109/MPE.2009.934876.

61. Alam M. M., Malik H., Khan M. I., Pardy T., Kuusik A., Le Moullec Y. A Survey on the Roles of Communication Technologies in IoT-Based Personalized Healthcare Applications. *IEEE Access*. 2018. Vol. 6. P. 36611–36631. DOI: https://doi.org/10.1109/ACCESS.2018.2853148.

62. ITU-T Recommendation G.8013/Y.1731. Operations, administration and maintenance (OAM) functions and mechanisms for Ethernet-based networks. Geneva : International Telecommunication Union, 2015. URL: https://www.itu.int/rec/T-REC-G.8013/en (дата звернення: 28.03.2026).

63. 3GPP TS 28.552. Management and Orchestration; 5G performance measurements. Release 17. Sophia Antipolis : 3GPP, 2022. URL: https://www.3gpp.org/ftp/Specs/archive/28_series/28.552/ (дата звернення: 28.03.2026).

64. ANSI/TIA-942-B-2017. Telecommunications Infrastructure Standard for Data Centers. Arlington : Telecommunications Industry Association, 2017. URL: https://tiaonline.org/ (дата звернення: 28.03.2026).

65. ISO/IEC 30134-2:2016. Information technology - Data centres - Key performance indicators - Part 2: Power usage effectiveness (PUE). Geneva : ISO, 2016. URL: https://www.iso.org/standard/63451.html (дата звернення: 28.03.2026).

66. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи управління інформаційною безпекою. Вимоги. [Чинний від 2024-01-01]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2024. 36 с.

67. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 28.03.2026).

68. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX. *Відомості Верховної Ради України*. 2022. № 2. Ст. 3. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 28.03.2026).

69. Про телекомунікації : Закон України від 18.11.2003 р. № 1280-IV. *Відомості Верховної Ради України*. 2004. № 12. Ст. 155. URL: https://zakon.rada.gov.ua/laws/show/1280-15 (дата звернення: 28.03.2026).

70. Про електроенергетику : Закон України від 16.10.1997 р. № 575/97-ВР. *Відомості Верховної Ради України*. 1998. № 1. Ст. 1. URL: https://zakon.rada.gov.ua/laws/show/575/97-вр (дата звернення: 28.03.2026).

71. Правила улаштування електроустановок. 5-те вид., переробл. й доп. Київ : Міненерговугілля України, 2017. 736 с.

72. Про затвердження Порядку формування переліку об'єктів критичної інформаційної інфраструктури, включення таких об'єктів до державного реєстру об'єктів критичної інформаційної інфраструктури та його ведення : постанова Кабінету Міністрів України від 09.10.2020 р. № 943. URL: https://zakon.rada.gov.ua/laws/show/943-2020-п (дата звернення: 29.03.2026).

73. ISO/IEC 27019:2017. Information technology - Security techniques - Information security controls for the energy utility industry. Geneva : ISO, 2017. URL: https://www.iso.org/standard/68091.html (дата звернення: 29.03.2026).

74. IEEE 1547-2018. IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces. Piscataway : IEEE, 2018. 138 p. DOI: https://doi.org/10.1109/IEEESTD.2018.8332112.

75. IEC 62351 Series. Power systems management and associated information exchange - Data and communications security. Geneva : IEC, 2023. URL: https://www.iec.ch/ (дата звернення: 29.03.2026).

76. NERC CIP Standards. Critical Infrastructure Protection Reliability Standards. Atlanta : North American Electric Reliability Corporation, 2023. URL: https://www.nerc.com/ (дата звернення: 29.03.2026).

77. CIGRÉ Technical Brochure 762. Cyber Security Requirements for PACS and the Resilience of EPCIP. Paris : CIGRÉ, 2019. URL: https://www.cigre.org/ (дата звернення: 29.03.2026).

78. IEEE NT 2030-2011. IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads. Piscataway : IEEE, 2011. DOI: https://doi.org/10.1109/IEEESTD.2011.6018239.

79. IEC 61970. Energy management system application program interface (EMS-API). Geneva : IEC, 2022. URL: https://www.iec.ch/ (дата звернення: 29.03.2026).

80. IEC 61968. Application integration at electric utilities - System interfaces for distribution management. Geneva : IEC, 2022. URL: https://www.iec.ch/ (дата звернення: 29.03.2026).

ДОДАТОК А

(обов’язковий)

Лістинг основних модулів програмного забезпечення

Модуль «Обчислення стану акумуляторного масиву»

```
"""Battery state calculation module."""
from dataclasses import dataclass
from datetime import datetime
from typing import List
import statistics

from .models import BatteryBank, TelemetrySnapshot
from .config import BATTERY_HEALTH_WEIGHTS_LIFEPO4


@dataclass
class BatteryHealth:
    soh: float
    temp_score: float
    cycle_score: float
    age_score: float
    integral: float
    autonomy_minutes: float


def lifepo4_temp_factor(temp_c: float) -> float:
    """Temperature correction factor for LiFePO4 capacity.

    Returns 1.0 in the optimal range (15-30°C),
    decreases linearly outside this range.
    """
    if 15 <= temp_c <= 30:
        return 1.0
    if temp_c < 15:
        return max(0.65, 1.0 - (15 - temp_c) * 0.01)
    return max(0.85, 1.0 - (temp_c - 30) * 0.005)


def peukert_factor(load_a: float, capacity_ah: float) -> float:
    """Peukert effect derate factor for LiFePO4 (k ≈ 1.05)."""
    c_rate = load_a / capacity_ah
    if c_rate < 0.5:
        return 1.0
    return 1.0 + (c_rate - 0.5) * 0.05


def calculate_battery_health(
    battery: BatteryBank,
    snapshot: TelemetrySnapshot,
) -> BatteryHealth:
    weights = BATTERY_HEALTH_WEIGHTS_LIFEPO4

    # SoH from coulomb counting + voltage curve
    soh = battery.measured_capacity / battery.nominal_capacity
```

```
    # Temperature score
    avg_temp = statistics.mean(snapshot.cell_temperatures)
    if 15 <= avg_temp <= 30:
        temp_score = 1.0
    elif avg_temp < 15:
        temp_score = max(0.0, 1.0 - (15 - avg_temp) * 0.05)
    else:
        temp_score = max(0.0, 1.0 - (avg_temp - 30) * 0.04)

    # Cycle score
    cycle_score = max(0.0, 1.0 - battery.cycles_used / battery.max_cycles)

    # Age score
    age_years = (datetime.utcnow() - battery.installation_date).days / 365.0
    age_score = max(0.0, 1.0 - age_years / battery.expected_lifetime_years)

    integral = (
        weights[0] * soh
        + weights[1] * temp_score
        + weights[2] * cycle_score
        + weights[3] * age_score
    )

    # Autonomy prediction
    effective_capacity = battery.nominal_capacity * soh
    temp_factor = lifepo4_temp_factor(avg_temp)
    derate = peukert_factor(snapshot.current_load_a, battery.nominal_capacity)
    autonomy_hours = (effective_capacity * temp_factor) / (
        snapshot.current_load_a * derate
    )

    return BatteryHealth(
        soh=soh,
        temp_score=temp_score,
        cycle_score=cycle_score,
        age_score=age_score,
        integral=integral,
        autonomy_minutes=autonomy_hours * 60,
    )
```

