NETWORK-CENTRIC APPROACH TO BUILDING INFORMATION INFRASTRUCTURE: PRINCIPLES AND BENEFITS

МЕРЕЖЕЦЕНТРИЧНИЙ ПІДХІД ДО ПОБУДОВИ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ: ПРИНЦИПИ ТА ПЕРЕВАГИ

Maxim Holoborodko[1]
Yulii Kondratenko[2]

DOI: https://doi.org/10.30525/978-9934-26-536-5-28

Сучасні інформаційні інфраструктури розвиваються в умовах зростаючих вимог до безпеки, продуктивності та керованості. Одним із ключових підходів до їх побудови є мережецентрична архітектура, яка передбачає централізоване управління інформаційними потоками та ресурсами через єдину мережеву структуру. В умовах оборонних і державних систем мережецентричність сприяє підвищенню ситуаційної обізнаності та ефективності рішень, що є критично важливим для національної безпеки.

Однією з цих основних переваг є можливість гнучкого управління ресурсами, що забезпечується уніфікованими протоколами, програмно-визначеним мережам (SDN) та автоматизованим механізмам маршрутизації. Висока відмовостійкість і масштабованість таких систем досягається за рахунок динамічного перерозподілу навантаження, резервування критичних вузлів і використання хмарних технологій. Водночас мережецентрична модель має високі вимоги до безпеки мережі, зокрема щодо захисту каналів зв'язку та управління доступом, що вимагає комплексного підходу до її впровадження.

Мережецентричний підхід широко використовується у військових системах провідних країн, зокрема США та НАТО, для інтеграції всіх елементів бойових операцій в єдину інформаційну мережу. Це сприяє обміну даними в реальному часі та прийняттю оперативних, скоординованих рішень. Одним із прикладів є система C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and

[1] National Defence University of Ukraine
Centre for Military and Strategic Studies, Ukraine
[2] National Defence University of Ukraine
Centre for Military and Strategic Studies, Ukraine

Reconnaissance), яка об'єднує командні центри, розвідувальні підрозділи та бойові групи в єдиному інформаційному просторі.

Мережецентрична архітектура активно використовується в хмарних екосистемах таких провайдерів, як AWS, Azure і GCP. Архітектура таких провайдерів складається з регіонів, доступних зон і крайових серверів, що формують глобальну мережецентричну інфраструктуру. В її основі лежить концепція мережі як головного середовища передачі, обробки та управління даними. Інтеграція серверів, пристроїв і користувачів в єдину інформаційну систему забезпечує високий рівень доступності, масштабованості та надійності зв'язку незалежно від фізичного розташування компонентів [1].

Обробка інформації в мережецентричних інфраструктурах здійснюється на різних рівнях мережі, що зменшує навантаження на центральні сервери та покращує продуктивність системи.

Масштабованість мережецентричної інфраструктури забезпечується як вертикально (шляхом підвищення обчислювальних потужностей серверів), так і горизонтально (через додавання нових вузлів). Це дає змогу адаптувати систему до змін навантаження та зростання обсягу трафіку. Автоматизоване управління ресурсами реалізується за допомогою штучного інтелекту (AI) та програмно-налаштованих мереж (SDN), що дозволяє оптимізувати маршрутизацію трафіку, балансувати навантаження та забезпечувати кібербезпеку. У великих дата-центрах AI-алгоритми аналізують потоки даних у режимі реального часу, коригуючи роботу мережевих елементів для досягнення максимальної ефективності.

Забезпечення стійкості до збоїв та безперебійного доступу до інформації досягається за рахунок резервування каналів зв'язку, багаторівневих механізмів безпеки та розподілених систем збереження даних. Для захисту від кіберзагроз використовуються методи сегментації мережі, шифрування трафіку, багатофакторна автентифікація (MFA) та концепція ZTA (Zero Trust Architecture), що мінімізує ризики несанкціонованого доступу та атак на рівні мережі [2, с. 67–77].

Мережецентрична інфраструктура (NCI) забезпечує ефективну організацію інформаційних систем, в якій ключову роль відіграють гнучке керування мережею та розподілена обробка даних. Її принципи взаємопов'язаності, адаптивності, безпеки та стійкості до відмов роблять NCI критично важливою для хмарних обчислень, військових систем, IoT та розподілених дата-центрів.

Для масштабованого управління мережецентричними системами активно використовуються програмно-налаштовані мережі (Software-Defined Networking, SDN) та віртуалізація мережевих функцій (Network Functions Virtualization, NFV). SDN дозволяє централізовано керувати

мережею, автоматично перенаправляти трафік і оптимізувати навантаження, що підвищує продуктивність і знижує ризик перевантаження інфраструктури [3, с. 70–76].

Віртуалізація мережевих функцій (NFV) замінює апаратні мережеві пристрої (маршрутизатори, брандмауери, балансувальники навантаження) їх віртуалізованими аналогами, що працюють у хмарному середовищі або на стандартному серверному забезпеченні. Це скорочує витрати, спрощує розгортання сервісів і підвищує ефективність мережі.

