DOI 10.15276/imms.v16.no1.157
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.16 (2026), No. 1, pp. 157-168

БАГАТОКРИТЕРІАЛЬНИЙ ФРЕЙМВОРК ВИБОРУ АРХІТЕКТУРИ ПІДКЛЮЧЕННЯ ДО БАЗ ДАНИХ У РОЗПОДІЛЕНИХ СИСТЕМАХ З ПІДВИЩЕНИМИ ВИМОГАМИ ДО КІБЕРБЕЗПЕКИ

О.А. Сиропятов, Л.М. Тимошенко

Національний університет «Одеська політехніка»
1, Шевченка пр., Одеса, 65044, Україна
Emails: o.a.syropiatov@op.edu.ua, l.m.timoshenko@op.edu.ua

Розглянуто розробку багатокритеріального фреймворку для обґрунтованого вибору архітектури підключення до баз даних у системах з підвищеними вимогами до кібербезпеки, а саме в сегментах SCADA/IoT, зокрема, критичній інфраструктурі, енергетиці, промисловості тощо. Запропонований підхід поєднує ієрархію критеріїв (безпека, продуктивність, експлуатаційно-вартісні характеристики) з методами багатокритеріального аналізу рішень (MCDM) (зокрема, AHP та TOPSIS), що дозволяє формалізовано оцінювати компроміс між конфіденційністю, цілісністю, затримками, відмовостійкістю та витратами для різних архітектур: локальне розміщення власних серверів з підключенням через безпечний VPN-тунель, пряма публічна хмара, гібридні хмари, краєцентричний підхід та супутникове покращення (включаючи низькоорбітальний резерв). Проведений аналіз пов'язаних робіт виявив невирішене питання – відсутність уніфікованого MCDM-фреймворку для порівняння архітектур у багатоканальних середовищах з урахуванням стандартів NIST CSF 2.0, IEC 62443 та GDPR. Запропонована модель перевірена на аналізі ситуації віддаленої підстанції, де переважною є гібридна архітектура з крайовими компонентами та супутниковим резервуванням. Практична реалізація фреймворку містить послідовність кроків (Вхід→Ваги→Оцінювання→ Ранжування→Валідація), чекліст, матриці оцінок та рекомендації щодо табличного онлайн інструменту. Результати демонструють адаптивність підходу до різних профілів пріоритетів та доменів, що сприяє зниженню суб'єктивності архітектурних рішень і підвищенню рівня кібербезпеки розподілених систем.

Ключові слова: архітектура підключення до БД, кібербезпека, SCADA/IoT, гібридна/мультихмара, граничні обчислення, супутниковий зв'язок, багатокритеріальний аналіз рішень.

Вступ. Сучасні інформаційні системи з підвищеними вимогами до кібербезпеки – від SCADA/IoT-сегментів критичної інфраструктури до фінансових платформ – потребують постійного та передбачуваного доступу до баз даних, розподілених між локальними, хмарними та периферійними контурами. Перехід до гібридних хмарних моделей, розвиток периферійних обчислень і поява супутникових каналів зв'язку значно ускладнили архітектури підключення до БД, посиливши залежність від мережі та площу атаки.

У цих умовах вибір архітектури перетворюється на багатокритеріальну задачу, що вимагає одночасного врахування регуляторних вимог і стандартів (NIST CSF 2.0, IEC 62443, GDPR [1-3]), моделі загроз домену та обмежень щодо затримок, пропускної спроможності й вартості. На практиці рішення часто приймаються в багатоканальному середовищі (публічна хмара, приватні VPN-тунелі, 5G/периферійне підключення, супутникові сегменти), компроміси між безпекою, продуктивністю та експлуатаційними витратами слабо формалізовані й залежать від суб'єктивного досвіду архітекторів [4, 5].

Метою роботи є розроблення багатокритеріального фреймворку для обґрунтованого та відтворюваного вибору архітектури підключення до баз даних у системах з високими вимогами до кібербезпеки. Запропонований підхід поєднує ієрархію критеріїв (безпека, продуктивність, експлуатаційні та вартісні характеристики)

з методами багатокритеріального аналізу рішень (зокрема AHP/TOPSIS, вже застосованими в кібербезпеці [6, 7]) і забезпечує вибір архітектури з урахуванням кібербезпеки, затримки, відмовостійкості та співвідношення з витратами.

Огляд пов'язаних робіт та аналіз предметної області. У літературі та галузевих рекомендаціях архітектуру підключення до баз даних у захищених системах класифікують за типом каналу зв'язку та ступенем централізації:

– публічні прямі хмарні архітектури, пряме підключення застосунків до систем управління базами даних (СУБД) у публічній хмарі через захищені інтернет-канали;

– приватні або локальні рішення – доступ через VPN-тунелі до внутрішніх баз даних у власних центрах обробки даних організації;

– гібридні схеми з кількома хмарами – дані та сервіси розподілені між кількома хмарними провайдерами та локальною інфраструктурою;

– крайові (edge) варіанти – частина даних і логіки дублюється або кешується на периферійних вузлах, тоді як основна база даних залишається в хмарі чи локально;

– спеціальні сценарії – використання супутникових і 5G-каналів для віддалених сегментів систем промислової автоматизації (SCADA) та Інтернету речей (IoT), а також розподілених промислових об'єктів [6].

