**УДК 004.75** https://doi.org/10.31713/vt1202623

**Дрогобицький М.В.** [1; ORCID ID: 0009-0009-6865-6034],
аспірант,
**Луцик Н.С.** [1; 0000-0002-0361-6471],
Ph.D., доцент
**Мудрий І. В.** [1; 0009-0003-1409-2612],
аспірант
**Лотоцький В. П.** [1; 0009-0008-0531-5876],
аспірант

[1]Тернопільський національний технічний університет
імені Івана Пулюя, м. Тернопіль

# АНАЛІЗ АРХІТЕКТУР КОМП'ЮТЕРНИХ СИСТЕМ ДЛЯ МОНІТОРИНГУ ТА КЕРУВАННЯ МІКРОМЕРЕЖАМИ

**У статті розглянуто архітектури комп'ютерних систем, призначених для моніторингу та керування мікромережами. Актуальність дослідження зумовлена зростанням масштабів впровадження мікромереж, що супроводжується трансформацією сучасних електроенергетичних систем у складні кіберфізичні інфраструктури, ефективність і надійність функціонування яких значною мірою визначаються архітектурою комп'ютерних систем та мереж зв'язку.**

**У роботі проаналізовано багаторівневу організацію систем, що охоплює польові пристрої, крайові вузли, підсистеми обробки й управління даними та операторські інтерфейси. Розглянуто комунікаційну інфраструктуру, підходи до збору та обробки даних, програмні платформи підтримки функцій енергоменеджменту, крайові обчислення та механізми забезпечення кібербезпеки. Узагальнено особливості централізованих, децентралізованих і гібридних архітектур, а також визначено роль комунікаційно-орієнтованого проєктування у забезпеченні стійкості та масштабованості систем.**

**Запропоновано узагальнену класифікаційну характеристику архітектур комп'ютерних систем мікромереж, визначено типові архітектурні підходи та окреслено основні проєктні особливості й обмеження. У результаті огляду виявлено ключові наукові**

ISSN 2306-5478

**прогалини, пов'язані з відсутністю уніфікованих референсних архітектур, недостатньою розробленістю edge-орієнтованих рішень, проблемами інтероперабельності та фрагментарною інтеграцією засобів кібербезпеки. Запропоновано узагальнену багаторівневу архітектуру комп'ютерної системи моніторингу та керування мікромережею. Отримані результати можуть бути використані як основа для подальшого аналізу та проєктування стійких, масштабованих і інтероперабельних систем моніторингу та керування мікромережами.**

**Ключові слова:** мікромережі, архітектура комп'ютерних систем, системи моніторингу та керування, комунікаційна інфраструктура, крайові обчислення, кібербезпека

**Актуальність теми.** Стрімке зростання частки розподілених джерел енергії (Distributed Energy Resources, DER) суттєво прискорило впровадження мікромереж як одного з ключових елементів сучасних електроенергетичних систем. На відміну від традиційних централізованих енергомереж, мікромережі функціонують як локально керовані енергетичні системи, що базуються на тісній координації фізичних енергетичних об'єктів та цифрової інформаційної інфраструктури. У результаті мікромережі набувають ознак кіберфізичних комп'ютерних систем, у яких процеси моніторингу, обробки даних і програмно-орієнтованого керування є визначальними для забезпечення надійності та стійкості функціонування.

Більшість наукових досліджень [3,24] у сфері мікромереж зосереджена на питаннях силової електроніки, стратегій керування та алгоритмів оптимізації енергетичних потоків. Водночас інформаційно-комунікаційні технології (ІКТ) у таких роботах часто розглядаються як допоміжний компонент, а основний акцент робиться на теоретичних аспектах керування або електротехнічних характеристиках системи. На практиці ж ефективність і стабільність роботи мікромережі значною мірою визначаються архітектурою комп'ютерної системи, зокрема організацією мереж зв'язку, розподілених обчислювальних платформ і програмних систем керування.

Подальший розвиток концепцій Інтернету речей (Internet of Things, IoT) суттєво ускладнив системи моніторингу та керування мікромережами. Дані з польових пристроїв повинні передаватися, оброблятися та інтегруватися в процеси енергоменеджменту з

дотриманням вимог щодо мінімальної затримки та високої надійності. Крім того, мікромережі мають зберігати працездатність за умов збоїв зв'язку або часткових відмов інфраструктури. Додаткові обмеження формуються кіберзагрозами, які висувають підвищені вимоги до архітектури системи порівняно з традиційними централізованими системами керування. Тому дослідження архітектури комп'ютерних систем для моніторингу та керування мікромережами є актуальним завданням. Метою статті є цілісний аналіз архітектур комп'ютерних систем моніторингу та керування мікромережами та уніфікована класифікація комунікаційної інфраструктури, підсистем управління даними, крайових обчислень і програмних платформ із єдиної архітектурної позиції.

**Викладення основного матеріалу.** Системи моніторингу та керування мікромережами поєднують різноманітні сенсорні пристрої, мережі зв'язку, розподілені обчислювальні платформи та програмні застосунки керування. Опис архітектур у науковій літературі часто має фрагментарний і несистемний характер. Сучасні роботи підкреслюють різноманітність підходів до архітектурного проєктування мікромереж та інтелектуальних енергосистем, а також відсутність єдиної класифікаційної рамки [1-3]. Комп'ютерні системи мікромереж зазвичай мають багаторівневу архітектуру: польовий, крайовий, рівень управління даними та операторський.

Кожен рівень виконує свої функції та має свої вимоги до ресурсів. Багаторівневі кіберфізичні моделі інтелектуальних енергосистем широко застосовуються для розмежування функцій збору даних, керування, комунікації та диспетчерського контролю [1-2]. Архітектури можуть бути централізованими, децентралізованими або гібридними. Централізовані рішення є простішими й цілісними, децентралізовані — стійкі та масштабовані, але складні у координації. Гібридні архітектури поєднують ці підходи і є найпоширенішими. Дослідження [1-2, 4] показують перехід від централізованих до гібридних систем. Вибір архітектури впливає на затримки, надійність та гнучкість системи. В роботах [5-7] показано, що стійкість залежить від топології та протоколів.