Модуль «Класифікації стану об'єкта»

```
"""Object state classification engine."""
from enum import Enum
from typing import List

from .events import Event
from .models import ObjectSnapshot


class ObjectState(str, Enum):
    NORMAL = "Normal"
    DEGRADED = "Degraded"
    PRE_EMERGENCY = "Pre-emergency"
    EMERGENCY = "Emergency"
    RECOVERY = "Recovery"
    MAINTENANCE = "Maintenance"
```

```
def classify_state(
    current_state: ObjectState,
    snapshot: ObjectSnapshot,
    events: List[Event],
) -> ObjectState:
    """Apply state transition rules to compute next state."""

    # Priority 1: emergency events override everything
    if any(e.type in {"fire_detected", "flood_detected"} for e in events):
        return ObjectState.EMERGENCY
    if snapshot.min_critical_autonomy_minutes() < 5:
        return ObjectState.EMERGENCY

    # Maintenance is set explicitly by operator
    if current_state == ObjectState.MAINTENANCE:
        if any(e.type == "maintenance_finished" for e in events):
            return ObjectState.NORMAL
        return ObjectState.MAINTENANCE

    # Pre-emergency conditions
    if (
        snapshot.s_object < 0.65
        or snapshot.min_critical_autonomy_minutes() < 15
        or any(e.type == "second_redundancy_lost" for e in events)
    ):
        return ObjectState.PRE_EMERGENCY

    # Degraded conditions
    if (
        snapshot.s_object < 0.85
        or any(e.type == "redundancy_lost" for e in events)
        or snapshot.min_critical_autonomy_minutes() < 30
        or snapshot.max_critical_zone_temp() > 35
    ):
        return ObjectState.DEGRADED

    # If we were in degraded/emergency and conditions cleared
    if current_state in {ObjectState.DEGRADED, ObjectState.PRE_EMERGENCY}:
        return ObjectState.RECOVERY

    if current_state == ObjectState.RECOVERY:
        # Stable for at least 15 minutes
        if snapshot.stable_minutes >= 15:
            return ObjectState.NORMAL
        return ObjectState.RECOVERY

    return ObjectState.NORMAL
```

Модуль «Протоколу Modbus»

```
"""Modbus TCP/RTU adapter for telemetry collection."""
import asyncio
import struct
from typing import Optional

from pymodbus.client import AsyncModbusTcpClient
```

```
from .base import BaseAdapter, RawValue, Quality
from ..models import PointDef


class ModbusAdapter(BaseAdapter):
    """Adapter for Modbus TCP/RTU protocols."""

    def __init__(self, config: dict):
        super().__init__(config)
        self._clients: dict = {}

    async def _get_client(self, device: dict) -> AsyncModbusTcpClient:
        key = (device["host"], device["port"])
        if key not in self._clients:
            client = AsyncModbusTcpClient(device["host"], port=device["port"],
                                          timeout=device.get("timeout", 2))
            await client.connect()
            self._clients[key] = client
        return self._clients[key]

    def _decode(self, registers, data_type: str):
        if data_type == "uint16":
            return registers[0]
        if data_type == "int16":
            v = registers[0]
            return v - 65536 if v >= 32768 else v
        if data_type == "uint32":
            return (registers[0] << 16) | registers[1]
        if data_type == "int32":
            v = (registers[0] << 16) | registers[1]
            return v - 4294967296 if v >= 2147483648 else v
        if data_type == "float32":
            packed = struct.pack(">HH", registers[0], registers[1])
            return struct.unpack(">f", packed)[0]
        raise ValueError(f"Unsupported data type: {data_type}")

    async def read_point(self, point: PointDef) -> RawValue:
        client = await self._get_client(point.device)
        try:
            if point.register_type == "holding":
                rsp = await client.read_holding_registers(
                    point.address, point.count, slave=point.slave_id)
            elif point.register_type == "input":
                rsp = await client.read_input_registers(
                    point.address, point.count, slave=point.slave_id)
            elif point.register_type == "coil":
                rsp = await client.read_coils(
                    point.address, point.count, slave=point.slave_id)
            else:
                rsp = await client.read_discrete_inputs(
                    point.address, point.count, slave=point.slave_id)

            if rsp.isError():
                return RawValue(None, Quality.BAD,
                                comment=f"Modbus error: {rsp}")

            if point.register_type in ("holding", "input"):
                value = self._decode(rsp.registers, point.data_type)
```

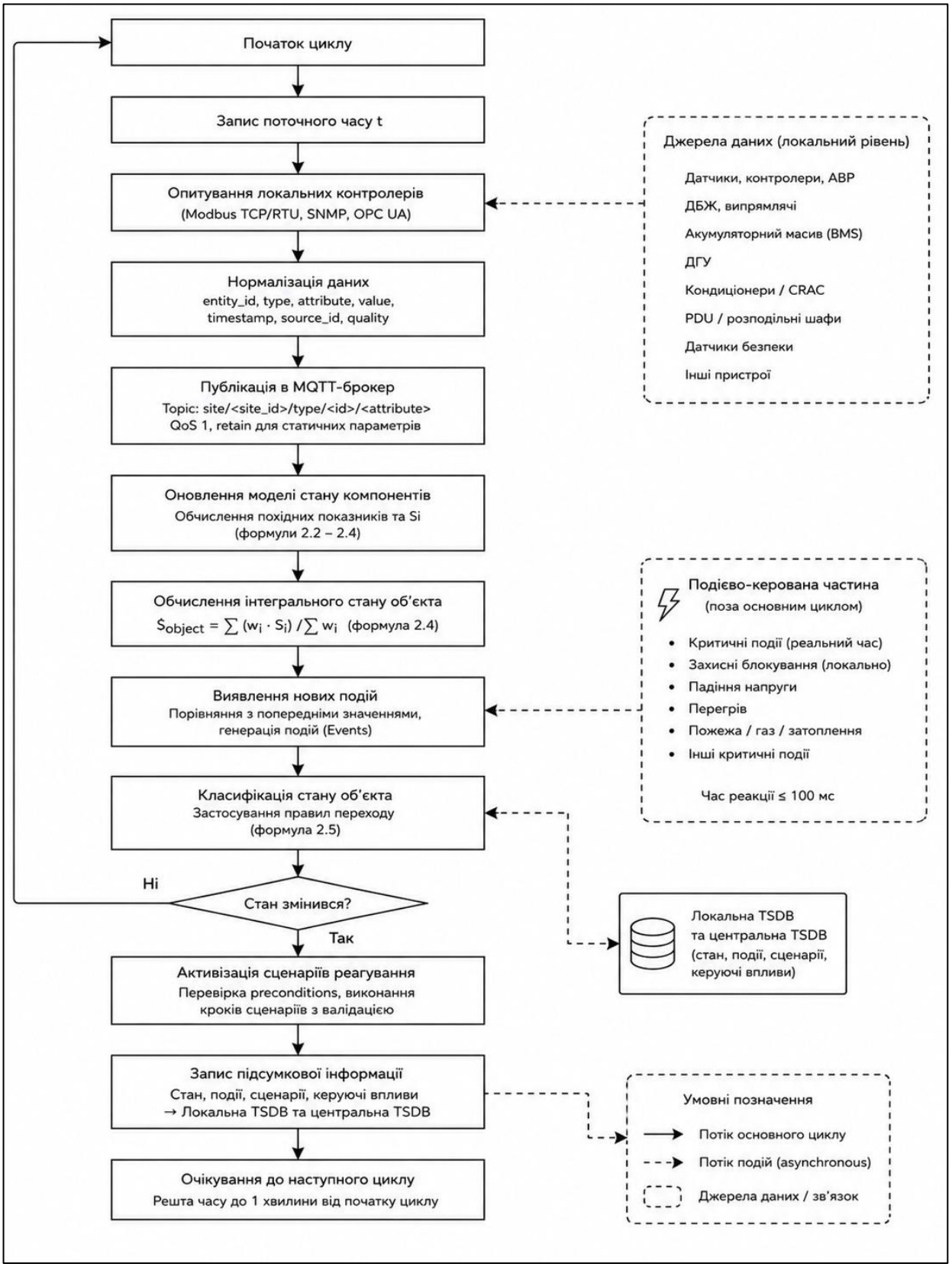
```
            if point.scale:
                value = value * point.scale
            if point.offset:
                value = value + point.offset
        else:
            value = bool(rsp.bits[0])
        return RawValue(value, Quality.GOOD)

    except asyncio.TimeoutError:
        return RawValue(None, Quality.BAD, comment="Timeout")
    except Exception as exc:
        return RawValue(None, Quality.BAD, comment=str(exc))
```