Стандарти IEC 62443 та галузеві рекомендації для промислових систем підкреслюють важливість сегментації мережі та зонального доступу до промислових БД. Однак вони розглядають підключення переважно в контексті загальної конвергенції промислових і інформаційних технологій, без формалізованого порівняння прямого хмарного доступу, VPN, гібридних і крайових рішень за єдиними критеріями [8, 9]. Дослідження безпеки гібридних і мультихмарних середовищ пропонують класифікації розміщення даних (одна хмара, кілька хмар, гібрид, континуум хмара-край), але архітектури підключення до БД описують лише на рівні типових шаблонів, без окремої багатокритеріальної оцінки [6].

Оцінювання безпеки компонентів підключення (СУБД, проміжне ПЗ, VPN-шлюзи, хмарні сервіси) базується на стандартизованих метриках, зокрема CVSS для вразливостей та моделі NIST CSF 2.0 для управління ризиками. У сфері критичної інфраструктури та систем SCADA/IoT безпека каналів і вузлів додатково відповідає вимогам IEC 62443, зокрема концепціям рівнів безпеки, зон і каналів зв'язку, які непрямо визначають дозволені схеми доступу до промислових баз даних [9].

Продуктивність каналів і архітектур оцінюють за затримкою, варіацією затримки, пропускною здатністю та доступністю. Це особливо актуально для хмарних, крайових і супутникових сценаріїв. Публікації про продуктивність хмарних і крайових систем зосереджуються переважно на мережевих та обчислювальних аспектах, ігноруючи спільний облік безпеки, експлуатаційні витрати, складності управління та прив'язку до постачальника під час вибору архітектури підключення [10]. Окрема група - роботи з багатокритеріального аналізу рішень, зокрема методи AHP, TOPSIS та їх модифікації. Ці методи застосовують для оцінювання ризиків кібербезпеки, пріоритизації заходів захисту та порівняльного вибору технічних рішень. Вони дозволяють одночасно враховувати критерії безпеки, вартості, експлуатаційної складності та продуктивності, отримуючи числову оцінку й ранжування варіантів. Проте такі дослідження переважно стосуються вибору засобів захисту (міжмережеві екрани, IDS, шифрування) або загального оцінювання ризиків, а не архітектур підключення до баз даних у мультихмарних, крайових чи промислових системах. Огляд літератури свідчить про таке:

– стандарти (NIST CSF 2.0, IEC 62443, GDPR) встановлюють загальні вимоги до захисту даних і каналів, але не пропонують формалізованого механізму вибору архітектури підключення [1, 9];

– дослідження хмарної, гібридної та крайової безпеки описують архітектури переважно на рівні загальних рекомендацій і кращих практик, фокусуючись на загрозах

і заходах захисту, а не на кількісному аналізі компромісів «безпека–продуктивність–вартість» для різних схем доступу до баз даних [6];

– методи MCDM успішно застосовуються в кібербезпеці для оцінювання ризиків і вибору засобів захисту, без адаптації до задачі вибору архітектур підключення в багатоканальних середовищах та галузевих сценаріях.

Отже, відсутній інтегрований багатокритеріальний механізм, який поєднував би класифікацію архітектур підключення до баз даних, систему критеріїв та формалізований механізм ранжування альтернатив для багатоканальних високобезпечних сценаріїв.

Методика та запропонована модель оцінювання. Запропонований фреймворк орієнтований на системи з високими вимогами до кібербезпеки та доступності даних, переважно в сегментах SCADA та Інтернету речей (IoT) енергетики й суміжних галузей критичної інфраструктури. Галузеві звіти вказують на зростання атак і вразливостей у промисловій автоматизації, пов'язаних насамперед з віддаленим доступом, недостатньою сегментацією мережі та незахищеними каналами зв'язку [10]. Тому архітектури підключення до технологічних баз даних мають враховувати мережеву експозицію, гібридні схеми доступу та резервування.

Зокрема, в енергетиці поширені змішані схеми: крайові обчислення на об'єктах, VPN-тунелі до центрів керування та аналітичних платформ, а також супутникові канали як основний або резервний маршрут для важкодоступних вузлів. Локальна крайова обробка забезпечує затримки в одиниці-десятки мілісекунд і розвантажує магістральні канали. Крайові вузли повинні відповідати принципам IEC 62443 (зони безпеки, канали зв'язку, автентифікація, сегментація) [7,11]. Для супутникових сценаріїв типові затримки становлять 25–50 мс в оптимальних умовах і 40-80 мс у реальних для низькоорбітальних систем (наприклад, Starlink), з можливими сплесками до 150–250 мс; для геостаціонарних – понад 600 мс. Хоча основний фокус – на SCADA/енергетиці, фреймворк адаптується до інших доменів (транспорт, логістика, корпоративні інформаційні системи) з подібними компромісами між безпекою, затримками, доступністю та вартістю. У них застосовують ті ж класи архітектур, але з іншими пріоритетами та обмеженнями.

Модель оцінювання базується на ієрархії критеріїв, поділених на три групи, що узгоджується з дослідженнями багатокритеріальних методів у кібербезпеці.