З точки зору організації обчислень, архітектури можуть бути хмарно-орієнтованими, крайово-орієнтованими або повністю розподіленими. Кожна з цих моделей характеризується певними компромісами між масштабованістю, затримками, стійкістю та складністю експлуатації. Сучасні дослідження у сфері edge- та fog-

 ISSN 2306-5478

обчислень в енергосистемах деталізують цю класифікацію, зокрема шляхом розмежування крайових вузлів, орієнтованих на агрегацію даних, та автономних розподілених контролерів [8–10].

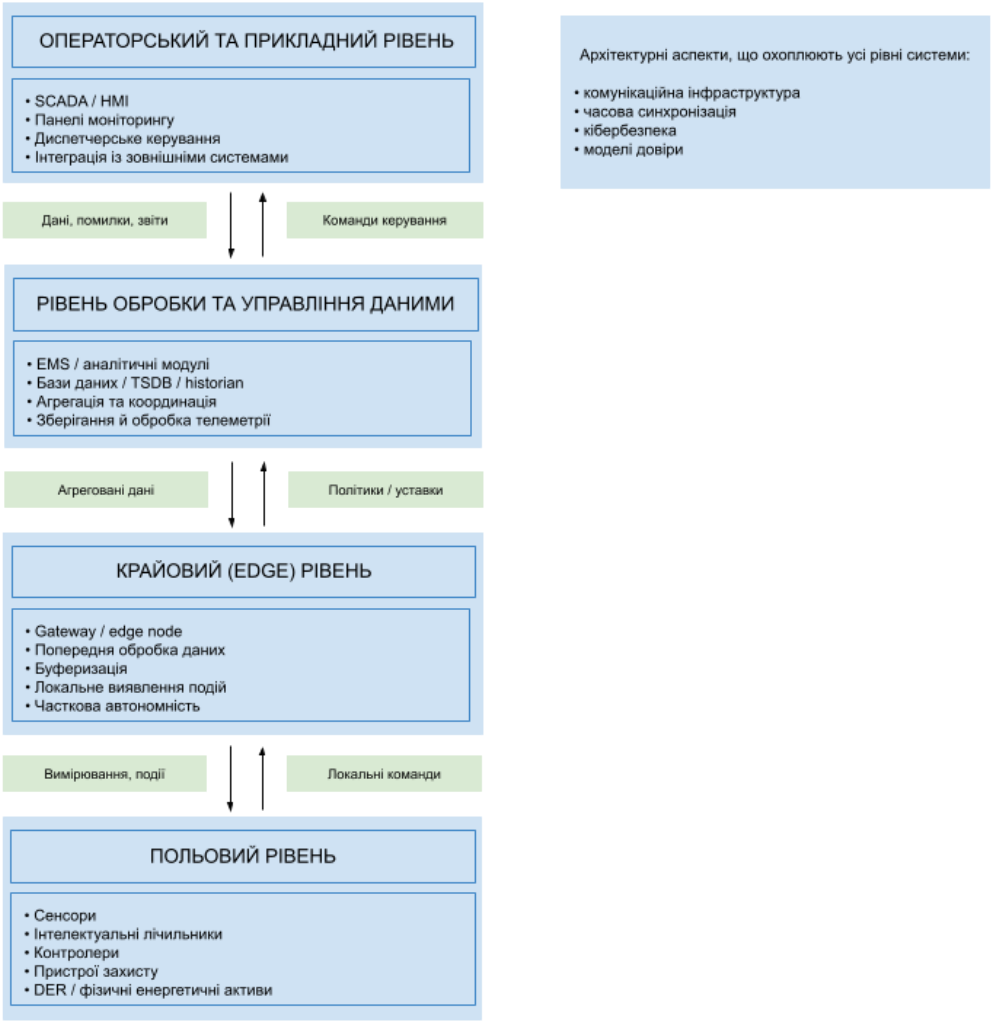


Рис. 1. Узагальнена багаторівнева архітектура комп'ютерної системи моніторингу та керування мікромережами

Підходи до забезпечення безпеки коливаються від централізованого управління системою доступу до розподілених і моделей нульової довіри (Zero Trust). Вибір архітектури безпеки впливає на продуктивність, складність і стійкість системи і має узгоджуватися з багаторівневою структурою.

Табл. 1. Узагальнена характеристика архітектур комп'ютерних систем для моніторингу та керування мікромережами

| Класифікаційний вимір | Категорія | Проєктні особливості та обмеження |
|---|---|---|
| Функціональна рівнева організація | Польовий рівень | Високі вимоги до детермінованості, обмежені ресурси |
| | Крайовий рівень | Локальна обробка й менші затримки, складніше розгортання |
| | Рівень обробки та управління даними | Масштабована координація й аналітика, залежність від зв'язку |
| | Операторський та прикладний рівень | Зручне керування й візуалізація, абстрагування від фізичного рівня |
| Архітектурна парадигма | Централізована | Просте керування, залежність від центрального вузла |
| | Децентралізована | Вища стійкість і автономність, складніша координація |
| | Гібридна | Поєднання централізованого нагляду й локальної автономності |
| Комунікаційна інфраструктура | Провідні промислові мережі | Висока надійність і передбачуваність, вища вартість розгортання |
| | Бездротові мережі | Гнучке розгортання, варіабельність затримок і надійності |
| | Передача даних по силових лініях (PLC) | Використання наявної інфраструктури, чутливість до завад |
| Протокольний стек | Промислові протоколи | Детермінований обмін, обмежена гнучкість інтеграції |
| | Сервіс-орієнтовані / протоколи обміну повідомленнями | Масштабований обмін, менш жорсткі часові гарантії |
| Обчислювальна модель | Хмарно-орієнтована | Висока масштабованість, залежність від якості зв'язку |
| | Крайово-орієнтована | Низька затримка й локальна автономність, обмежені ресурси |
| | Розподілені обчислення | Гнучкий розподіл функцій, складніша оркестрація |
| Модель безпеки та довіри | Централізоване управління безпекою | Спрощене адміністрування, концентрація ризиків |
| | Розподілені / Zero Trust моделі | Посилений контроль доступу, додаткові накладні витрати |

ISSN 2306-5478

Дослідження [11–13] підкреслюють важливість узгодженої інтеграції моделей довіри на всіх рівнях — від польового до крайового та диспетчерського. Запропонована таксономія (табл. 1.) демонструє, що системи моніторингу та керування мікромережами не можуть бути коректно описані в межах одного архітектурного виміру. Натомість вони характеризуються структурованими поєднаннями багаторівневої організації, архітектурних парадигм, комунікаційної інфраструктури, моделей обчислень і механізмів безпеки. Така багатовимірна класифікація створює системну основу для порівняння існуючих рішень і дозволяє виявляти ключові архітектурні компроміси.

