

Андрощук О. В., кандидат психологічних наук (0000-0002-1032-7459)
Голобородько М. Ю., кандидат технічних наук, старший науковий співробітник (0000-0003-2381-7219)
Кондратенко Ю. В., доктор філософії (0000-0002-9575-5101)
Литовченко Г. Д. (0000-0002-8625-1438)

Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ

Мережецентричність та кросплатформність: інтеграція підходів до побудови інформаційної інфраструктури

Резюме. У статті розглянуто сучасні підходи до побудови інформаційної інфраструктури на основі мережецентричної та кросплатформної архітектури. Проведено аналіз їхніх переваг і недоліків, а також визначено ключові аспекти, що впливають на ефективність використання цих рішень.

Ключові слова: мережецентричність; кросплатформність; хмарні технології; контейнеризація; оркестрація; інформаційні системи; безпека; масштабованість.

Постановка проблеми. У сучасних умовах стрімкого розвитку цифрових технологій організації все частіше впроваджують хмарні рішення для забезпечення гнучкості, масштабованості та безпеки інформаційної інфраструктури. Одним із ключових викликів у цьому контексті є оптимізація мережевих та обчислювальних ресурсів у розподілених середовищах, які охоплюють як датацентричні, так і мультихмарні інфраструктури. У зв'язку з цим зростає інтерес до двох підходів – мережецентричності та кросплатформності, які пропонують альтернативні стратегії вирішення проблем інтеграції та управління інформаційними потоками.

Попри переваги кожного з підходів, їхнє окреме застосування має деякі обмеження. Мережецентричні архітектури централізовані, що створює ризики відмови критичних компонентів, у той час кросплатформні рішення можуть стикатися з проблемами сумісності та продуктивності. Тому доцільним виглядає пошук шляхів поєднання переваг обох концепцій для досягнення балансу між централізованим управлінням та гнучкістю в розгортанні послуг.

Окремою проблемою при впровадженні сучасних архітектур є забезпечення кібербезпеки та дотримання нормативних вимог у розподілених інформаційних системах. Високий рівень взаємодії між компонентами різних платформ потребує єдиних стандартів та ефективних механізмів захисту даних у процесі обміну.

Таким чином, дослідження ролі мережецентричності та кросплатформності у

розвитку хмарних та дата-центричних інфраструктур є актуальним завданням.

Аналіз сучасних досліджень і публікацій. У сучасних дослідженнях активно розглядаються питання впровадження хмарних технологій, їхні переваги та недоліки. У своїй роботі, такі вчені як Батаєв С.В. та Мельник О.С. аналізують підходи до хмарних технологій, акцентуючи увагу на масштабованості, доступності та автоматизації процесів [1]. Водночас, проблеми кібербезпеки в контексті розвитку хмарних середовищ з розвитком штучного інтелекту, створює нові загрози, які можуть використовуватися кіберзлочинцями для нападу на хмарну інфраструктуру, що вимагає посилення заходів захисту та впровадження нових методів безпеки [2].

Огляд існуючих хмарних технологій та їхньої архітектури представлений у роботах, які досліджують особливості розподілених обчислень, роль автоматизації в управлінні великомасштабними інфраструктурами та значення віртуалізації для підвищення ефективності хмарних сервісів [3]. Значна увага також приділяється питанням балансування навантаження та маршрутизації трафіку, після чого саме ці аспекти суттєво впливають на продуктивність хмарних платформ. Дослідники пропонують математичні моделі для оцінки та підвищення продуктивності хмарних обчислень [4].

У науковій літературі окреслено низку сучасних трендів, таких як мультихмарні стратегії, безсерверні обчислення та застосування штучного інтелекту в управлінні IT-інфраструктурами. Ці підходи сприяють цифровій трансформації як приватного, так і

державного секторів, створюючи передумови для гнучкіших та стійкіших інформаційних систем [5].