Критерії безпеки:

– конфіденційність і цілісність даних (шифрування каналу та бази даних, актуальні криптоалгоритми, контроль цілісності);

– доступність (цільові показники 99,9% або 99,99% відповідно до вимог енергетичних об'єктів);

– підтримка ідеальної прямої секретності (PFS) у протоколах;

– принципи нульової довіри (zero trust): строга автентифікація та авторизація на кожному сегменті, мінімізація довірених зон;

– рівень сегментації та мікросегментації за зонами і каналами IEC 62443 [7, 9].

Для критичної інфраструктури особливе місце – у сегментації, обмеженні привілеїв, мінімізації експозиції, нульової довіри для зовнішніх, супутникових каналів [10].

Критерії продуктивності:

– затримка: одиниці-десятки мс для локального краю, десятки мс для хмарних центрів даних, 40–80 мс для LEO-супутників, понад 600 мс для GEO;

– варіація затримки: критична для протоколів реального часу;

– пропускна здатність: сотні Мбіт/с низхідного і десятки Мбіт/с висхідного каналу зв'язку для сучасних LEO-систем;

– стійкість: резервні маршрути, відмовостійкість, схеми

активний/резервний, багатоканальне підключення.

Експлуатаційно-вартісні критерії:

– капітальні та операційні витрати: крайові вузли підвищують капітальні, але можуть знижувати операційні за рахунок оптимізації трафіку; чистий хмарний підхід діє навпаки;

– ризик залежності від постачальника, особливо в публічних хмарах і спеціалізованих периферичних платформах;

– складність управління (потреба в спеціалістах, кількість компонентів для оновлення, централізований моніторинг).

Кількісні параметри (затримка, пропускна здатність, доступність) базуються на звітах і вимірюваннях; якісні за напівкількісними шкалами, каліброваними на галузевих даних.

Формалізація метрик і багатокритеріальний процес.

Різнотипні критерії нормалізуються до шкали [0;1] за допомогою min-max або z-score перетворень. Для негативних критеріїв (затримка, витрати) застосовується обернена формула. Якісні показники кодуються впорядкованими шкалами.

Вагові коефіцієнти визначаються методом аналітичного ієрархічного процесу або його модифікаціями [11, 12]. Експерти будують матриці попарних порівнянь, що дозволяє отримати узгоджені ваги для конкретного домену (наприклад, пріоритет безпеки та доступності над вартістю в критичній інфраструктурі).

Агрегування виконують зваженою сумою або методом TOPSIS, де визначають найкращу та найгіршу альтернативи, обчислюють близькість реальних варіантів до еталонів. Це забезпечує прозоре ранжування архітектур (прямий хмарний, локальний/ VPN, гібридний/мультихмарний, крайовий, супутниковий) у SCADA/ енергетиці.

Стійкість результатів перевіряється аналізом чутливості за вагами та ключовими параметрами. Формуються сценарії пріоритетів («безпека понад усе», «доступність понад усе», «врахування вартості» тощо) з варіюванням ваг у реалістичних межах. Це дозволяє виявити стійкі рішення та архітектури, чутливі до змін пріоритетів.

Для супутникових архітектур моделюються затримки на основі даних LEO-систем (медіанна затримка 40-80 мс, співставна з наземними мережами, але з можливими сплесками) порівняно з GEO (понад 600 мс). Показники інтегрують в критерії затримки, варіація затримки та стійкості й застосовують в сценаріях «основний наземний/VPN + резервний LEO» або «супутниковий як основний для віддалених об’єктів».

Методика базується на трьох принципах.

1. Вибір архітектури підключення – домен-специфічна багатокритеріальна задача: для SCADA/енергетики визначається набір архітектур і профіль вимог, що відображає регуляторні обмеження, модель загроз та експлуатаційний контекст .

2. Оцінювання будуєть на ієрархії критеріїв безпеки, продуктивності, експлуатаційно-вартісних характеристиках. Кількісні параметри калібруються за галузевими даними.

3. Метрики нормалізують, ваги визначають через експертні профілі, агрегування – за допомогою багатокритеріального механізму з обов’язковим аналізом чутливості, особливо для затримки та доступності в крайових і супутникових сценаріях.

У межах запропонованого фреймворку розглядають п’ять базових класів архітектур підключення до баз даних у системах SCADA/енергетики та суміжних доменах.

1. Прямий публічний хмарний доступ – застосунки або SCADA-шлюзи звертаються до СУБД у публічній хмарі через захищені інтернет-канали без виділених приватних.

2. Локальні/VPN-архітектури – бази даних розміщуються в локальних центрах обробки даних або на майданчиках оператора критичної інфраструктури; віддалені об’єкти підключаються через IPsec/OpenVPN/MPLS-тунелі та міжмережеві екрани.

3. Гібридні/мультихмарні сценарії – дані та сервіси розподілені між локальними сегментами та одним або кількома хмарними провайдерами; доступ до БД здійснюється через комбінацію приватних каналів, VPN і прямого хмарного підключення.

4. Крайово-орієнтовані архітектури – використовують промисловий крайовий рівень (шлюзи, локальні вузли) для зберігання й обробки ключових даних та агрегатів телеметрії з подальшою передачею агрегованих або відкладених даних до центральної бази в хмарі чи центрі обробки даних.