***Комунікаційна інфраструктура комп'ютерних систем мікромереж.***

Комунікаційна інфраструктура є ключовою складовою архітектури комп'ютерних систем моніторингу та керування мікромережами. На відміну від традиційних корпоративних IT-систем, комунікаційні мережі мікромереж функціонують в умовах жорстких обмежень щодо затримок, надійності, детермінованості та синхронізації, оскільки характеристики зв'язку безпосередньо впливають на стабільність і безпечність фізичних енергетичних процесів. Відповідно, проєктування комунікаційної підсистеми має розглядатися як базовий елемент архітектури, а не як допоміжний компонент. Сучасні дослідження [6, 7, 14] приділяють значну увагу комунікаційно-орієнтованому архітектурному проєктуванню в інтелектуальних енергосистемах і мікромережах, підкреслюючи тісний зв'язок між характеристиками мережі та стійкістю процесів керування.

Вимоги до комунікацій у мікромережах істотно відрізняються від вимог традиційних мереж передачі даних, оскільки функції моніторингу та керування залежать від рівня системи та операційного контексту. До ключових вимог належать гарантована низька затримка, висока доступність, детермінована доставка критичних даних, точна часова синхронізація та захищене розмежування операційного й інформаційного трафіку. Дослідження [6, 7] підкреслюють, що саме затримка, детермінованість і синхронізація є критичними для надійного диспетчерського керування, тоді як різнорідність трафіку потребує використання різних класів комунікації та стратегій QoS [5]. Провідні технології зв'язку залишаються основним вибором для критичних задач

завдяки високій надійності та передбачуваності характеристик. Ethernet широко використовується на рівні підстанцій, керування та агрегації даних, доповнюючись механізмами резервування та пріоритезації трафіку [5-6]. Водночас провідні рішення є менш гнучкими та дорожчими у розгортанні. Бездротові технології, навпаки, забезпечують гнучкість інтеграції енергетичних активів, проте характеризуються варіабельністю затримок, пропускної здатності та надійності, що зумовлює потребу в механізмах крайової обробки, буферизації та адаптивної передачі [7, 14].

Технології PLC дають змогу використовувати наявну електричну інфраструктуру для обміну даними, що робить їх привабливими для модернізації існуючих систем. Однак їх ефективність залежить від електричних завад, топології мережі та режимів навантаження, тому PLC зазвичай застосовують для некритичних задач моніторингу або в поєднанні з іншими комунікаційними технологіями.

Ієрархічні архітектури природно відповідають багаторівневим структурам керування мікромережами. Польові пристрої взаємодіють із локальними шлюзами або крайовими вузлами, які здійснюють агрегацію даних і передають їх до центральних платформ керування. Такий підхід спрощує організацію системи та реалізацію політик управління, однак за недостатньо продуманого проєктування може призводити до виникнення вузьких місць і єдиних точок відмови. Ієрархічні моделі комунікації добре узгоджуються з традиційними архітектурами диспетчерського керування та широко застосовуються у системах енергоменеджменту мікромереж (EMS) [1-2].

Архітектури типу peer-to-peer і mesh передбачають розподіл комунікаційних функцій між багатьма вузлами, що підвищує відмовостійкість і підтримує локальну координацію, але ускладнює маршрутизацію, синхронізацію та забезпечення безпеки [5, 15]. Гібридні архітектури поєднують ієрархічну агрегацію даних із peer-to-peer координацією, забезпечуючи локальну автономність при збереженні загальної видимості стану системи. Аналіз літератури показує, що саме гібридні підходи забезпечують найкращий баланс між масштабованістю, стійкістю та керованістю у практичних реалізаціях мікромереж [1-2]. На польовому рівні та рівні керування домінують промислові комунікаційні протоколи, орієнтовані на надійність, роботу в реальному часі та передбачуваність

ISSN 2306-5478

характеристик, хоча вони часто мають обмежену гнучкість інтеграції [6]. На вищих рівнях системи дедалі ширше застосовуються сервіс-орієнтовані моделі та моделі взаємодії на основі повідомлень. Механізми publish–subscribe та асинхронний обмін повідомленнями забезпечують масштабоване розповсюдження даних, слабке зв'язування компонентів і спрощують інтеграцію з аналітичними платформами, хмарними сервісами та зовнішніми системами [5]. Точна часова синхронізація є критичною для коректної кореляції вимірювань між розподіленими компонентами мікромережі, а узгодженість даних між вузлами залишається важливим архітектурним викликом [6]. Для його вирішення сучасні підходи дедалі частіше використовують буферизацію, версіонування та моделі узгодженості з відкладеною синхронізацією.

Відмови комунікацій є невід'ємною характеристикою розподілених середовищ мікромереж. Замість припущення про постійну доступність зв'язку, сучасні архітектури проєктуються з урахуванням можливості деградації функціональності, зберігаючи при цьому критично важливі функції моніторингу та керування під час порушень комунікації. Підходи до проєктування стійких комунікаційних систем підкреслюють важливість резервування, адаптивної маршрутизації та локальних fallback-механізмів [5, 14]. Комунікаційна інфраструктура безпосередньо визначає реалізованість, масштабованість і стійкість комп'ютерних систем мікромереж. Порівняльні дослідження архітектур інтелектуальних енергосистем, орієнтованих на комунікації, підтверджують, що врахування мережевих аспектів у проєктуванні суттєво підвищує стійкість і ефективність роботи систем [6, 7].