Попри інтенсивний розвиток хмарних технологій, у більшості робіт недостатньо уваги приділяються питанням взаємодії між мережецентричним та кросплатформним підходами. Саме цей аспект становить дослідницький інтерес даної роботи, яка спрямована на виявлення потенціалу інтеграції зазначених концепцій для побудови ефективної та гнучкої інформаційної інфраструктури.

Метою статті є аналіз мережецентричного та кросплатформного підходів до побудови інформаційної інфраструктури, визначення їх переваг і недоліків, а також оцінка впливу цих підходів на безпеку, масштабованість та управління ресурсами.

Викладення основного матеріалу. У сучасному світі хмарні технології стали основою для побудови ефективних і гнучких інформаційних інфраструктур. Поєднання таких підходів, як мережецентричність та кросплатформність, а також використання мультихмарних та гібридних архітектур, відкриває нові можливості для забезпечення масштабованості, надійності та безпеки, які є ключовими вимогами для побудови єдиного інформаційного простору організації.

Хмарні технології – це модель надання обчислювальних ресурсів (серверів, сховищ, мереж, програмного забезпечення) як сервісів через Інтернет з можливістю масштабування за потреби. Ця модель забезпечує гнучкість, ефективність використання інфраструктури та оптимізацію витрат на ІТ (інформаційні технології), що робить її ключовим компонентом сучасних інформаційних систем.

Хмарні технології стали ключовим елементом сучасної інформаційної інфраструктури, забезпечуючи їхню гнучкість, масштабованість та ефективність. Поєднання мережецентричного підходу, кросплатформності дозволяє організаціям оптимізувати використання ресурсів, підвищити надійність та забезпечити кібербезпеку.

Хмарні технології є ефективним середовищем для зберігання та обробки даних, які використовують власні апаратні ресурси, ліцензійне програмне забезпечення, канали зв'язку та технічну підтримку користувачів [6]. Використання хмарних послуг спрямоване на зменшення витрат і підвищення продуктивності підприємств.

Концепція хмарних обчислень суттєво трансформувала традиційний підхід до управління та інтеграції програмного забезпечення. На відміну від класичної ІТ-інфраструктури, побудованої на фізичних серверах з жорстко закріпленими ресурсами та локальним управлінням, хмарні платформи здатні ефективно керувати значними обчислювальними ресурсами, одночасно обслуговуючи велику кількість користувачів у межах кількох або декількох взаємопов'язаних хмар. Вони забезпечують високу доступність сервісів завдяки механізмам автоматичного масштабування та балансування навантаження. Хоча використання хмарних технологій передбачає певну залежність від постачальника послуг, провайдери змушені приділяти особливу увагу питанням безпеки. Використання хмарних технологій зумовлена низкою переваг, які роблять їх привабливими для користувачів. Основні з них систематизовано в Табл. 1.

Таблиця 1

Переваги використання хмарних технологій

Перевага	Короткий опис
Зручність використання	Не потребує глибоких технічних знань; користувачі працюють із готовими службами провайдера
Оптимізація витрат	Відсутня потреба у витратах на серверне обладнання та програмне забезпечення
Економічна ефективність	Модель оплати "pay-as-you-go": сплата лише за фактично використані ресурси.
Мобільність	Доступ до послуг із будь-якого місця при наявності інтернет-з'єднання
Гнучкість і масштабованість	Можливість динамічно змінювати обсяг ресурсів відповідно до потреби
Продуктивність	Потужні обчислювальні ресурси забезпечують ефективну роботу з великими масивами даних.
Надійність	Провайдери гарантують безперервність роботи сервісів відповідно до рівня обслуговування (SLA).
Безпека	Використання віртуалізації, шифрування та кіберзахисту мінімізує ризики втрати або компрометації даних
Стійкість бізнес-процесів	Архітектури з резервуванням забезпечують стабільність критичних функцій навіть у разі збоїв.