5. Архітектури з супутниковим/5G-підсиленням – забезпечують доступ для віддалених об’єктів через супутникові або 5G-канали (як основний або резервний маршрут) у поєднанні з одним із зазначених варіантів розміщення баз даних.

Це забезпечує відтворюваність, адаптованість і прозорість обґрунтування вибору архітектури в системах критичної енергетичної інфраструктури (рис.1).

Класифікація відображає осі варіативності: місце розміщення бази даних та ступінь розподіленості (одна хмара, мультихмарна/гібридна).

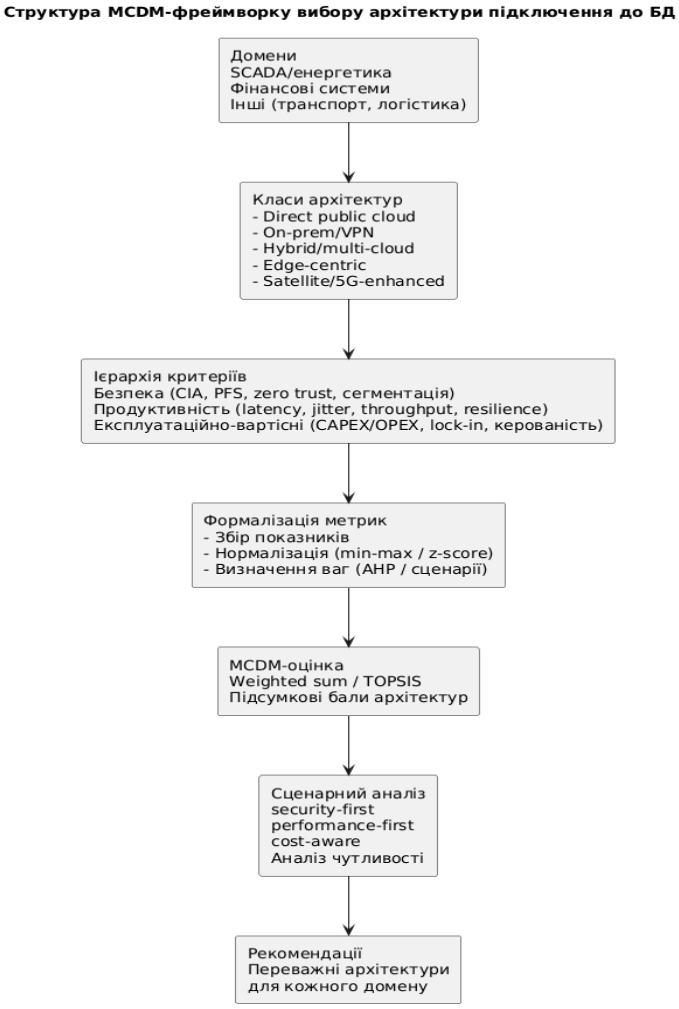

Рис. 1. Структура MCDM-фреймворку

Кожен клас оцінюють за ієрархією критеріїв безпеки, продуктивності, експлуатаційно-вартісних характеристик (рис.2).

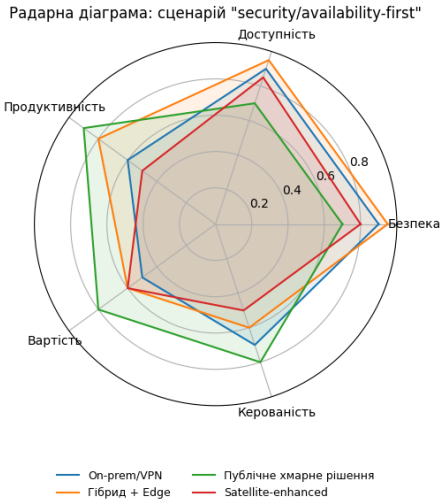

Рис. 2. Радарна діаграма оцінок п’яти архітектур за трьома групами критеріїв

Гібридна/крайова архітектура демонструє найбільш збалансований профіль(табл.1). Оцінки формують на основі кількісних і якісних даних, нормалізують до шкали [0;1].

Таблиця 1

Нормалізовані оцінки та підсумкові бали архітектур у базовому сценарії

Архітектура	Безпека	Продуктивність	Експлуатаційно-вартісні	Підсумковий бал (TOPSIS)	Ранг
Гібридна/мультихмарна + крайова	0,95	0,85	0,70	0,88	1
Локальна/VPN	0,90	0,75	0,80	0,82	2
З супутниковим/5G-підсиленням (резерв)	0,75	0,65	0,75	0,71	3
Крайово-орієнтована	0,85	0,90	0,60	0,78	4
Прямий публічний хмарний	0,60	0,80	0,85	0,68	5

У базовому сценарії «безпека/доступність понад усе» найбільшу вагу мають критерії безпеки та доступності, меншу – продуктивності, найменшу – експлуатаційно-вартісні.

Застосування моделі TOPSIS показує, що верхні позиції мають гібридні крайово-орієнтовані архітектури, де низькі затримки на рівні об’єкта, висока відмовостійкість завдяки локальній обробці, жорстка сегментація за IEC 62443 при прийнятних витратах.