***Управління даними та програмні платформи для моніторингу та керування мікромережами.***

Підсистеми управління даними та програмні платформи формують базову інфраструктуру систем моніторингу та керування мікромережами, забезпечуючи перетворення первинних вимірювань у аналітичні висновки та узгоджені рішення на рівні всієї системи [16-17]. Системи моніторингу мікромереж генерують переважно часові ряди даних із сенсорів, лічильників, пристроїв захисту, контролерів і крайових вузлів. Такі потоки характеризуються високою часовою роздільною здатністю, різною частотою дискретизації та подієвими сплесками, що вимагає архітектур даних, здатних забезпечити безперервний прийом, низьку затримку, агрегацію та довготривале зберігання інформації [16]. Збір даних

зазвичай реалізується у вигляді конвеєрної архітектури, де дедалі частіше використовуються слабко зв'язані асинхронні механізми обміну повідомленнями замість жорстко зв'язаних схем опитування, що підвищує масштабованість і відмовостійкість системи. При цьому моніторинг у реальному часі потребує потокової обробки з мінімальною затримкою, тоді як історичний аналіз і оптимізаційні задачі можуть виконуватися в пакетному режимі [18].

Для зберігання телеметрії широко застосовуються бази даних часових рядів і системи типу data historian, для яких важливими є політики зберігання, downsampling, реплікація та резервне копіювання. Інтероперабельність залишається однією з ключових проблем управління даними в мікромережах [19], тому моделі даних мають забезпечувати узгоджену інтерпретацію інформації між різнорідними компонентами. Якщо ранні системи здебільшого будувалися як монолітні платформи, то сучасні рішення тяжіють до модульних, сервіс-орієнтованих і мікросервісних архітектур, які спрощують масштабування та інтеграцію із зовнішніми системами [10]. Для забезпечення цілісності даних застосовуються буферизація, валідація, узгодження та резервування, а ефективність таких платформ тісно пов'язана зі стратегіями крайових обчислень і комунікаційно-орієнтованим проєктуванням. У цілому архітектури, орієнтовані на слабко зв'язані конвеєри обробки даних, гнучкі моделі даних і модульну побудову програмного забезпечення, демонструють кращі показники масштабованості, інтероперабельності та стійкості.

***Крайові обчислення у комп'ютерних системах мікромереж.***

Крайові обчислення (edge computing) стали одним із ключових архітектурних підходів у системах мікромереж, оскільки дають змогу зменшити затримки, підвищити стійкість і знизити залежність від постійної доступності централізованих платформ. На відміну від традиційних централізованих архітектур, що потребують стабільного зв'язку між польовими пристроями та центральними контролерами, edge-підхід передбачає введення проміжних обчислювальних рівнів для локальної обробки даних і часткової автономності системи [20]. Це дозволяє зменшити обсяг переданих даних, підтримати роботу критичних функцій під час збоїв зв'язку та покращити масштабованість.

Крайові вузли забезпечують збір і попередню обробку даних, локальний моніторинг і виявлення подій, а в окремих випадках —

ISSN 2306-5478

обмежене локальне прийняття рішень. Така автономність дає змогу системі коректно деградувати в умовах порушення комунікації та зберігати виконання критично важливих функцій навіть у режимі ізоляції [9]. Крайові обчислення можуть реалізовуватися за різними моделями розгортання [8], а ефективність таких архітектур значною мірою залежить від чітко визначеної взаємодії між крайовими вузлами та централізованими платформами, зокрема ієрархічної координації, подієво-орієнтованої синхронізації та асинхронного обміну даними [10].

Водночас edge-архітектури супроводжуються низкою викликів. Збільшення кількості обчислювальних вузлів розширює поверхню атаки та підвищує вимоги до захисту, включаючи secure boot, автентифікацію пристроїв, шифрування комунікацій і контроль доступу. Крім того, розподілене розгортання ускладнює конфігураційне управління й оркестрацію, а обмежені ресурси крайових вузлів потребують ретельного розподілу функцій між локальними та централізованими компонентами. Тому збалансування цих проєктних обмежень залишається одним із ключових завдань розроблення edge-архітектур мікромереж, тоді як відсутність стандартизованих методологій їх проєктування і координації є важливим напрямом подальших досліджень [20-21].

**Аспекти кібербезпеки в комп'ютерних системах мікромереж.**

На відміну від традиційних IT-систем, кіберінциденти в мікромережах можуть безпосередньо впливати на стабільність системи, її безпечність і безперервність енергопостачання. Тому кібербезпека має розглядатися як невід'ємна складова архітектури, а не як додатковий компонент. Комп'ютерні системи мікромереж функціонують на перетині OT та IT, успадковуючи вразливості обох доменів, а інтеграція різнорідних пристроїв, мереж і програмних платформ формує широку поверхню атаки [13]. Загрози можуть виникати на різних рівнях системи — від польових пристроїв і каналів зв'язку до крайових вузлів і платформних сервісів. Саме тому багато архітектур покладають на крайовий рівень функції автентифікації, контролю доступу, перевірки протоколів і виявлення аномалій, що також сприяє локалізації інцидентів [20].

На вищих рівнях архітектури ключовими завданнями залишаються забезпечення конфіденційності й цілісності даних, автентифікація сервісів і узгодженість політик безпеки в розподілених програмних компонентах. Централізоване управління політиками спрощує адміністрування, але створює єдині точки

компрометації, тоді як розподілені моделі довіри та Zero Trust підходи підвищують безпеку ціною додаткових накладних витрат і складнішого управління ідентичностями [13, 23]. Механізми шифрування, автентифікації, журналювання та моніторингу мають бути узгоджено впроваджені на всіх рівнях системи без порушення вимог до затримок і надійності.