У поєднанні з SDN, технологія NFV підвищує адаптивність, продуктивність і рівень безпеки хмарних середовищ, дата-центрів та критично важливих систем. Мережецентричний підхід розглядає мережу як ключовий елемент обміну даними, координації та управління ресурсами. Він забезпечує динамічний зв'язок між обчислювальними потужностями, сервісами та користувачами, підвищуючи ефективність використання ресурсів і гнучкість системи.

У військових системах мережецентричність реалізується через концепцію Network-Centric Warfare (NCW), а в цивільних інфраструктурах – в автоматизованих системах управління, великих дата-центрах і хмарних середовищах [4, с. 36–39].

Мережецентричний підхід побудови інформаційної інфраструктури забезпечує високу масштабованість і гнучкість завдяки розподілу обчислювальних потужностей та ресурсів. Оскільки мережа виступає основним елементом, організація може динамічно адаптуватися до змін у навантаженні, оптимізовуючи використання ресурсів на різних рівнях. Такий підхід має підвищену відмовостійкість, оскільки при збоях в одній частині мережі система може автоматично перенаправити трафік на резервні вузли. Це дозволяє забезпечити безперервну роботу критичних додатків та послуг.

Однак мережецентричний підхід має й свої недоліки. Одним з основних є складність управління великою кількістю розподілених мережевих компонентів. Це вимагає високої кваліфікації для адміністрування мережі, а також впровадження складних систем моніторингу та управління, що може бути затратним та трудомістким. Також, велика залежність від мережі може призвести до уразливості в разі мережевих атак чи збоїв у зв'язку. Надмірне навантаження в мережі може спричинити затримки або втрату даних, що погіршує продуктивність. Більш детально переваги і недоліки мережецентричного підходу можна подивитись у таблиці 1.

Мережецентричний підхід підходить для критичної інфраструктури, де надійність і масштабованість є головними параметрами, але він

вимагає ретельного управління і ресурсів для підтримки стабільної роботи.

Таблиця 1

Переваги і недоліки впровадження мереженцентричного підходу

Вимоги	Переваги	Недоліки
Масштабованість	Легке розширення системи завдяки розподіленій мережі	Складність у керуванні великою кількістю елементів мережі
Відмовостійкість	Автоматичне перенаправлення ресурсів трафіку на резервні ресурси	Залежність від стабільності мережі
Продуктивність	Оптимізація мережевих ресурсів та розподіл навантаження	Високі вимоги до моніторингу адміністрування мережі, як результат, завищені витрати і складність
Безпека	Централізоване управління безпекою, при необхідності швидко адаптується до нових загроз	Потенційна уразливість до мережевих атак, які можуть вплинути на всю інфраструктуру

Джерело: розроблено авторами

Мережецентрична архітектура забезпечує ефективну організацію інформаційних систем за рахунок централізованого управління, розподіленої обробки даних та динамічної маршрутизації трафіку. Вона дозволяє масштабувати обчислювальні ресурси, підвищувати продуктивність мережі та забезпечувати її стійкість до збоїв, що є критично важливим для хмарних середовищ, військових систем та IoT. Однак, незважаючи на всі переваги використання, мережецентричний підхід вимагає узгодженості технологічних стандартів та сумісності між різнорідними системами. У цьому контексті ключову роль виконує кросплатформний підхід, який забезпечує інтеграцію різнорідних систем та уніфікацію даних, що дозволяє ефективно взаємодіяти між сервісами незалежно від їх реалізації чи середовища виконання.

Список використаних джерел:

1. AWS, Azure чи GCP: яку хмару вибрати? URL: https://itedu.center/ua/blog/comparisons/aws-azure-chi-gcp-yaku-xmaru-vibrati/?srsltid=AfmBOopqC9keCmhNf5vwG75OcDS_mdh-i7Tpb68libn1jrTGM7kqGOBG (дата звернення: 17.03.2025).

2. Коробейнікова Т. І., Журавель І. М., Бодак А. О., Бороденко Д. В. Концепція нульової довіри: сучасні методи забезпечення кібербезпеки в корпоративних мережах. *Вісник Львівського державного університету безпеки життєдіяльності.* 2024. № 30. С. 67–77.

3. Телешко І. В. Аналіз особливостей основних концепцій побудови віртуальних мереж. *Проблеми інформатизації та управління*. 2019. № 2 (62). С. 70–76.

4. Mendonca M., Astuto B. N., Obraczka K., Turletti T. Software Defined Networking for Heterogeneous Networks. *IEEE MMTC E-Letters*. 2013. Т. 8, № 3. С. 36–39. URL: http://committees.comsoc.org/mmc/e-news/E-Letter-May13.pdf (дата звернення: 17.03.2025).