Прямі публічно-хмарні архітектури отримують нижчі бали через більшу поверхню атаки та залежність від публічних інтернет-каналів, попри переваги за витратами. Архітектури з супутниковим/5G-підсиленням займають проміжні позиції, залежно від ролі каналу (основний чи резервний) та критичності затримок і варіації затримки.

Стійкість результатів перевіряється трьома профілями пріоритетів: «безпека понад усе», «продуктивність понад усе» та «врахування вартості».

У сценарії «продуктивність понад усе» зростають ваги затримки, варіація затримки та пропускної здатності, що підвищує позиції архітектур із низькими затримками (прямий хмарний і гібридний з близькими центрами даних), тоді як супутниково-домінуючі рішення знижуються через нестабільну затримку. У сценарії «врахування вартості» перевагу мають простіші архітектури (чистий хмарний або спрощений локальний/VPN) завдяки нижчим вартості та простоті управління порівняно з крайовими рішеннями.

Аналіз чутливості свідчить, що гібридні крайово-орієнтовані архітектури стабільно входять до топ-позицій за високого пріоритету безпеки та доступності, типового для SCADA/енергетики. Це базові для пілотних впроваджень, тоді як чисто публічно-хмарні та «супутник як основний» підходи доцільні лише як спеціалізовані з додатковими заходами захисту. Гібридна/крайова стабільно в топ-2, супутникова знижується в «продуктивність понад усе», пряма хмарна підвищується у «врахування вартості» (рис.3).

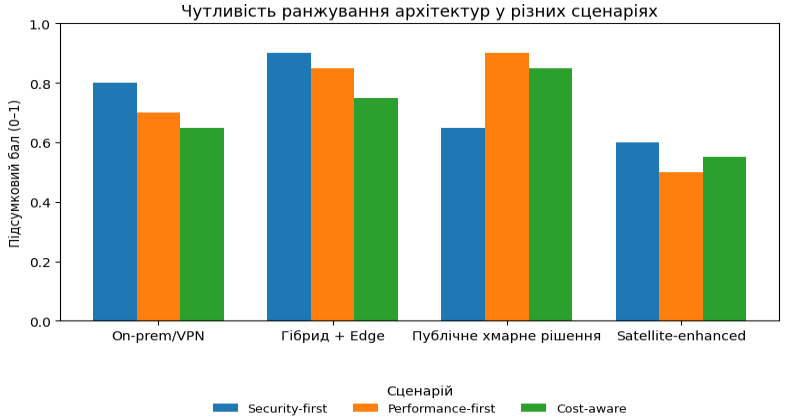

Рис. 3. Результати аналізу чутливості: підсумкові бали архітектур у трьох сценаріях

У SCADA/енергетиці за профілем «безпека/доступність понад усе» найбільш збалансованими є гібридні крайово-орієнтовані архітектури з високим рівнем безпеки й доступності з прийнятною продуктивністю й витратами. Прямі публічно-хмарні та супутникові варіанти мають обережне застосування через підвищені ризики або затримки.

Сценарний аналіз підтверджує стабільність переваги гібридних/крайових підходів при зміні пріоритетів. Це створює основу для практичного фреймворку: поетапної процедури вибору архітектури, дерева рішень та ситуації дослідження для типового енергетичного об’єкта, що ілюструють інтеграцію моделі в реальне архітектурне проєктування.

Запропонований фреймворк і практичне застосування. Послідовність кроків фреймворку.

Крок 1 (Вхідні дані). Формалізація вимог домену – профіль загроз, регуляторні обмеження (NIST CSF, IEC 62443, галузеві стандарти), допустимі затримки та втрати, цільові показники доступності, бюджет і експлуатаційні обмеження. Фіксується перелік допустимих архітектур (прямий хмарний доступ, локальний/VPN, гібридний/ мультихмарний, крайово-орієнтований, з супутниковим/5G-підсиленням).

Крок 2 (Ваги критеріїв). Налаштування пріоритетів –аналітичний ієрархічний процес за участю експертів (інженери SCADA, оператори) [13] або сценарні профілі («безпека понад усе», «доступність понад усе», «продуктивність понад усе», «врахування вартості»).

Крок 3 (Оцінювання кандидатів). Збір кількісних та якісних показників з подальшою нормалізацією за ієрархією критеріїв.

Крок 4 (Ранжування та рекомендація). Застосування багатокритеріального механізму для розрахунку балів, ранжування та виділення оптимальних варіантів.

Крок 5 (Валідація). Перевірка рекомендацій через пілотні впровадження, моделювання сценаріїв/порівняння з даними інцидентів і SLA, з можливою корекцією ваг.

Фреймворк реалізується як спрощена схема ухвалення рішень (рис.4).