Стратегії реагування на інциденти в мікромережах повинні враховувати обмеження фізичних процесів і підтримувати контрольовану деградацію функціональності та безпечні fallback-режими. Аналіз літератури свідчить, що стійке й надійне функціонування мікромереж можливе лише за умови інтеграції безпеки на рівні архітектури, а не як набору ізольованих механізмів [12]. Водночас відсутність уніфікованих архітектурно-орієнтованих підходів до забезпечення безпеки залишається суттєвим обмеженням для створення надійних, масштабованих і довірених систем моніторингу та керування мікромережами.

***Порівняльний аналіз та відкриті наукові проблеми.***

Таблиця 2 узагальнює ключові архітектурні характеристики за такими вимірами, як комунікаційна інфраструктура, управління даними, крайові обчислення та кібербезпека, формуючи цілісне системне бачення [1-2, 8-9].

Порівняльний аналіз дозволяє виявити низку повторюваних архітектурних закономірностей. Централізовані архітектури домінують на ранніх етапах впровадження та в системах невеликого масштабу, забезпечуючи простоту реалізації, проте мають обмежену масштабованість і стійкість [12,23].

Гібридні архітектури виступають найбільш поширеним підходом у сучасних системах, поєднуючи централізовану координацію з розподіленими можливостями крайових обчислень.

Повністю децентралізовані архітектури зустрічаються рідше, однак демонструють високу стійкість і автономність за умов нестабільних комунікацій. Архітектури, чутливі до комунікаційних обмежень (communication-aware), стабільно перевершують рішення, що базуються на припущенні ідеальних мережевих умов. Системи, які використовують крайову буферизацію, локальну аналітику та подієво-орієнтовану синхронізацію, демонструють підвищену стійкість у середовищах із варіабельними затримками та нестабільною доступністю зв'язку. Підходи до управління даними еволюціонують від жорстко зв'язаних централізованих систем

 ISSN 2306-5478

історичних даних (data historian) до слабко зв'язаних, сервіс-орієнтованих конвеєрів обробки, що забезпечують масштабованість і інтероперабельність. Аналогічно, підходи до інтеграції безпеки трансформуються від периметрових моделей до багаторівневих і Zero Trust архітектур, узгоджених із багаторівневою структурою системи.

Табл. 2.

Порівняльний огляд репрезентативних архітектур комп'ютерних систем мікромереж

| **Архітектурна парадигма** | **Модель комунікації** | **Роль крайових обчислень** | **Підхід до управління даними** | **Інтеграція безпеки** |
|---|---|---|---|---|
| **Централізо-вана** | Ієрархічна, провідна | Мінімальна (ретрансляція даних) | Централізоване сховище історичних даних (data historian) | Периметрова модель безпеки |
| | Гібридна (провідна / бездротова) | Обмежена попередня обробка | Централізована база даних часових рядів (TSDB) | Централізована автентифікація |
| **Гібридна** | Ієрархічна | Локальна агрегація | Розподілена TSDB | Багаторівнева безпека |
| | | Делегування аналітики (offload) | Сервіс-орієнтована архітектура | Політико-орієнтована безпека |
| | Ізоляція відмов | Модульна платформа | Багаторівневий захист (defense-in-depth) | Ізоляція відмов |
| | Гібридна | Виявлення подій, буферизація | Декупльовані (слабо зв'язані) конвеєри обробки даних | Забезпечення безпеки на рівні edge |
| **Децентралі-зована** | Mesh / P2P | Локальна автономність | Розподілене зберігання даних | Розподілена модель довіри |
| | Гібридна | Підтримка керування | Подієво-орієнтована обробка | Zero Trust модель |

У таблиці 3 узагальнено ключові компроміси між edge-орієнтованими та хмарно-орієнтованими підходами, що широко застосовуються у комп'ютерних системах мікромереж. Проаналізовано системні наслідки вибору розміщення обчислень з

точки зору комунікаційної інфраструктури, управління даними та забезпечення безпеки.

*Таблиця 3.*

*Порівняння edge-орієнтованих та хмарно-орієнтованих архітектур у комп'ютерних системах мікромереж*

| Вимір | Edge-орієнтовані архітектури | Хмарно-орієнтовані архітектури |
|---|---|---|
| Затримка (latency) | Низька та обмежена завдяки локальній обробці | Вища та варіабельна, залежить від мережевих умов |
| Стійкість (resilience) | Висока, підтримує автономну роботу при втраті зв'язку | Обмежена, значною мірою залежить від постійного з'єднання |
| Навантаження на мережу | Зменшене завдяки локальній агрегації та фільтрації | Високе через централізований збір даних |
| Масштабованість | Горизонтальне масштабування за рахунок додавання edge-вузлів | Вертикальне масштабування через централізовані ресурси |
| Узгодженість даних | Моделі локальної або відкладеної узгодженості (eventual consistency) | Сильніша глобальна узгодженість |
| Поверхня атаки | Розширена (більше вузлів), але з можливістю локалізації інцидентів | Централізована поверхня атаки з потенційно більшим впливом |
| Операційна складність | Вища через розподілене розгортання та оркестрацію | Нижча завдяки централізованому управлінню |

Порівняльний аналіз дозволяє виявити низку системних прогалин у сучасних наукових досліджень:

ISSN 2306-5478

1) відсутність уніфікованих референсних архітектур, що інтегрують комунікації, обчислення, управління даними та безпеку в єдину узгоджену системну модель;
2) недостатній розвиток методологій проєктування, орієнтованих на комунікаційні обмеження, зокрема з урахуванням затримок і сценаріїв відмов;
3) обмежені архітектурні підходи до побудови edge-орієнтованих систем, включаючи критерії розподілу функцій і механізми координації;
4) фрагментованість моделей даних та проблеми інтероперабельності, що ускладнюють інтеграцію між гетерогенними платформами;
5) розгляд безпеки як додаткового компонента, а не як невід'ємної архітектурної характеристики системи.

Існуючі дослідження зосереджуються на окремих компонентах системи без належного врахування їх системної взаємодії.