Такі характеристики роблять хмарні технології ключовим компонентом сучасних інформаційної інфраструктури, особливо в контексті масштабних розподілених обчислень та мережецентричних інфраструктур.

Ефективність хмарних технологій значною мірою визначається архітектурними принципами їх побудови. Серед основних підходів, що забезпечують оптимальне функціонування сучасних інформаційної інфраструктури, виділяються мережецентричний та кросплатформний підхід.

Використання мережецентричного та кросплатформного підходів дозволяє оптимізувати управління обчислювальними ресурсами, підвищити рівень автоматизації процесів та забезпечити масштабованість сервісів у розподілених середовищах. З огляду на зростаючі вимоги до адаптивності та ефективності хмарних платформ, інтеграція мережецентричних і кросплатформних підходів стає критично важливою для побудови стійких і продуктивних інфраструктур.

Мережецентричний підхід у хмарних середовищах сприяє централізованому управлінню мережею, оптимізує передачу даних і забезпечує безпеку взаємодії між сервісами. Це особливо актуально для державних і оборонних структур, де критично важливо забезпечити контрольованість інформаційних потоків та високий рівень захисту даних. Кросплатформність, у свою чергу, полегшує інтеграцію різних технологій, забезпечує сумісність між хмарними провайдерами та підтримує гнучкість у виборі інфраструктури. Це дає змогу знизити ризики залежності від конкретного постачальника (vendor lock-in) та адаптувати інформаційні системи до різних сценаріїв використання.

Застосування мережецентричного та кросплатформного підходів у хмарних технологіях дозволяє створити ефективні, безпечні та гнучкі інформаційні системи, здатні відповідати сучасним викликам цифрової трансформації.

Розгляд цих підходів дозволить визначити їх переваги, обмеження та можливості інтеграції в хмарні та датацентричні інфраструктури.

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 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. Вони забезпечують розподіл обчислювальних ресурсів залежно від навантаження, географічного розташування користувачів і бізнес-потреб. 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 інфраструктуру забезпечує високий рівень доступності, масштабованості та надійності зв'язку незалежно від фізичного розташування компонентів [7].

Обробка інформації в мережецентричних інфраструктурах здійснюється на різних рівнях мережі, що зменшує навантаження на центральні сервери та покращує продуктивність системи. Децентралізована обробка даних дозволяє скорочувати затримки, оскільки дані опрацьовуються ближче до місця їх використання.

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, багатфакторна автентифікація (MFA) та концепція ZTA (Zero Trust Architecture), що мінімізує ризики несанкціонованого доступу та атак на рівні мережі [8].

Мережецентрична інфраструктура (NCI) забезпечує ефективну організацію інформаційної інфраструктури, 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 (Internet of Things) та розподілених дата-центрів.

Довідка. Інтернет речей (IoT, Internet of Things) – це концепція обчислювальної мережі, яка передбачає об'єднання фізичних об'єктів, пристроїв, сенсорів і систем в єдину інфраструктуру, що дозволяє їм створювати, обмінюватися та обробляти дані через Інтернет без участі людини. Основною метою IoT є забезпечення автоматизації, адаптивного управління та оперативного моніторингу у сфері промисловості, транспорту, енергетики, охорони здоров'я, “розумного дому” та військових систем. IoT-системи функціонують на перетині хмарних технологій, мережевої інфраструктури, обчислювальних платформ і штучного інтелекту, що робить їх критично важливими для сучасних інформаційних інфраструктур.

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 [9].

Спочатку SDN розроблялася для центрів обробки даних (ЦОД), де централізоване управління є ключовим фактором ефективності. Однак її впровадження в децентралізованих безпроводних “ad hoc” і “mesh”-мережах створює проблеми в сферах безпеки, балансування навантаження та управління мережею, що потребує подальших досліджень і вдосконалення механізмів взаємодії між комутаторами та контролерами.