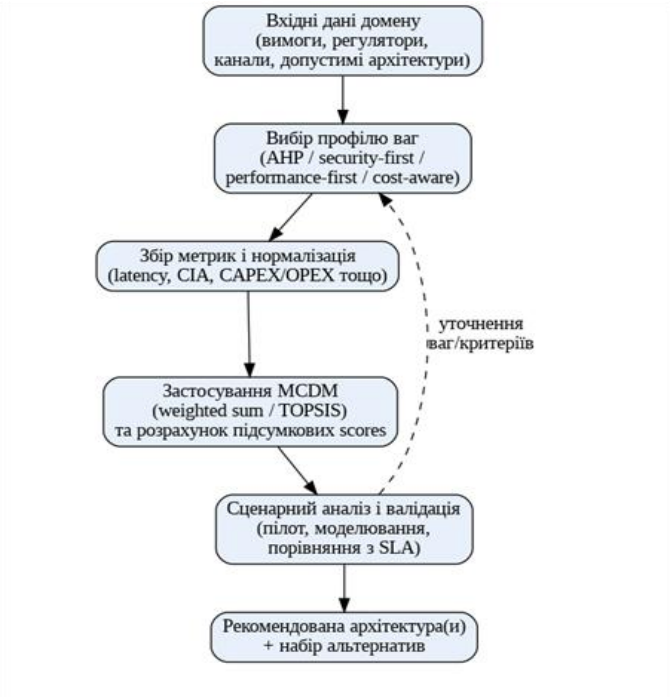

Рис. 4. Схема фреймворку

Процес починається з вибору домену (SCADA/енергетика, чи інший), уточнення вимог та каналів. Далі – вибір профілю ваг (наприклад, «безпека/доступність понад усе» для SCADA). Фінальні вузли рекомендують 1-2 архітектури (гібридний/мультихмарний + крайовий для об’єктів з надійним каналом; локальний/VPN + супутниковий резерв для віддалених).

Ситуація: SCADA у віддаленій енергетиці з супутниковим резервуванням (рис.5).

Розглянемо віддалений енергетичний об’єкт (підстанція чи вузол відновлюваної енергетики)з основним VPN-каналом і низькоорбітальним супутниковим резервом.

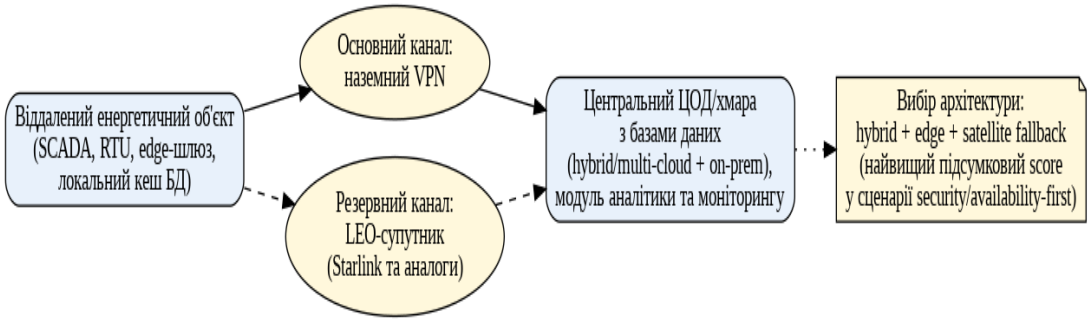

Рис. 5. Схема кейсу для віддаленої підстанції

Вимоги: відповідність IEC 62443 (оновлені 2025 року правила сегментації та мікросегментації), доступність ≥99,9%, затримка телеметрії ≤200 мс, обмежені витрати і навантаження на персонал. Допустимі архітектури: локальний/VPN, гібридний/ мультихмарний + крайовий, з супутниковим резервом; прямий публічний хмарний – лише допоміжний. Профіль ваг: «безпека/доступність понад усе» (вага безпеки та доступності 0,6–0,7; продуктивності 0,2-0,25; витрат 0,1–0,15). На основі даних 2025 року (медіанна затримка Starlink у пікові години 25-45 мс з тенденцією зниження) розрахунок TOPSIS показує лідерство гібридного/мультихмарного+крайового варіанту (локальне кешування, основний VPN + LEO резерв). Переваги: висока безпека/сегментація, стійкість до відмов, прийнятні затримки та витрати. У табл. 2 зображено чекліст за кроками.

Таблиця 2.

Чекліст за кроками (контрольні запитання для кожного етапу)

Крок	Ключові контрольні пункти	Статус	Примітки
Вхідні дані (Input)	Домен: SCADA/енергетика, віддалена підстанція. Доступність≥99,9%, затримка ≤200 мс Регуляторні вимоги. .Допустимі архітектури та виключення	Так / Ні / Частково	
Вибір профілю ваг	Профіль «безпека/доступність понад усе». Ваги: безпека+ доступність 0,6–0,7; продуктивність 0,2–0,25; витрати 0,1–0,15. Джерело ваг задокументовано (AHP або сценарний)	Так / Ні / Корекція	
Збір метрик та нормалізація	Дані затримки/jitter для VPN, краю та LEO. Оцінка CAPEX/OPEX .Опис сегментації, нульової довіри, керованості. Нормалізація без аномалій	Так / Ні / Частково	
Оцінка та ранжування (MCDM)	Застосовано зважена сума / TOPSIS. Бали узгоджуються з експертною оцінкою. Виділено лідера (гібридний + крайовий з VPN + LEO резерв)	Так / Ні / Перегляд	Документувати результати
Валідація (Validation)	Моделювання відмов каналів Порівняння з історичними інцидентами/SLA Підтвердження або корекція архітектури	Виконано / Заплановано / Корекція	

У табл. 3 наведено приклад збору метрик та оцінок для кейсу віддаленої підстанції.