***Висновки***

У роботі представлено комплексний огляд архітектур комп'ютерних систем для моніторингу та керування мікромережами з акцентом на програмні платформи, комунікаційну інфраструктуру, механізми управління даними, крайові обчислення та аспекти кібербезпеки. Розглянуто мікромережі як кіберфізичні комп'ютерні системи, ефективність і стійкість яких визначаються архітектурними рішеннями у сфері інформаційно-комунікаційних технологій. На основі систематизованого огляду запропоновано багатовимірну таксономію, що охоплює функціональну рівневу організацію, архітектурні парадигми, комунікаційні інфраструктури, моделі обчислень та підходи до забезпечення безпеки. Проведений аналіз показав, що сучасні системи мікромереж дедалі більше орієнтуються на гібридні та edge-архітектури для вирішення задач, пов'язаних із затримками, масштабованістю та стійкістю. Комунікаційно-орієнтоване проєктування, ефективні конвеєри управління даними та інтегровані механізми кібербезпеки визначаються як ключові архітектурні елементи, а не допоміжні компоненти. Водночас виявлено відсутність уніфікованих референсних архітектур, системних методологій проєктування edge-рішень, інтероперабельних моделей даних та архітектурно-орієнтованих підходів до безпеки. Узагальнюючи фрагментовані результати досліджень у цілісну системну перспективу, дана робота формує

структуровану основу для аналізу, проєктування та оцінювання систем моніторингу та керування мікромережами як для науковців, так і для практиків. Подальші дослідження мають бути спрямовані на розроблення комплексних архітектурних фреймворків, що інтегрують обчислювальні, комунікаційні, інформаційні та безпекові аспекти, забезпечуючи створення масштабованих, стійких та інтероперабельних комп'ютерних систем мікромереж, здатних відповідати зростаючим вимогам сучасних енергетичних систем.

1. Ahmed M., Meegahapola L., Vahidnia A., Datta M. Stability and control aspects of microgrid architectures: a comprehensive review // IEEE Access. 2020. Vol. 8. P. 144730–144766. DOI: 10.1109/ACCESS.2020.3014977. 2. Bordbari M. J., Nasiri F. Networked microgrids: a review on configuration, operation, and control strategies // Energies. 2024. Vol. 17, No. 3. P. 715. DOI: 10.3390/en17030715. 3. Punitha S., Subramaniam N. P., Vimal Raj P. A. D. A comprehensive review of microgrid challenges in architectures, mitigation approaches, and future directions // Journal of Electrical Systems and Information Technology. 2024. Vol. 11, No. 1. P. 60. DOI: 10.1186/s43067-024-00188-4. 4. Quizhpe K., Arévalo P., Ochoa-Correa D., Villa-Ávila E. Optimizing microgrid planning for renewable integration in power systems: a comprehensive review // Electronics. 2024. Vol. 13, No. 18. P. 3620. DOI: 10.3390/electronics13183620. 5. Starke M., Herron A., King D., Xue Y. Implementation of a publish–subscribe protocol in microgrid islanding and resynchronization with self-discovery // IEEE Transactions on Smart Grid. 2019. Vol. 10, No. 1. P. 361–370. DOI: 10.1109/TSG.2017.2739246. 6. Gungor V. C. et al. Smart grid technologies: communication technologies and standards // IEEE Transactions on Industrial Informatics. 2011. Vol. 7, No. 4. P. 529–539. DOI: 10.1109/TII.2011.2166794. 7. Tariq F., Dooley L. S. Smart grid communication and networking technologies: recent developments and future challenges // Smart Grids: Opportunities, Developments, and Trends. London: Springer, 2013. P. 199–213. DOI: 10.1007/978-1-4471-5210-1_9. 8. Habibi P. et al. Fog computing: a comprehensive architectural survey // IEEE Access. 2020. Vol. 8. P. 69105–69133. DOI: 10.1109/ACCESS.2020.2983253. 9. Yıldırım F. et al. Comprehensive review of edge computing for power systems: state of the art, architecture, and applications // Applied Sciences. 2025. Vol. 15, No. 8. P. 4592. DOI: 10.3390/app15084592. 10. Li J., Gu C., Xiang Y., Li F. Edge-cloud computing systems for smart grid: state-of-the-art, architecture, and applications // Journal of Modern Power Systems and Clean Energy. 2022. Vol. 10, No. 4. P. 805–817. DOI: 10.35833/MPCE.2021.000161. 11. Nejabatkhah F. et al. Cyber-security of smart microgrids: a survey // Energies. 2020. Vol. 14, No. 1. P. 27. DOI: 10.3390/en14010027. 12. Jamil N. et al. Cybersecurity of