Ad hoc і mesh – це типи бездротових мереж, які працюють без централізованої

інфраструктури. Ad hoc-мережа – це тимчасова мережа, у якій пристрої напряду з'єднуються один з одним без маршрутизатора чи точки доступу. Кожен пристрій виконує роль і клієнта, і маршрутизатора. Такі мережі швидко створюються і зазвичай застосовуються в екстрених ситуаціях або для локального обміну даними. Mesh-мережа (сітчаста мережа) більш стійка і масштабована структура, де всі вузли (пристрої) рівноправні й з'єднані між собою. Інформація може передаватися через кілька вузлів, що забезпечує надійність і автоматичне перенаправлення трафіку при виході з ладу частини мережі. Обидва типи мереж особливо актуальні в умовах обмеженого доступу до інфраструктури – наприклад, у військових або польових умовах.

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 [10].

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, оптимізуючи 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 потребує високої кваліфікації персоналу 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 наведені у Табл. 2.

Таблиця 2

Переваги і недоліки впровадження мережецентричного 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

Ефективність мережецентричної архітектури залежить від здатності балансувати переваги централізації з потенційними ризиками.

Мережецентричний підхід ідеально підходить для масштабованих, дистрибуційних середовищ, але потребує збалансованості з іншими підходами для оптимізації. Системи мають бути спроектовані таким чином, щоб забезпечити надійність і безпеку, враховуючи які ризики мережевих атак і збоїв. Мережецентричний підхід підходить для критичної інфраструктури, де надійність і масштабованість є головними параметрами, але він потребує ретельного управління і ресурсів для підтримки стабільної роботи.

Мережецентрична архітектура забезпечує ефективну організацію інформаційної інфраструктури 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 потребує 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.

Кросплатформність (Cross-Platform) – це здатність програмного забезпечення, апаратних систем або мережевих компонент функціонувати на різних операційних системах, пристроях або технологічних середовищах без втрати продуктивності та функціональності. *Кросплатформність* – властивість програмного забезпечення працювати більш ніж на одній програмній або апаратній платформі; технології, що дозволяють досягти такої властивості. Кросплатформність дозволяє суттєво скоротити витрати на розробку нового або адаптацію існуючого програмного забезпечення [11]. Кросплатформність у мережевих та хмарних інфраструктурах забезпечує інтеграцію різних сервісів незалежно від їхнього середовища виконання, що є критичним для мультихмарних архітектур (AWS, Azure, GCP). У військовій сфері концепція хмарних обчислень реалізується через такі системи, як SitaWare Headquarters (система оперативного управління для планування та моніторингу бойових дій), JADC2 (Joint All-Domain Command and Control – концепція об'єднаного багатодоменного управління та зв'язку, яка інтегрує всі рівні Збройних сил США в єдину інформаційну мережу), а також IVAS (Integrated Visual Augmentation System – інтегрована система доповненої реальності для підвищення ситуаційної обізнаності солдатів). Ці рішення сприяють координації операцій, обміну даними в реальному часі та

взаємодії між розрізненими інформаційними системами. [12].

До ключових технологій кросплатформного підходу належать API, контейнеризація та віртуалізація. API стандартизує взаємодію між застосунками та сервісами, забезпечуючи узгоджену комунікацію без залежності від конкретної реалізації. Інтерфейси можуть бути реалізовані у вигляді веб-сервісів, зокрема REST (Representational State Transfer – архітектурний стиль для створення масштабованих мережових сервісів на основі протоколу HTTP) або SOAP (Simple Object Access Protocol – протокол обміну структурованими повідомленнями на основі XML). Це створює можливості для узгодженої взаємодії між різними програмними платформами та середовищами в рамках спільної інформаційної інфраструктури [13].

Контейнеризація забезпечує ізоляцію застосунків у компактних середовищах (контейнерах), які використовують спільне ядро операційної системи, що підвищує ефективність використання ресурсів та забезпечує портативність. Це мінімізує витрати, прискорює розгортання та спрощує управління розподіленими системами, зокрема завдяки інструментам оркестрації, таким як *Kubernetes*.