ДОДАТОК Б

(обов’язковий)

Блок-схема основного циклу алгоритму функціонування кіберфізичної системи



ДОДАТОК В

(обов'язковий)

Тези у VII Міжнародній науково-практичній конференції Таврійського національного університету імені В. І. Вернадського

Кіберфізична система управління системами енергозабезпечення центрів комутації телекомунікаційних мереж

Сучасний стан телекомунікаційної інфраструктури України характеризується зростаючими вимогами до надійності та безперебійності функціонування в умовах цифрової трансформації та нестабільності зовнішнього електропостачання, зумовленої воєнним станом. Центри комутації телекомунікаційних мереж є критично важливими об'єктами, що безпосередньо визначають якість надання цифрових послуг. Ефективне управління системами енергозабезпечення таких об'єктів неможливе в рамках традиційних ізольованих підходів [7].

Концепція кіберфізичних систем (Cyber-Physical Systems, CPS) передбачає тісну інтеграцію обчислювальних компонентів із фізичними процесами через сенсорні мережі, вбудовані контролери та алгоритми інтелектуального управління. Застосування принципів CPS до задач управління енергозабезпеченням телекомунікаційних вузлів дозволяє підвищити ефективність функціонування обладнання, скоротити витрати на технічне обслуговування та мінімізувати час простою у разі аварійних ситуацій [5].

Стандарт EN 50600-2-2 визначає вимоги до систем електропостачання та розподілу об'єктів інформаційно-комунікаційних технологій, формуючи критерії надійності, резервування та безперервності роботи, що безпосередньо слугують методологічною основою при постановці задачі кіберфізичного управління енергозабезпеченням центрів комутації [1].

Аналіз предметної області виявив три взаємопов'язані площини об'єкта: енергетичну (зовнішнє електропостачання, ДБЖ, дизель-генераторні установки, акумуляторні батареї); інформаційно-керуючу (контролери, шлюзи,

SCADA/DCIM-рівні, аналітичні підсистеми); експлуатаційно-організаційну (регламенти обслуговування, процедури аварійного реагування, кібербезпека). Встановлено, що локальна оптимізація окремого вузла не гарантує стійкості системи загалом [3].

Порівняльний аналіз існуючих архітектурних підходів (централізованої AC, DC-орієнтованої та гібридної AC/DC архітектур) показав, що жоден з них в ізольованому вигляді не вирішує завдання комплексного кіберфізичного управління. Централізовані AC-системи мають зайві каскади перетворення енергії та критичну залежність від UPS як вузла концентрації ризику. DC-орієнтовані системи, хоча й оптимальні для телекомунікаційного навантаження, потребують додаткового AC-контуру для допоміжного обладнання. Гібридні архітектури є найбільш гнучкими, однак без єдиної інформаційної моделі перетворюються на набір ізольованих підсистем, які складно адмініструвати [2].

Запропонована архітектура кіберфізичної системи управління базується на взаємодоповнювальних підходах та включає три ієрархічні рівні: нижній (локальні контролери з гарантованим збором телеметрії в реальному часі та виконанням базових сценаріїв захисту навіть за втрати зв’язку), середній (нормалізація даних, координація між енергетичним та кліматичним контурами) та верхній (аналітика, довгострокове прогнозування та кореляція з мережевими платформами оператора). Така побудова поєднує локальну автономність з централізованою інтелектуальною підтримкою [3].

Ключовою особливістю запропонованого підходу є єдина інформаційна модель об’єкта з уніфікованим каталогом сутностей: ввід живлення, секція шин, випрямляч, батарейна гілка, генератор, АВР, кондиціонер, група критичного навантаження, датчик середовища. Для кожної сутності визначені атрибути, ідентифікатор, місце в ієрархії, критичність та зв’язки з іншими компонентами. Така модель є основою цифрового представлення об’єкта, що дозволяє перейти від простого опитування пристроїв до повноцінної кіберфізичної взаємодії [3].

Предиктивна аналітика реалізується через сукупний індикатор технічного стану батарейного контуру, що враховує температуру, струми заряду/розряду,

внутрішній опір, історію циклів та вікові характеристики. Поряд із цим для кліматичних підсистем оцінюється тепловий ризик та здатність підтримувати допустимий температурно-вологісний режим. Координація енергетичного та кліматичного контурів є принциповою, оскільки перегрів суттєво прискорює старіння акумуляторів та може спричинити аварійне вимкнення частини навантаження [4].

Пріоритизація навантаження за рівнями критичності дозволяє продовжити роботу ядра мережі навіть у сценаріях критичного дефіциту енергоресурсів. Для типових аварійних сценаріїв (зникнення зовнішнього живлення, збій UPS-модуля, зростання температури, відмова генератора) сформовані алгоритми реагування з визначенням дій, що виконуються автоматично, та дій, що рекомендуються оператору [7].

Архітектура підтримує інтеграцію різнорідних протоколів на нижньому рівні (Modbus RTU/TCP, SNMP, MQTT, OPC UA) при нормалізації даних на верхньому рівні. Це забезпечує поетапне підключення нових джерел даних без повного перепроєктування системи. Вимоги до кібербезпеки відповідають стандартам ISA/IEC 62443 та рекомендаціям NIST SP 800-82: зонування мереж, контроль доступу, захищений міжрівневий обмін даними, журналювання дій персоналу [3; 6].

Таким чином, запропонована кіберфізична система управління дозволяє подолати ключові проблеми традиційних підходів: фрагментарність моніторингу, реактивний характер технічної експлуатації та неузгодженість енергетичного і кліматичного контурів. Впровадження такої системи дозволить зменшити ризик раптових відмов, скоротити час виявлення та локалізації проблем, підвищити обґрунтованість експлуатаційних рішень та покращити використання енергетичних ресурсів критичної телекомунікаційної інфраструктури [5].