ISSN 2306-5478

microgrid: state-of-the-art review and possible directions of future research // Applied Sciences. 2021. Vol. 11, No. 21. P. 9812. DOI: 10.3390/app11219812. 13. Achaal B. et al. Study of smart grid cyber-security: architectures, communication networks, cyber-attacks, countermeasures and challenges // Cybersecurity. 2024. Vol. 7, No. 1. P. 10. DOI: 10.1186/s42400-023-00200-w. 14. Ayele E. D., Gonzalez J. F., Teeuw W. B. Enhancing cybersecurity in distributed microgrids: a review of communication protocols and standards // Sensors. 2024. Vol. 24, No. 3. P. 854. DOI: 10.3390/s24030854. 15. Elsebaay A. et al. Multi-level internet of things communication strategy for microgrid smart network // Proceedings. 2019. Vol. 42, No. 1. P. 38. DOI: 10.3390/ecsa-6-06554. 16. Zia M. F., Elbouchikhi E., Benbouzid M. Microgrids energy management systems: a critical review on methods, solutions, and prospects // Applied Energy. 2018. Vol. 222. P. 1033–1055. DOI: 10.1016/j.apenergy.2018.04.103. 17. Chaudhary G. et al. Review of energy storage and energy management system control strategies in microgrid // Energies. 2021. Vol. 14, No. 16. P. 4929. DOI: 10.3390/en14164929. 18. Mwinuka L. et al. Big data energy systems: a survey of practices and associated challenges // Computer Science Review. 2026. Vol. 60. DOI: 10.48550/arXiv.2507.19154. 19. Liu D. et al. Edge computing application, architecture, and challenges in ubiquitous power internet of things // Frontiers in Energy Research. 2022. Vol. 10. P. 850252. DOI: 10.3389/fenrg.2022.850252. 20. Tank B., Gandhi V. A comparative study on cloud computing, edge computing and fog computing // Advances in Transdisciplinary Engineering. 2023. P. 665–670. DOI: 10.3233/ATDE221329. 21. Gautam V. L., Lanjewar U. A. Cloud, fog, and edge computing: a comparative analysis of architectures, applications, security challenges and performance // Proceedings of the International Conference on Advances in Management & Technology (ICAMT). 2025. P. 130–137. 22. Sanjalawe Y. et al. AI-powered smart grids in the 6G era: a comprehensive survey on security and intelligent energy systems // IEEE Open Journal of the Communications Society. 2025. Vol. 6. P. 7677–7719. DOI: 10.1109/OJCOMS.2025.3609144. 23. Ahmad Khan A. et al. A compendium of optimization objectives, constraints, tools and algorithms for energy management in microgrids // Renewable and Sustainable Energy Reviews. 2016. Vol. 58. P. 1664–1683. DOI: 10.1016/j.rser.2015.12.259. 24. Olatomiwa L. et al. Energy management strategies in hybrid renewable energy systems: a review // Renewable and Sustainable Energy Reviews. 2016. Vol. 62. P. 821–835. DOI: 10.1016/j.rser.2016.05.040. 25. Caiza G. et al. Fog computing at industrial level: architecture, latency, energy, and security: a review // Heliyon. 2020. Vol. 6, No. 4. P. e03706. DOI: 10.1016/j.heliyon.2020.e03706.

## REFERENCES

1. Akhmed M., Mihakhapola L., Vakhidniya A., Datta M. Aspekty stabil'nosti ta keruvannya arkhitekturamy mikromerezh: kompleksnyy ohlyad // IEEE Access. 2020. Tom 8. S. 144730–144766. DOI: 10.1109/ACCESS.2020.3014977. 2. Bordbari M. Dzh., Nasiri F. Merezhevi mikromerezhi: ohlyad stratehiy konfihuratsiyi, ekspluatatsiyi ta keruvannya // Energies. 2024. Tom 17, № 3. S. 715. DOI: 10.3390/en17030715. 3. Punita S., Subramaniam N. P., Vimal Radzh P. A. D. Kompleksnyy ohlyad problem mikromerezh v arkhitekturakh, pidkhodiv do pom'yakshennya naslidkiv ta maybutnikh napryamkiv // Zhurnal elektrychnykh system ta informatsiynykh tekhnolohiy. 2024. Tom... 11, № 1. S. 60. DOI: 10.1186/s43067-024-00188-4. 4. Kvizhpe K., Arevalo P., Ochoa-Korrea D., Vil'ya-Avila E. Optymizatsiya planuvannya mikromerezh dlya intehratsiyi vidnovlyuvanykh dzherel enerhiyi v enerhetychni systemy: kompleksnyy ohlyad // Elektronika. 2024. Tom 13, № 18. S. 3620. DOI: 10.3390/electronics13183620. 5. Starke M., Kherron A., Kinh D., Syue YU. Realizatsiya protokolu publikatsiyi-pidpysky v ostrivtsi mikromerezhi ta resynkhronizatsiyi iz samovyyavlennyam // IEEE Transactions on Smart Grid. 2019. Tom 10, № 1. S. 361–370. DOI: 10.1109/TSG.2017.2739246. 6. Hunhor V. K. ta in. Tekhnolohiyi intelektual'nykh merezh: komunikatsiyni tekhnolohiyi ta standarty // IEEE Transactions on Industrial Informatics. 2011. Tom 7, № 4. S. 529–539. DOI: 10.1109/TII.2011.2166794. 7. Tarik F., Duli L. S. Tekhnolohiyi komunikatsiyi ta merezh dlya intelektual'nykh merezh: ostanni rozrobky ta maybutni vyklyky // Smart Grids: Opportunities, Developments, and Trends. London: Springer, 2013. S. 199–213. DOI: 10.1007/978-1-4471-5210-1_9. 8. Khabibi P. ta in. Tumanni obchyslennya: kompleksnyy arkhitekturnyy ohlyad // IEEE Access. 2020. Tom... 8. S. 69105–69133. DOI: 10.1109/ACCESS.2020.2983253. 9. Yildyrym F. ta in. Kompleksnyy ohlyad peryferiynykh obchyslen' dlya enerhetychnykh system: suchasnyy stan, arkhitektura ta zastosuvannya // Prykladni nauky. 2025. Tom 15, № 8. S. 4592. DOI: 10.3390/app15084592. 10. Li Dzh., Hu K., Syan YU., Li F. Systemy peryferiynykh khmarnykh obchyslen' dlya intelektual'noyi merezhi: suchasnyy stan, arkhitektura ta zastosuvannya // Zhurnal suchasnykh enerhetychnykh system ta chystoyi enerhiyi. 2022. Tom 10, № 4. S. 805–817. DOI: 10.35833/MPCE.2021.000161. 11. Nedzhabatkha F. ta in. Kiberbezpeka intelektual'nykh mikromerezh: ohlyad // Enerhetyka. 2020. Tom 14, № 1. S. 27. DOI: 10.3390/en14010027. 12. Dzhamil' N. ta in. Kiberbezpeka mikromerezhi: ohlyad suchasnoho stanu ta mozhlyvi napryamky maybutnikh doslidzhen' // Prykladni nauky. 2021. Tom 11, № 21. S. 9812. DOI: 10.3390/app11219812. 13. Achaal B. ta in. Doslidzhennya kiberbezpeky intelektual'nykh merezh: arkhitektury, komunikatsiyni merezhi, kiberataky, kontrzakhody ta vyklyky // Kiberbezpeka. 2024. Tom... 7, № 1. S. 10. DOI: 10.1186/s42400-023-00200-w. 14. Ayele E. D., Honsales Dzh. F., Teuv V. B. Pidvyshchennya kiberbezpeky v rozpodilenykh mikromerezhakh: ohlyad komunikatsiynykh protokoliv ta