Оркестрація – це програмна технологія для автоматичного керування контейнерами. А самі контейнери є середовищами для виконання ізольованих процесів, файли для запуску яких знаходяться в одному образі. Контейнери не пов'язані з апаратною частиною обладнання, тому їх легко переносити між фізичними машинами, хмарами та операційними системами [14].

Kubernetes та технологія контейнеризації тісно пов'язані із сучасними практиками розроблення та розгортання програмного забезпечення. Контейнеризація забезпечує пакування застосунку разом з усіма необхідними залежностями у відокремлене середовище, що дозволяє запускати його на будь-якій інфраструктурі без модифікації коду. Це спрощує тестування, масштабування та обслуговування застосунків. *Kubernetes* – це система оркестрації контейнерів, яка автоматизує їх розгортання, масштабування та управління. Вона підтримує різні середовища виконання контейнерів (container runtimes), зокрема Docker, containerd, CRI-O, які відповідають специфікації CRI (Container Runtime

Interface) – стандартного інтерфейсу для взаємодії між *Kubernetes* і середовищами виконання контейнерів [15].

Віртуалізація дозволяє створювати віртуальні машини (VM), кожна з яких має власну операційну систему та працює незалежно від інших. Це забезпечує високий рівень ізоляції, підвищує безпеку та ефективно розподіляє обчислювальні ресурси через гіпервізор. Вона широко використовується в хмарних інфраструктурах і дата-центрах, оптимізуючи використання апаратних ресурсів та спрощуючи управління середовищем.

Основна відмінність між віртуалізацією та контейнеризацією полягає в рівні ізоляції: контейнери працюють у межах спільного ядра ОС, тоді як віртуальні машини мають власні операційні системи. Завдяки поєднанню API, контейнеризації та віртуалізації можна створювати гнучкі та масштабовані технології, які ефективно працюють у мультихмарних і гібридних інфраструктурах.

Кросплатформність дає змогу створювати додатки та сервіси, які можуть працювати на різних платформах, незалежно від операційної системи або апаратного забезпечення. Це знижує витрати на розробку, оскільки один і той самий код може бути використаний для різних середовищ (Windows, Linux, macOS, мобільні платформи). Крім того, це забезпечує гнучкість при виборі технологічних підходів, що дозволяє організаціям швидко адаптуватися до нових умов і вимог. Кросплатформність також підвищує доступність програм, забезпечуючи підтримку ширшого кола користувачів і пристроїв.

Незважаючи на численні переваги, кросплатформність має і свої недоліки. Перш за все, універсальні рішення можуть бути менш ефективними порівняно з програмами, розробленими спеціально для однієї платформи. Це пов'язано з необхідністю підтримки сумісності між різними операційними системами та пристроями. Важливою проблемою є також обмеження в функціональності: деякі специфічні можливості платформи можуть бути недоступними через використання кросплатформних інструментів. Також, у разі значних змін в одній із платформ, розробникам може знадобитися оновлення чи адаптація коду для забезпечення сумісності. Більш детально переваги і недоліки кросплатформного підходу наведені у Табл. 3.

Таблиця 3

Переваги і недоліки впровадження кросплатформного підходу

Вимоги	Переваги	Недоліки
Гнучкість	Зменшення витрат на розроблення за рахунок запуску на різних операційних системах	Постійні оновлення і адаптації коду для підтримки на нових версіях платформ
Продуктивність	Оптимізація витрат на розроблення та підтримку коду за рахунок універсального коду для всіх платформ	Універсальний код може бути менш ефективним відносно з оптимізованим для конкретної платформи
Покриття	Доступність додатків для усіх користувачів на усіх видах пристроїв	Обмеження в доступі до спеціальних можливостей і функціоналу окремих платформ
Адаптивність	Легкість адаптації до нових платформ	Специфічні вимоги дуже складно реалізувати під конкретні платформи

Кросплатформність є ідеальним рішенням для організацій, які потребують швидкого виходу на різні платформи з мінімальними витратами, але вона не завжди підходить для розв'язання складних технічних завдань, що потребують високої продуктивності або особливу функціональність. Слід ретельно обирати підхід для кожного конкретного випадку, враховуючи обмеження та специфіку використовуваних платформ. Використання таких інструментів, як Docker, Kubernetes, або використання кросплатформних фреймворків може значно полегшити задачу забезпечення сумісності та підтримки різних середовищ.