Список використаних джерел:

1. EN 50600-2-2:2019. Information technology. Data centre facilities and infrastructures. Part 2-2: Power supply and distribution. 2019. URL:

https://knowledge.bsigroup.com/products/information-technology-data-centre-facilities-and-infrastructures-power-supply-and-distribution (дата звернення: 18.03.2026).

2. ETSI EN 300 132-3-1 V2.1.1. Environmental Engineering (EE); Power supply interface at the input to telecommunications and datacom (ICT) equipment; Part 3-1: Direct current source up to 400 V. 2012. URL: https://www.etsi.org/deliver/etsi_en/300100_300199/3001320301/02.01.01_60/en_3001320301v020101p.pdf (дата звернення: 20.03.2026).

3. Griffor E., Greer C., Wollman D., Burns M. Framework for Cyber-Physical Systems: Volume 1, Overview. NIST Special Publication 1500-201. Gaithersburg, 2017. 48 p. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf (дата звернення: 18.03.2026).

4. ITU-T Recommendation L.1300. Best practices for green data centres. Geneva, 2014. URL: https://www.itu.int/rec/T-REC-L.1300/en (дата звернення: 20.03.2026).

5. Rajkumar R., Lee I., Sha L., Stankovic J. Cyber-Physical Systems: The Next Computing Revolution. Proceedings of the 47th Design Automation Conference (DAC). New York, 2010. P. 731–736. DOI: 10.1145/1837274.1837461.

6. Stouffer K., Pillitteri V., Lightman S., Abrams M., Hahn A. Guide to Industrial Control Systems (ICS) Security. NIST SP 800-82 Rev. 2. Gaithersburg, 2015. 247 p. URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf (дата звернення: 20.03.2026).

7. Правила технічної експлуатації електроустановок споживачів. Затверджено наказом Міністерства енергетики України від 13.02.2012 р. № 91. Київ, 2012. 272 с.

ДОДАТОК Г

(обов'язковий)

Програма конференції

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТАВРІЙСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ В.І. ВЕРНАДСЬКОГО
(Навчально-науковий інститут управління,
економіки та природокористування – ННІУЕП)
EUROPEAN INSTITUTE OF FURTHER EDUCATION, Slovakia
ACADEMY OF ECONOMIC STUDIES OF MOLDOVA, Republic of Moldova
МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ЖИТОМИРСЬКИЙ ЕКОНОМІКО-ГУМАНІТАРНИЙ ІНСТИТУТ
УНІВЕРСИТЕТУ «УКРАЇНА»
КЛАСИЧНИЙ ПРИВАТНИЙ УНІВЕРСИТЕТ (м. Запоріжжя)
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ МОЛДОВИ
ASSOTSIATION AGROVOLTATYKY UKRAINY
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ

VII
Міжнародна науково-практична конференція

«ТЕОРЕТИКО-ПРАКТИЧНІ ЗАСАДИ УПРАВЛІННЯ, ЕКОНОМІКИ ТА ПРИРОДОКОРИСТУВАННЯ: АСПЕКТИ РЕІНТЕГРАЦІЇ КРИМУ В ГОСПОДАРСЬКИЙ КОМПЛЕКС УКРАЇНИ»

31 березня 2026 року
м. Київ

О Р Г А Н І З А Ц І Й Н И Й К О М І Т Е Т

Голова оргкомітету: Бортняк В.А. – доктор юридичних наук, професор, ректор ТНУ імені В.І. Вернадського

Заступник голови оргкомітету: Горник В.Г. – доктор наук з державного управління, професор, директор ННІУЕП ТНУ імені В.І. Вернадського

Члени оргкомітету:

Парубчак І.О. – доктор наук з державного управління, професор, ректор Львівського національного університету ветеринарної медицини та біотехнологій імені С.З. Гжицького

Тарасенко Д.Л. – доктор економічних наук, професор, директор навчально-наукового інституту управління Маріупольського державного університету

Покатаєв П.С. – доктор наук з державного управління, доктор юридичних наук, професор, перший проректор Класичного приватного університету

Домбровська С.М. – доктор наук з державного управління, професор, заслужений працівник освіти України, проректор з наукової роботи Національного аерокосмічного університету «Харківський авіаційний інститут»

Щелкунов В.І. – доктор економічних наук, професор, Президент Українського Національного Комітету Міжнародної торгової Палати

Безус П.І. – кандидат економічних наук, доцент, завідувач кафедри менеджменту та міжнародних економічних відносин ННІУЕП ТНУ імені В.І. Вернадського

Петровська І.О. – кандидат економічних наук, доцент, завідувач кафедри публічного управління, туризму та готельно-ресторанної справи ННІУЕП ТНУ імені В.І. Вернадського

Путінцев А.В. – кандидат економічних наук, доцент, завідувач кафедри фінансів та обліку ННІУЕП ТНУ імені В.І. Вернадського

Євмєшкіна О.Л. – доктор наук з державного управління, професор кафедри публічного управління, туризму та готельно-ресторанної справи ННІУЕП ТНУ імені В.І. Вернадського

Stratan Alexandr – Habilitated Doctor, University Professor, Rector, Academy of Economic Studies of Moldova, Republic of Moldova

Дульський Іон Філіпович – доцент Державного університету Молдови

Jozef ZATKO – LL.M, MBA, Honor. Prof. Mult., President European Institute of Further Education, Slovakia

Кучерявий В.М. – PhD з публічного управління та адміністрування, Голова Ради молодих вчених ТНУ імені В.І. Вернадського

Шемелинець І.І. – кандидат юридичних наук, доцент, проректор з навчально-методичної роботи Державного податкового університету

Шановні науковці, молоді вчені та студенти!

Таврійський національний університет імені В.І. Вернадського запрошує Вас взяти участь у VII Міжнародній науково-практичній конференції «Теоретико-практичні засади управління, економіки та природокористування: аспекти реінтеграції Криму в господарський комплекс України», що відбудеться 31 березня 2026 року.

Основні тематичні напрями роботи конференції:

1. Відновлення публічного управління та цифрова трансформація державних інститутів.
2. Інформаційні технології та кіберфізичні системи в управлінні інфраструктурою.
3. Розвиток фінансової системи України в умовах воєнного стану та повоєнного відновлення.
4. Вплив геополітичних процесів на розвиток світового господарства та міжнародних економічних відносин.
5. Менеджмент, підприємництво та інновації в умовах становлення інформаційного суспільства.

За результатами проведення міжнародної науково-практичної конференції планується видання електронного збірника матеріалів конференції та розміщення його на сайті ТНУ імені В.І. Вернадського. Збірник тез доповідей та сертифікати будуть надіслані всім учасникам на електронну пошту після 25 травня 2026 року.

Участь у конференції БЕЗКОШТОВНА.
Робочі мови конференції – українська, англійська.

Контакти оргкомітету: tnu2020konf@ukr.net

РЕЖИМ РОБОТИ КОНФЕРЕНЦІЇ

Конференція проводиться у змішаному форматі: в приміщенні Навчально-наукового інституту управління, економіки та природокористування ТНУ імені В.І. Вернадського за адресою: м. Київ, вулиця Кирилівська, 164, актова зала, та дистанційно за допомогою Google Meet.