Таблиця 3.

Матриця критеріїв та нормалізованих оцінок

Архітектура	Доступність С1	Затримка С2)	Безпека (С3)	Витрати (С4)	Складність (С5)
А1: Локальний/VPN	0,80	0,70	0,75	0,40	0,50
А2: Гібридний + крайовий (VPN + LEO резерв)	0,90	0,80	0,85	0,60	0,65
А3: Супутниковий як основний	0,70	0,65	0,70	0,55	0,45

Аналіз матриці критеріїв підтверджує переваги рекомендованої архітектури.

А1. Висока доступність і прийнятна затримка, але обмежена масштабованість та вищі операційні витрати на локальну інфраструктуру.

А2.Завдяки локальному кешуванню та резервному низькоорбітальному каналу досягає найкращого балансу – високі показники доступності, низька затримка та посилена безпека за помірних витрат (лідер за С1-С3, середні С4-С5). Це дозволяє знизити загальні витрати на 10-30% порівняно з локальними рішеннями за рахунок оптимізації трафіку та зменшення залежності від дорогого обладнання.

А3. Спрощує локальну інфраструктуру (нижчі витрати), але має нестабільності затримок і підвищених вимог до управління (нижчі бали за С2 та С5).

Для організацій з розвиненою ІТ-інфраструктурою можлива реалізація онлайн-інструменту (web- або intranet-застосунку), інтегрує базу типових архітектур, профілів доменів і актуальних метрик, автоматизує нормалізацію, розрахунок та візуалізацію (радарні діаграми, чутливість).

Розглянемо приклад роботи онлайн-інструменту (кейс: віддалена підстанція). Інтерфейс складається з трьох екранів.

Домен та вимоги: вибір профілю «SCADA/енергетика – віддалена підстанція», параметри: доступність ≥99,9%, затримка ≤200 мс, VPN основний + LEO резерв. Архітектури: варіанти А1, А2, А3. Автоматичне завантаження даних (затримка LEO 2025: 25-45 мс, тенденція <30 мс). Пріоритети: сценарій «безпека/доступність понад усе» (ваги: безпека+доступність ≈0,65; продуктивність ≈0,2; витрати ≈0,15), можливість коригування.

Інструмент автоматично нормалізує та розраховує TOPSIS (А2 – лідер), виводить рейтинг у таблиці та радарній діаграмі, генерує діаграму чутливості для альтернативних

сценаріїв, формує звіт: припущення, ваги, рекомендація (гібридний + крайовий з LEO резерв) та ключові компроміси. Прискорює ухвалення рішень у 2-3 рази, економить до 50% часу архітекторів та 15-30% витрат на проєктування/впровадження.

Запропонований фреймворк показує, що в домені SCADA/енергетики пріоритетними є не традиційні локальні/VPN-архітектури, а гібридні рішення з крайовими компонентами та хмарними сервісами. Цей результат дещо несподіваний для організацій, які вважають повне локальне розміщення баз даних «найбезпечнішим». Насправді поєднання сегментації, локального кешування та резервних каналів (наприклад, низькоорбітальних супутникових LEO) забезпечує кращий баланс безпеки, доступності та продуктивності [13]. У кейсі віддаленої підстанції гібридна/мультихмарна + крайова архітектура з VPN та LEO резервом найвищі бали, а не «інтуїтивно безпечніший» локальний підхід.

Фреймворк кількісно демонструє чутливість рішень до профілю пріоритетів: невелика зміна ваг на користь продуктивності чи витрат може змінити лідера, але гібридні крайові варіанти стабільно залишаються в топі. Це узгоджується з галузевими трендами – переходом до гібридних/мультихмарних і промислових крайових рішень, широким впровадженням LEO-супутників у критичній інфраструктурі. На відміну від евристичних підходів фреймворк надає формалізоване обґрунтування, дозволяючи архітекторам працювати зі звичними метриками (угода про послуги, затримка, витрати, IEC 62443) у прозорій багатокритеріальній процедурі.

Обмеження моделі. Перевірено переважно на SCADA/енергетиці; інші домени (наприклад, з жорсткими вимогами до затримки) потребують окремої адаптації та калібрування. Спрощено аспекти: не враховуються детальні топології мереж, внутрішні механізми СУБД, засоби виявлення/реагування, взаємозалежності критеріїв (вплив додаткового захисту на затримку, витрати). Багато даних базуються на моделюванні, узагальнених показниках провайдерів, експертних оцінках, а не на вимірюваннях.

Висновки та подальші дослідження. У роботі запропоновано класифікацію архітектур підключення до баз даних: прямий публічний хмарний доступ, локальний/VPN, гібридний/мультихмарний, крайово-орієнтований, з супутниковим/5G-підсиленням, на критеріях безпеки, продуктивності, доступності, витрат та експлуатаційної складності, як основа формалізованого порівняння альтернатив. На її базі розроблено багатокритеріальну модель оцінки з нормалізацією показників, методами AHP/TOPSIS та сценарним аналізом для різних профілів пріоритетів («безпека понад усе», «продуктивність понад усе», «врахування вартості»).