Отже, зважаючи на зазначене мережецентричний підхід створює інформаційну інфраструктуру навколо мережних зв'язків, забезпечуючи централізоване управління та ефективний розподіл ресурсів. Така архітектура дає змогу мінімізувати затримки запиту, покращити безпеку передачі даних і підвищити надійність системи. Водночас мережецентричні рішення потребують значних інвестицій у розвиток мережевої інфраструктури та впровадження програмно-орієнтованих технологій, таких як SDN (Software-Defined Networking) та NFV (Network Functions Virtualization).

Кросплатформність забезпечує створення уніфікованих сервісів, які можуть функціонувати в різних хмарних середовищах та апаратних платформах. Завдяки використанню API, контейнеризації (Docker, Kubernetes) та технологій віртуалізації забезпечується взаємодія між сервісами та провайдерами. Це знижує залежність від конкретних постачальників хмарних послуг (vendor lock-in) і підвищує гнучкість у розподілі обчислювальних ресурсів.

Висновок. Аналіз особливостей мережецентричного та кросплатформного підходів до побудови інформаційної

інфраструктури показав доцільність їх інтегрованого застосування в умовах цифрової трансформації.

Мережецентричний підхід забезпечує централізоване управління, високу масштабованість та відмовостійкість, що робить його ефективним для побудови великих корпоративних, державних і оборонних інформаційних систем. Його ключовими перевагами є оптимізація мережних ресурсів, надійна координація компонентів та розподілена обробка даних із дотриманням вимог безпеки.

Кросплатформність, натомість, сприяє гнучкій інтеграції розрізнених сервісів, уніфікації інтерфейсів і забезпеченню сумісності між різними технологічними платформами. Це дозволяє знизити залежність від конкретного провайдера, зменшити витрати на розробку та обслуговування, а також підвищити адаптивність до динамічних змін середовища.

Отже, комбіноване застосування мережецентричного та кросплатформного підходів створює передумови для формування стійкої, масштабованої та безпечної інформаційної інфраструктури. Такий підхід є доцільним для застосування в критичних сферах, зокрема в обороні, державному управлінні та системах національної безпеки.

У подальших дослідженнях планується зосередити увагу на практичному обґрунтуванні доцільності використання мережецентричного та кросплатформного підходів, а також їх варіативних поєднань, для побудови Єдиного інформаційного простору Міністерства оборони України. Особливий акцент буде зроблено на гібридних і мультимарних архітектурах як стратегічному напрямі розширення функціональності сучасних мережецентричних систем із урахуванням вимог до безпеки,