09:30 – 10:00	Реєстрація учасників (фойє)
10:00 – 13:00	Пленарне засідання (актова зала / Google Meet)
13:00 – 14:00	Обідня перерва
14:00 – 17:00	Секційні засідання (Google Meet, секційні кімнати)
17:00 – 17:30	Підбиття підсумків конференції. Закриття

Посилання для приєднання до Google Meet буде надіслане учасникам на електронну пошту за 2 доби до початку конференції.

ПРОГРАМА КОНФЕРЕНЦІЇ

ПЛЕНАРНЕ ЗАСІДАННЯ (10:00 – 13:00)

Голова пленарного засідання: Бортняк В.А. – д.ю.н., професор, ректор ТНУ імені В.І. Вернадського
Співголова: Горник В.Г. – д.н.держ.упр., професор, директор ННІУЕП ТНУ імені В.І. Вернадського

10:00 – 10:15
Відкриття конференції. Вступне слово ректора ТНУ імені В.І. Вернадського

10:15 – 10:45
Горник В.Г. Стратегічні орієнтири реінтеграції Криму в господарський комплекс України: управлінський вимір

10:45 – 11:10
Парубчак І.О. Публічне управління в умовах повоєнного відновлення: виклики та інституційні відповіді

11:10 – 11:35
Stratan Alexandr. Integration of Ukraine into European Economic Space: Lessons from Moldova's Experience (Republic of Moldova)

11:35 – 12:00
Домбровська С.М. Реформування системи цивільного захисту в умовах гібридної війни та в постконфліктний період

12:00 – 12:25
Щелкунов В.І. Міжнародна торгова палата та механізми підтримки відновлення економіки України

12:25 – 12:50
Jozef ZATKO. Digital Transformation of Public Administration: European Best Practices for Post-War Recovery (Slovakia)

12:50 – 13:00
Дискусія. Відповіді на запитання

СЕКЦІЯ 1.
ВІДНОВЛЕННЯ ПУБЛІЧНОГО УПРАВЛІННЯ ТА ЦИФРОВА ТРАНСФОРМАЦІЯ ДЕРЖАВНИХ ІНСТИТУТІВ

(14:00 – 17:00, Google Meet)

Бондарук М.В.
ТНУ імені В.І. Вернадського, м. Київ
Кризова комунікація та управління репутацією органів публічної влади в умовах воєнного стану

Логоша В.В.
ТНУ імені В.І. Вернадського, м. Київ
Імплементація досвіду країн ЄС у сфері цифрового врядування в Україні

Музика Ю.Д.
ТНУ імені В.І. Вернадського, м. Київ
Організація надання адміністративних послуг в умовах децентралізації: виклики та перспективи

Студзінський Р.В., Лісний М.В.
Класичний приватний університет, м. Запоріжжя
Механізми забезпечення кібербезпеки органів державної влади: міжнародний та вітчизняний досвід

Ясенчук Х.В.
ННІУЕП ТНУ імені В.І. Вернадського, м. Київ
Державне регулювання інформаційного простору в умовах гібридних загроз

Кисельов Є.В.
Класичний приватний університет, м. Запоріжжя
Публічне управління енергетичною безпекою в контексті реінтеграції тимчасово окупованих територій

Сімак С.В.
Маріупольський державний університет
Реформування публічного управління на деокупованих територіях: правові та організаційні аспекти

Штепа І.М.
ТНУ імені В.І. Вернадського, м. Київ
Електронне урядування як інструмент підвищення ефективності публічної служби

СЕКЦІЯ 2.
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА КІБЕРФІЗИЧНІ СИСТЕМИ В УПРАВЛІННІ ІНФРАСТРУКТУРОЮ

(14:00 – 17:00, Google Meet)

Васьков О.В.
Хмельницький національний університет, м. Хмельницький
Кіберфізична система управління системами енергозабезпечення центрів комутації телекомунікаційних мереж

Марченко О.І.
Хмельницький національний університет, м. Хмельницький
Застосування протоколів SCADA/DCIM для моніторингу критичної телекомунікаційної інфраструктури

Коваленко В.С., Дяченко Т.П.
Державний університет «Житомирська політехніка»
Методи підвищення відмовостійкості вузлів телекомунікаційних мереж на основі штучного інтелекту

Петренко А.М.
Національний університет «Львівська політехніка»
Інтеграція IoT-рішень у системи управління розподіленою телекомунікаційною інфраструктурою

Шевченко О.Л.
Одеська національна академія зв'язку ім. О.С. Попова
Архітектурні підходи до побудови захищених промислових мереж передачі даних

Лук'яненко І.В., Мороз Д.С.
Хмельницький національний університет, м. Хмельницький
Оцінка ризиків кібербезпеки об'єктів критичної інформаційної інфраструктури згідно зі стандартами IEC 62443

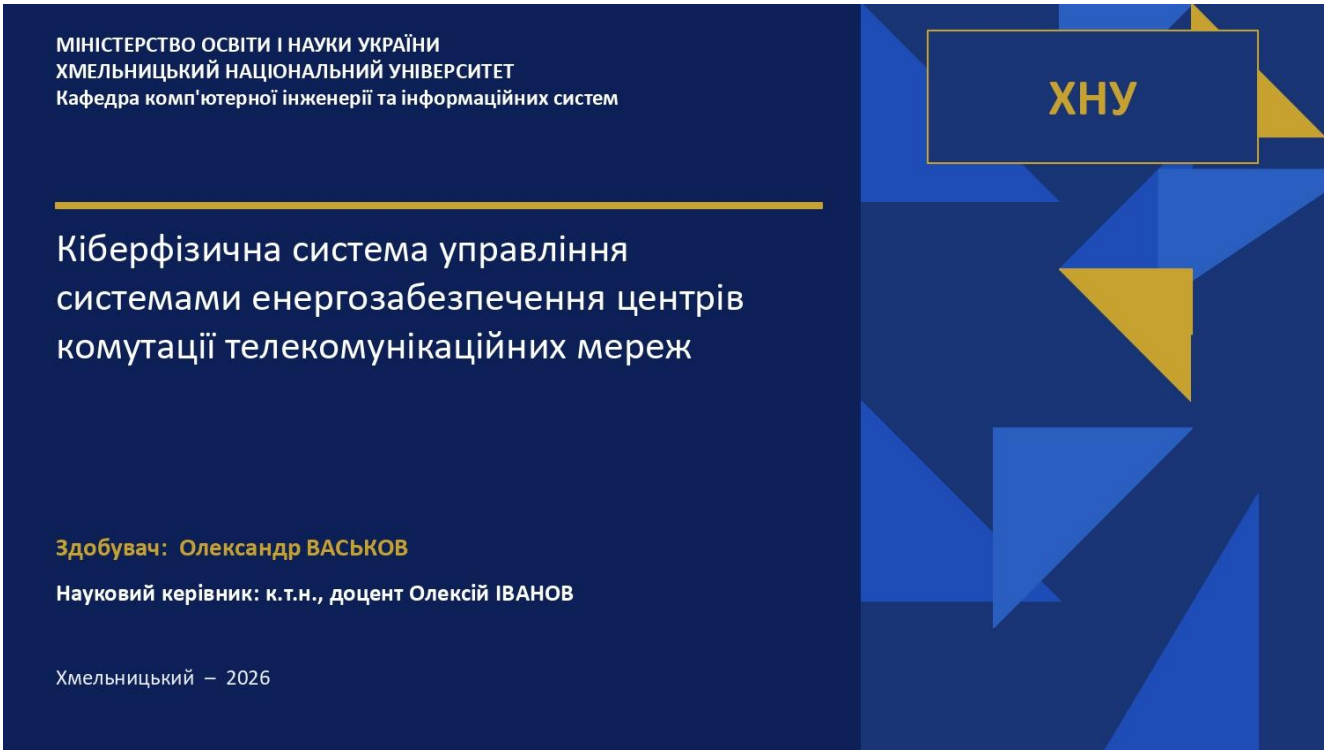
Бойченко Р.Т.
Національний технічний університет України «КПІ ім. Ігоря Сікорського»
Предиктивна аналітика технічного стану акумуляторних систем резервного електроживлення