Ключовий результат – практичний фреймворк вибору архітектури, орієнтований на SCADA/енергетику та критичну інфраструктуру. Це послідовність кроків, блок-схема рішень, чекліст, матриці критеріїв та кейс віддаленої підстанції з рекомендованою гібридною/мультихмарною + крайовою архітектурою та низькоорбітальним супутниковим резервом. Фреймворк переводить неформальні міркування у відтворювану, прозору процедуру, прискорює ухвалення рішень і полегшує обґрунтування перед стейкхолдерами. Прив’язка до реальних метрик, візуалізації та потенціал онлайн-інструменту роблять його ефективним для проєктування нових і модернізації наявних систем. Для операторів критичної інфраструктури це означає зниження суб’єктивних ризиків, економію ресурсів і повторне використання досвіду через типові профілі.

Напрямки подальших досліджень – розширення на нові домени: використання крайових/5G-рішень, супутникових систем нового покоління та високочастотних застосувань з низькою затримкою, інтеграція динамічних механізмів (AI-підтримка адаптації маршрутів і протоколів до умов мережі); участь у стандартизації методик оцінки архітектур для критичних інфраструктур, узгодження з IEC 62443 та міжнародними ініціативами. Реалізація цих напрямів підвищить надійність фреймворку та перетворить його на основу галузевих рекомендацій і кращих практик.

Список літератури

1. Pascoe C., Quinn S., Scarfone K. The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper (CSWP) 29. Gaithersburg: National Institute of Standards and Technology, 2024. DOI: 10.6028/NIST.CSWP.29.
2. ISA/IEC 62443 Series of Standards. International Society of Automation; International Electrotechnical Commission. 2024–2025. URL: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.
3. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation – GDPR). *Official Journal of the European Union*. 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.
4. Cloud Security Alliance. Top Threats to Cloud Computing 2024. Cloud Security Alliance, 2024. URL: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024.
5. Fortinet. Multi-Cloud Security Challenges and Best Practices. Fortinet Resources, 2025.
6. Multi-cloud and hybrid cloud security challenges. Computers & Security (various articles), 2024–2025.
7. Advantech. Industrial Edge Computing Security Solutions. Advantech Resources, 2024.
8. IoT Analytics. Satellite IoT Market Report 2025–2030. IoT Analytics, June 2025. URL: https://iot-analytics.com/satellite-iot-market-report-2025-2030.
9. Elisity. IEC 62443 in 2025: Network Segmentation Requirements and Changes. Elisity Blog, January 2025. URL: https://www.elisity.com/blog/iec-62443-in-2025-network-segmentation-requirements-and-changes.
10. Nozomi Networks OT/IoT Cybersecurity Trends and Insights Report. Nozomi Networks, February 2025. URL: https://www.nozominetworks.com/resources/reports/ot-iot-cybersecurity-trends-2025.
11. Reimagining SCADA: The Convergence of Cloud, Edge, and Intelligent Automation. Adisra, October 2025. URL: https://adisra.com/reimagining-scada-the-convergence-of-cloud-edge-and-intelligent-automation/
12. Saaty R. W. The analytic hierarchy process – what it is and how it is used. *Mathematical Modelling*. 1987. Т. 9, № 3–5. С. 161–176.
13. Ookla Starlink Performance Report 2025. Ookla Research, 2025. URL: https://www.ookla.com/articles/starlink-us-performance-2025.

О.А. Сиропятов, Л.М. Тимошенко

MULTI-CRITIARERIA FRAMEWORK FOR SELECTING DATABASE CONNECTION ARCHITECTURE IN DISTRIBUTED SYSTEMS WITH INCREASED CYBERSECURITY REQUIREMENTS

Syropyatov O.A. Tymoshenko L.M.

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
Emails: o.a.syropiatov@op.edu.ua, l.m.timoshenko@op.edu.ua

The article discusses the development of a multi-criteria framework for the informed choice of database connectivity architecture in systems with increased cybersecurity requirements, namely in the SCADA/IoT segments, in particular, critical infrastructure, energy, industry, etc. The proposed approach combines a hierarchy of criteria (security, performance, operating cost characteristics) with multi-criteria decision analysis (MCDM) methods (in particular, AHP and TOPSIS), which allows for a formal assessment of the trade-off between confidentiality, integrity, delays, fault tolerance and costs for different architectures: local placement of own servers with connection via a secure VPN tunnel, direct public cloud, hybrid clouds, edge-centric approach and satellite enhancement (including low-orbit reserve). The analysis of related works revealed an unresolved issue - the lack of a unified MCDM framework for comparing architectures in multi-channel environments, taking into account the NIST CSF 2.0, IEC 62443 and GDPR standards. The proposed model was tested on the analysis of a remote substation situation, where a hybrid architecture with edge components and satellite redundancy is predominant. The practical implementation of the framework contains a sequence of steps (Input → Weights → Evaluation → Ranking → Validation), a checklist, assessment matrices and recommendations for a tabular online tool. The results demonstrate the adaptability of the approach to different priority profiles and domains, which helps to reduce the subjectivity of architectural decisions and increase the level of cybersecurity of distributed systems.

Keywords: database connection architecture, cybersecurity, SCADA/IoT, hybrid/multicloud, edge computing, satellite communication, multi-criteria decision analysis.