масштабованості та стійкості критично важливої інформаційної інфраструктури.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Батаєв С. В., Мельник О. С. Принципи роботи хмарних рішень. URL: https://www.tech.vernadskyjournals.in.ua/journals/2024/3_2024/part_1/8.pdf (дата звернення: 10.02.2025).
2. Проблеми кібербезпеки в хмарних середовищах. URL: <https://archive.mcmd.org.ua/index.php/conference-proceeding/article/download/660/670> (дата звернення: 10.02.2025).
3. Огляд хмарних технологій та їхня архітектура. URL: https://www.tech.vernadskyjournals.in.ua/journals/2024/3_2024/part_1/8.pdf (дата звернення: 10.02.2025).
4. Балансування навантаження та маршрутизація трафіку у хмарних середовищах. URL: <https://csecurity.kubg.edu.ua/index.php/journal/article/view/717/579> (дата звернення: 11.02.2025).
5. 7 трендів розвитку хмарних технологій. URL: <https://gigacloud.ua/articles/7-trendiv-hmarnyh-tehnologij> (дата звернення: 11.02.2025).
6. Хмарні технології. URL: https://uk.wikipedia.org/wiki/Хмарні_технології (дата звернення: 11.02.2025).
7. AWS, Azure чи GCP: яку хмару вибрати? URL: https://itedu.center.ua/blog/comparisons/aws-azure-chi-gcp-yaku-xmaru-vibrati/?srsltid=AfmBOopqC9keCmhNf5vwG75OcsDS_mdh-i7Tpb68libn1jrTGM7kqGOBG (дата звернення: 12.02.2025).
8. Коробейнікова Т. І., Журавель І. М., Бодак А. О., Борошенко Д. В. Концепція нульової довіри: сучасні методи забезпечення кібербезпеки в корпоративних мережах // Вісник ЛДУБЖД. 2024. № 30. С. 67–77.
9. Телешко І. В. Аналіз особливостей основних концепцій побудови віртуальних мереж // Проблеми інформатизації та управління. 2019. № 2 (62). С. 70–76.
10. Mendonca M., Astuto B. N., Obraczka K., Turlatti T. Software Defined Networking for Heterogeneous Networks // IEEE MMTC E-Letters. 2013. Vol. 8, No. 3. С. 36–39. URL: <http://committees.comsoc.org/mmte/e-news/E-Letter-May13.pdf> (дата звернення: 12.02.2025).
11. Багатоплатформність // Вікіпедія. URL: <https://uk.wikipedia.org/wiki/Багатоплатформність> (дата звернення: 12.02.2025).
12. Why (and when) you should use Kubernetes. URL: <https://hackernoon.com/why-and-when-you-should-use-kubernetes8b50915d97d8> (дата звернення: 13.02.2025).
13. Kubernetes vs. Docker: A Primer. URL: <https://blog.colobridge.net/uk/2023/12/kubernetes-what-is-it-ua/> (дата звернення: 13.02.2025).
14. Kubernetes vs. Docker: A Primer. URL: <https://aws.amazon.com/ru/compare/the-difference-between-kubernetes-and-docker/> (дата звернення: 13.02.2025).
15. Kubernetes: що це таке? URL: <https://blog.colobridge.net/uk/2023/12/kubernetes-what-is-it-ua/> (дата звернення: 13.02.2025).

Стаття надійшла до редакційної колегії 17.03.2025

Network-centricity and cross-platform: integration of approaches to building information infrastructure

Annotation

In the context of rapid advancements in digital technologies, organizations are increasingly adopting cloud solutions to ensure flexibility, scalability, and security of their information infrastructure. One of the key challenges in this domain is the optimization of network and computational resources in distributed environments, encompassing both data-centric and multi-cloud infrastructures. Consequently, there is growing interest in two approaches – network-centric and cross-platform – which offer alternative strategies for addressing challenges related to integration and management of information flows.

The purpose of this article is to analyze network-centric and cross-platform approaches to building information infrastructure, identify their advantages and disadvantages, and evaluate their impact on security, scalability, and resource management.

The analysis of the characteristics of network-centric and cross-platform approaches demonstrates the feasibility of their integrated application in the context of digital transformation. The network-centric approach provides centralized management, high scalability, and fault tolerance, making it effective for developing large-scale corporate, governmental, and defense information systems. Its key advantages include optimization of network resources, reliable coordination of components, and distributed data processing while adhering to security requirements.

In contrast, cross-platform approach facilitates flexible integration of disparate services, unification of interfaces, and compatibility across diverse technological platforms. This reduces dependency on specific vendors, lowers development and maintenance costs, and enhances adaptability to dynamic environmental changes.

Keywords: network-centricity; cross-platform; cloud technologies; containerization; orchestration; information systems; security; scalability.