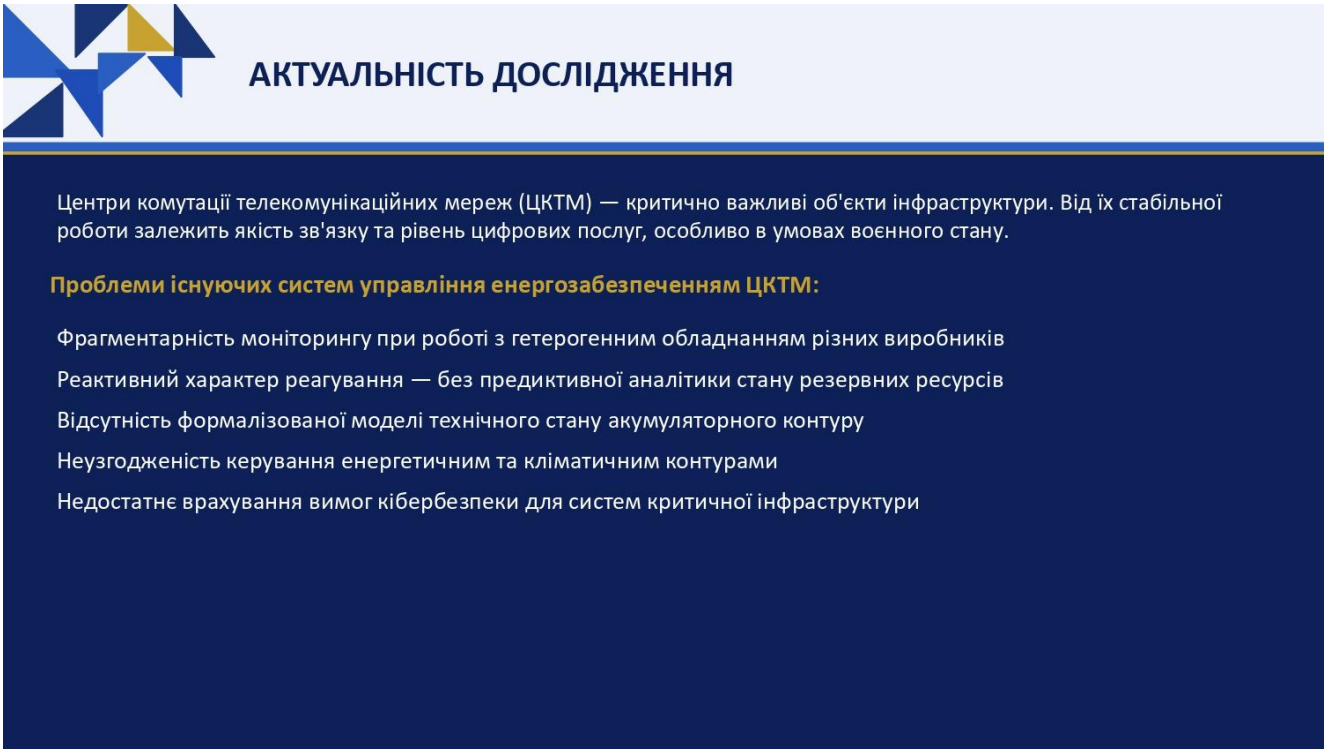
Семенченко В.В.
ННІУЕП ТНУ імені В.І. Вернадського, м. Київ
Цифрові двійники у системах управління енергоефективністю центрів обробки даних

ДОДАТОК Д

(обов’язковий)

Презентація





МЕТА, ОБ'ЄКТ ТА ПРЕДМЕТ ДОСЛІДЖЕННЯ

МЕТА

Підвищення надійності, спостережуваності та енергоефективності систем енергозабезпечення ЦКТМ шляхом створення кіберфізичної системи управління, яка інтегрує телеметрію, предиктивну аналітику стану обладнання та сценарне реагування.

ОБ'ЄКТ

Процес управління системами енергозабезпечення центрів комутації телекомунікаційних мереж в умовах впровадження кіберфізичних технологій.

ПРЕДМЕТ

Моделі, методи та програмні засоби побудови кіберфізичної системи управління, що забезпечують підвищення надійності та ефективності функціонування систем електроживлення телекомунікаційного обладнання.

ЗАДАЧІ ДОСЛІДЖЕННЯ

Поставлена мета досягається вирішенням таких основних задач:

1. Провести аналіз відомих моделей, методів та програмно-технічних засобів управління енергозабезпеченням ЦКТМ, виявити обмеження існуючих рішень
2. Розробити концепцію та структурно-функціональну модель кіберфізичної системи управління енергозабезпеченням
3. Розробити інформаційну модель об'єкта та модель технічного стану елементів енергетичної інфраструктури
4. Розробити метод адаптивного управління енергозабезпеченням з підтримкою предиктивної оцінки стану та сценарного реагування
5. Розробити алгоритми та архітектуру програмного забезпечення кіберфізичної системи
6. Реалізувати програмні засоби та провести експериментальні дослідження їхньої ефективності

НАУКОВА НОВИЗНА ТА ПРАКТИЧНА ЦІННІСТЬ

НАУКОВА НОВИЗНА

1. **Удосконалено** метод управління системами енергозабезпечення ЦКТМ за рахунок інтеграції предиктивної оцінки технічного стану обладнання, моделі ієрархічного подієво-станового керування та сценарного реагування. Забезпечено перехід від реактивного до проактивного режиму експлуатації.
2. **Набули подальшого розвитку** програмні засоби КФС-управління за рахунок уніфікованого шару абстракції даних поверх гетерогенних протоколів: Modbus, MQTT, SNMP, OPC UA, REST.