ISSN 2306-5478

standartiv // Sensors. 2024. Tom 24, № 3. S. 854. DOI: 10.3390/s24030854. 15. Elsebaay A. ta in. Bahatorivneva komunikatsiyna stratehiya Internetu rechey dlya intelektual'noyi merezhi mikromerezhi // Pratsi. 2019. Tom 42, № 1. S. 38. DOI: 10.3390/ecsa-6-06554. 16. Zia M. F., Elbuchikhi E., Benbuzid M. Systemy upravlinnya enerhiyeyu v mikromerezhakh: krytychnyy ohlyad metodiv, rishen' ta perspektyv // Prykladna enerhiya. 2018. Tom 222. S. 1033–1055. DOI: 10.1016/j.apenergy.2018.04.103. 17. Chaudkhari H. ta in. Ohlyad stratehiy keruvannya systemamy nakopychennya enerhiyi ta upravlinnya enerhiyeyu v mikromerezhi // Enerhetyka. 2021. Tom 14, № 16. S. 4929. DOI: 10.3390/en14164929. 18. Mvinuka L. ta in. Enerhetychni systemy velykykh danykh: ohlyad praktyk ta pov'yazanykh z nymy problem // Ohlyad komp'yuternykh nauk. 2026. Tom. 60. DOI: 10.48550/arXiv.2507.19154. 19. Lyu D. ta in. Zastosuvannya, arkhitektura ta problemy peryferiynykh obchyslen' u povsyudnomu enerhetychnomu Interneti rechey // Frontiers in Energy Research. 2022. Tom 10. S. 850252. DOI: 10.3389/fenrg.2022.850252. 20. Tank B., Handi V. Porivnyal'ne doslidzhennya khmarnykh obchyslen', peryferiynykh obchyslen' ta tumannykh obchyslen' // Dosyahnennya v transdystsyplinarniy inzheneriyi. 2023. S. 665–670. DOI: 10.3233/ATDE221329. 21. Hautam V. L., Landzhevar U. A. Khmarni, tumanni ta peryferiyni obchyslennya: porivnyal'nyy analiz arkhitektur, zastosuvan', problem bezpeky ta produktyvnosti // Materialy Mizhnarodnoyi konferentsiyi z dosyahnen' v menedzhmenti ta tekhnolohiyakh (ICAMT). 2025. S. 130–137. 22. Sandzhalave YU. ta in. Rozumni merezhi na bazi shtuchnoho intelektu v eru 6G: kompleksne doslidzhennya bezpeky ta intelektual'nykh enerhetychnykh system // IEEE Open Journal of the Communications Society. 2025. Tom 6. S. 7677–7719. DOI: 10.1109/OJCOMS.2025.3609144. 23. Akhmad Khan A. ta in. Zbirnyk tsiley optymizatsiyi, obmezhen', instrumentiv ta alhorytmiv dlya upravlinnya enerhiyeyu v mikromerezhakh // Renewable and Sustainable Energy Reviews. 2016. Tom 58. S. 1664–1683. DOI: 10.1016/j.rser.2015.12.259. 24. Olatomiva L. ta in. Stratehiyi upravlinnya enerhiyeyu v hibrydnykh systemakh vidnovlyuvanoyi enerhiyi: ohlyad // Renewable and Sustainable Energy Reviews. 2016. Tom 62. S. 821–835. DOI: 10.1016/j.rser.2016.05.040. 25. Kayza H. ta in. Tumanni obchyslennya na promyslovomu rivni: arkhitektura, zatrymka, enerhiya ta bezpeka: ohlyad // Heliyon. 2020. Tom 6, № 4. S. e03706. DOI: 10.1016/j.heliyon.2020.e03706.

**Drohobytskyi M.V.** [1; ORCID ID: 0009-0009-6865-6034],
PhD Student,
**Lutsyk N.S.** [1; 0000-0002-0361-6471],
Ph.D., Associate Professor
**Mudryi I.V.** [1; 0009-0003-1409-2612],
PhD Student
**Lototskyi V.P.** [1; 0009-0008-0531-5876],
PhD Student

[1] Ternopil Ivan Puluj National Technical University, Ternopil

# ANALYSIS OF COMPUTER SYSTEM ARCHITECTURES FOR MONITORING AND CONTROL OF MICROGRIDS

**The article examines computer system architectures designed for the monitoring and control of microgrids. The relevance of the study is driven by the fact that the growing deployment of microgrids is accompanied by the transformation of modern electric power systems into complex cyber-physical infrastructures, whose efficiency and operational reliability are largely determined by the architecture of computer systems and communication networks.**

**The paper analyzes the multi-level organization of such systems, including field devices, edge nodes, data processing and management subsystems, and operator interfaces. It considers communication infrastructure, approaches to data acquisition and processing, software platforms supporting energy management functions, edge computing, and cybersecurity mechanisms. The features of centralized, decentralized, and hybrid architectures are summarized, and the role of communication-aware design in ensuring system resilience and scalability is identified.**

**A generalized classification-based characterization of microgrid computer system architectures is proposed, typical architectural approaches are identified, and the main design features and constraints are outlined. As a result of the review, key research gaps were identified, including the lack of unified reference architectures, insufficient development of edge-oriented solutions, interoperability issues, and the fragmented integration of cybersecurity mechanisms. A generalized multi-level architecture of a computer system for microgrid monitoring and control is also**

ISSN 2306-5478

**proposed. The obtained results may serve as a basis for further analysis and design of resilient, scalable, and interoperable monitoring and control systems for microgrids.**
**Keywords: microgrids, computer system architecture, monitoring and control, communication infrastructure, edge computing, cybersecurity, review, architectural overview**

Отримано: 26 січня 2026 року
Прорецензовано: 20 лютого 2026 року
Прийнято до друку: 27 березня 2026 року