ПРАКТИЧНА ЦІННІСТЬ

×17	швидше виявлення деградації (32 год → 1.8 год)
×3	швидше розв'язання інцидентів
+37%	автономія критичного ядра мережі
−73%	зниження CAPEX порівняно з аналогами

АНАЛІЗ ВІДОМИХ МОДЕЛЕЙ ТА МЕТОДІВ

МОДЕЛІ КФС

Тришарові (фізичний – мережа – застосунки): прості, не враховують реальний час

5C-архітектура: детально описують перетворення телеметрії в рішення

Цифровий двійник ISO 23247: безперервна синхронізація з фізичним об'єктом

IIRA: 4-перспективна модель IIoT (бізнес, функціональна, реалізаційна, використання)

Обмеження для ЦКТМ:
Фрагментарність моніторингу; відсутність формальної моделі стану АКБ

7 ГРУП МЕТОДІВ

Реактивні порогові — проста логіка, лише реакція на факт

Скінченні автомати / сценарні дерева — SCADA, DCIM

Предиктивне обслуговування — аналіз деградації АКБ

Координоване управління (енергетика + клімат)

Гібридні джерела енергії (EMS-клас)

ML-виявлення аномалій та класифікація інцидентів

Ієрархічні edge-методи для розподіленої інфраструктури

КОНЦЕПЦІЯ КІБЕРФІЗИЧНОЇ СИСТЕМИ УПРАВЛІННЯ

ЦЕНТРАЛІЗОВАНИЙ РІВЕНЬ

Глибока аналітика, координація між майданчиками, навчання моделі

ОБ'ЄКТНИЙ РІВЕНЬ

Нормалізація телеметрії, обчислення моделі стану, YAML-сценарії реагування

ЛОКАЛЬНИЙ РІВЕНЬ

Збір телеметрії (5 протоколів), аварійні блокування ≤ 100 мс

8 ключових положень концепції:

6 станів: Normal → Degraded → Pre-emergency → Emergency → Recovery → Maintenance
Предиктивна оцінка стану АКБ, випрямного та генераторного контурів
Координація енергетичного та кліматичного контурів
5 адаптерів: Modbus, SNMP, OPC UA, MQTT, REST

СТРУКТУРНО-ФУНКЦІОНАЛЬНА ТА ІНФОРМАЦІЙНА МОДЕЛЬ КФС

СФМ: РІВНІ СИСТЕМИ

Локальний рівень:
Адаптери Modbus/SNMP/OPC UA/MQTT/REST
Аварійні блокування, гарантований час реакції ≤ 100 мс
Автономне функціонування при втраті зв'язку

Об'єктний рівень:
Нормалізація → уніфікований формат TelemetryPoint
Обчислення моделі стану та YAML-сценарії

Централізований рівень:
Глибока аналітика, TimescaleDB, контур навчання
API Gateway → React HMI з інтерактивним графом

ІНФОРМАЦІЙНА МОДЕЛЬ

$M = \langle E, T, A, R, P, S, H \rangle$

E — сутності (ДБЖ, ДГУ, АКБ, шини, датчики)
T — типи сутностей; A — атрибути; R — відношення

4 типи відношень R:
feeds (живить), monitors (моніторить)
controls (керує), thermally_coupled_with

Функція пріоритетів P:
Critical: АТС, захисний периметр
High: транспорт, синхронізація
Medium/Low: підтримувальні системи

МОДЕЛЬ ТЕХНІЧНОГО СТАНУ ТА МЕТОД АДАПТИВНОГО УПРАВЛІННЯ

Інтегральний показник АКБ: $S_{battery} = w_1 \cdot SoH + w_2 \cdot TempScore + w_3 \cdot CycleScore + w_4 \cdot AgeScore$

LiFePO4: w_1=0.40, w_2=0.20, w_3=0.25, w_4=0.15 | VRLA: w_1=0.30, w_2=0.30, w_3=0.20, w_4=0.20 | Кореляція SoH: r = 0.94

Метод адаптивного управління: 6 взаємопов'язаних етапів

1	2	3	4	5	6
Збір телеметрії	**Модель стану**	**Класифікація**	**Сценарій**	**Виконання**	**Навчання**
Modbus, SNMP, OPC UA, MQTT, REST → TelemetryPoint	SoH, SoC, TempScore, CycleScore, AgeScore, автономія	6 станів: Normal → Degraded → Emergency → Recovery...	YAML-декларації, пріоритизація навантажень	Керуючі впливи + когнітивна підтримка	Накопичення історії, оптимізація параметрів

АРХІТЕКТУРА ТА ПРОГРАМНА РЕАЛІЗАЦІЯ

8 МІКРОСЕРВІСІВ (event-driven + модульна архітектура)

- **Telemetry Collector** — адаптери Modbus / SNMP / OPC UA / MQTT / REST
- **State Engine** — обчислення моделі стану та класифікація
- **Scenario Executor** — виконання YAML-сценаріїв реагування
- **Analytics Service** — предиктивна аналітика, TimescaleDB
- **Alert Manager** — управління сповіщеннями та ескалація
- **API Gateway** — єдина точка доступу, авторизація JWT
- **HMI Frontend** — React + TypeScript, граф інфраструктури
- **Auth Service** — RBAC, CSRF-токени, TLS-автентифікація

ТЕХНОЛОГІЧНИЙ СТЕК

Backend:	Python · FastAPI · asyncio
БД:	TimescaleDB (часові ряди)
Брокер:	MQTT / Mosquitto
Frontend:	React · TypeScript · D3.js
DevOps:	Docker · Kubernetes
Безпека:	JWT · TLS · CSRF-токени

~24 500 рядків коду (Python + TypeScript)
Покриття тестами: 78.4% · ISA/IEC 62443 SL-2: 47/50

РЕЗУЛЬТАТИ ЕКСПЕРИМЕНТАЛЬНИХ ДОСЛІДЖЕНЬ

Тестовий стенд: Eaton 9PX (ДБЖ) · LiFePO4 280 Ah · PLC Wago · Moxa MB3170 · Edge-сервер Intel NUC 16 ГБ

Продуктивність	Час реакції	Точність прогнозу	Кореляція SoH
1.18 с	**46 мс**	**4.6%**	**0.94**
цикл збору (ціль: 2 с)	середній (47 сценаріїв) макс. 94 мс	середня похибка автономії	обчислений vs фактичний

П'ять серій дослідів:

Експеримент	Параметр	Результат
Продуктивність	Загальний цикл	1.18 с < 2 с ✓
Час реакції	Критичні події	18–94 мс < 100 мс ✓
Точність прогнозу	Похибка автономії	2.1–7.6%, середня 4.6% ✓
Автономія	Втрата зв'язку 24 год	14 400 повідомлень синхронізовано за 187 с ✓
Кіберстійкість	Penetration testing	Жодної вразливості не виявлено ✓

ПОРІВНЯЛЬНА ОЦІНКА ЕФЕКТИВНОСТІ

Показник	SCADA Ignition	EcoStruxure IT	Запропонована КФС
Предиктивна аналітика АКБ	Ні	Базова	✓ (4 фактори)
Гетерогенні протоколи	Частково	Обмежено	✓ (5 протоколів)
Сценарне реагування (YAML)	Ні	Ні	✓
Координація з кліматом	Ручна	✓	✓ (–11.4% енергії)
Автономія ядра мережі	Базова	Базова	✓ (+37%)
CAPEX	~$39 000	~$61 000	~$16 500 (–58–73%)
OPEX / рік	~$7 000	~$10 000	~$5 000 (–30–50%)
Виявлення деградації	32 год	~20 год	1.8 год (×17 швидше)

ВИСНОВКИ

У кваліфікаційній роботі розв'язано науково-прикладну задачу розроблення КФС управління енергозабезпеченням ЦКТМ. Основні результати:

СФМ КФС	Розроблено ієрархічну СФМ з 3 рівнів та інформаційну модель орієнтованого графу M=⟨E,T,A,R,P,S,H⟩
Метод управ.	Розроблено метод адаптивного управління з 6 етапами та предиктивною оцінкою стану АКБ
Реалізація	8 мікросервісів · ~24 500 рядків коду · покриття тестами 78.4% · ISA/IEC 62443 SL-2: 47/50
Ефективність	Виявлення деградації у ×17 разів швидше · час реакції ≤ 46 мс · похибка прогнозу 4.6%
Економія	CAPEX –58–73% · OPEX –30–50% · автономія ядра +37% · енергія кондиціювання –11.4%
Апробація	Наукова стаття у «Вісник ХНУ. Технічні науки» · тези на VII Міжнар. конф. ТНУ ім. Вернадського

ПУБЛІКАЦІЯ

Тези доповіді на конференції

Васьков О.В. Метод адаптивного управління енергозабезпеченням з предиктивною оцінкою технічного стану.

VII Міжнародна науково-практична конференція Таврійського національного університету імені В.І. Вернадського. 2026.

Дякую за увагу!

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

Здобувач: Олександр ВАСЬКОВ

Тема: Кіберфізична система управління системами енергозабезпечення центрів комутації телекомунікаційних мереж

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи магістра:

Кількість листів креслень – ; кількість сторінок записки 86

1. Короткий зміст роботи та прийнятих рішень У роботі розроблено кіберфізичну систему управління системами енергозабезпечення центрів комутації телекомунікаційних мереж.

2. Висновок про відповідність роботи дипломному завданню Кваліфікаційна робота магістра відповідає виданому завданню

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі проведено аналіз моделей, методів та засобів управління енергозабезпеченням телекомунікаційних об'єктів. У другому розділі розроблено концепцію, структурно-функціональну модель та метод адаптивного управління з предиктивною оцінкою стану. У третьому розділі розроблено алгоритм роботе системи, вимоги до ПЗ та архітектурне проєктування. У четвертому розділі виконано програмну реалізацію та експериментальні дослідження на тестовому стенді.

4. Позитивні сторони роботи: Запропонована кіберфізична система забезпечує перехід від реактивного до проактивного режиму експлуатації енергетичної інфраструктури та інтеграцію гетерогенного обладнання в єдиний контур керування.

5. Негативні сторони роботи: У роботі недостатньо розкрито економічне обґрунтування впровадження системи, а експериментальні дослідження виконано лише на тестовому стенді.

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка оформлена відповідно до встановлених вимог, структура чітка, текст викладено логічно та зрозуміло. Графічний матеріал (рисунки, схеми, таблиці) у переважній більшості відповідає змісту викладеного матеріалу

7. Відгук про роботу в цілому: Робота виконана на майже високому рівні, проте окремі розділи потребували б більш глибокого опрацювання.

8. Інші зауваження: Зауваження принципового характеру, які би вплинули на загальну оцінку роботи, відсутні.

9. Оцінка кваліфікаційної роботи магістра:

Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи магістра вважаю, що робота заслуговує оцінки «добре» 78.00 (С)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) Барнюк Олександр Володимирович, зав. кафедри Комп'ютерних наук, д.т.н. професор, Хмельницький національний університет

"1 травня" 2026р.

Зав. кафедри КІІС
д-р. філософії Ользі ПАВЛОВІЙ

Олександр ВАСЬКОВ

ПІБ здобувача вищої освіти

ФІТ, 2 курсу, групи КІ2м-24-1

ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів академічної відповідальності, ознайомлений (а). Про використання спеціалізованих програмних засобів (СПЗ) StrikePlagiarism та Anti-Plagiarism для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщений (а). Надаю університету право на передачу моєї роботи для обробки та збереження в базах даних СПЗ і використання роботи для виявлення академічного плагіату в інших роботах, які перевіряються СПЗ.

Також надаю свою згоду на обробку й збереження університетом моєї роботи в Інституційному репозитарії Хмельницького національного університету.

Робота надається для перевірки в електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

1 травня 2026 року

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ
ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Назва кваліфікаційної роботи Кіберфізична система управління системами енергозабезпечення центрів комутації телекомунікаційних мереж
Автор Олександр Васьков
Освітня програма Комп'ютерна інженерія та програмування
Рівень вищої освіти другий (магістерський)
Спеціальність 123 Комп'ютерна інженерія
Науковий керівник: к.т.н., доцент Олексій ІВАНОВ

На основі аналізу кваліфікаційної роботи на дотримання вимог академічної доброчесності (у т.ч. відсутності ознак академічного плагіату) з урахуванням результатів перевірки роботи спеціалізованим програмним засобом(ами) комісія зробила такий висновок:

№	Висновок	Позначка про відповідність
1	Ознаки академічного плагіату	
1.1	Запозичення, виявлені в роботі, є законними і не є академічним плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних, якщо потрібно). Робота приймається до захисту.	відповідає
1.2	Виявлені запозичення не є академічним плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована.	
1.3	Виявлені запозичення не є академічним плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота може бути допущена до захисту після того як буде відкоригована та доопрацьована і успішно пройде повторну перевірку на академічний плагіат.	
1.4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття текстових запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
2	Інші види порушень академічної доброчесності	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) усі запозичення фрагментарні, або мають належним чином оформленні посилання;

2) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з джерелами на один фрагмент речення;

3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

4) значна частина знайденого плагіату відноситься до списку використаних джерел

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості StrikePlagiarism, складає 4,47% і адресується до 37 першоджерела; та системою Anti-Plagiarism складає 0%, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

25.04.2026

Завідувач кафедри _____ Підпис — Ольга ПАВЛОВА Ім'я, ПРІЗВИЩЕ

Гарант освітньої програми _____ Підпис — Олег САВЕНКО Ім'я, ПРІЗВИЩЕ

Керівник кваліфікаційної роботи _____ Підпис — Олексій ІВАНОВ Ім'я, ПРІЗВИЩЕ

Протокол аналізу звіту подібності експертом

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системо виявлення і запобігання плагіату щодо роботи:

Автор: Олександр ВАСЬКОВ

Співавтор:

Назва: 8Кваліфікаційна_робота_магістра_Васьков_О_В_Антиплагіат

Експерт: Олексій ІВАНОВ

Підрозділ: Кафедра комп'ютерної інженерії та інформаційних систем

Коефіцієнт подібності 1:4.47%

Коефіцієнт подібності 2:1.06%

Мікропробіли: 0

Заміна букв: 2

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2026-05-19 22:34:56.0

Після аналізу Звіту подібності констатую наступне:

☒ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

2026-05-20 Доцент Андрій Нічепорук

Дата експерт

Anti-Plagiarism (http://ap.km.ua) v-15.701

Максимальне співпадіння з одним документом 0.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 13%**

	Документ		Сумарний збіг по Базі Даних	
ID: 271740 Назва: МКР Кіберфізична система управління системами енергозабезпечення центрів комутації телекомунікаційних мереж Додано в БД: 2026-05-19 Автора: Олександр ВАСЬКОВ Керівники: Олексій ІВАНОВ Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	142147	1206	2845 (2%)	45 (4%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми