

**Гіоргізова-Гай В.Ш.**

Національний технічний університет України  
«Київський політехнічний інститут імені Ігоря Сікорського»

**Кирюша Б.А.**

Національний технічний університет України  
«Київський політехнічний інститут імені Ігоря Сікорського»

## ХМАРНІ ПОСЛУГИ В КОРПОРАТИВНІЙ ІНФРАСТРУКТУРІ

*У статті проводиться аналіз звітів від всесвітньо відомих організацій та компаній про стан ринку застосування хмарних технологій, аналіз пропозицій світових та регіональних сервіс-провайдерів, які пропонують послуги в Україні. На основі цього аналізу надається порівняння можливостей, переваг та обмежень різних хмарних підходів до побудови сучасної корпоративної інфраструктури організацій, розглядаються проблеми впровадження приватних, гібридних і мультихмарних технологій та шляхи подолання цих проблем. Сучасні компанії поширюють застосування хмарних технологій для отримання конкурентних переваг на ринку. Досвід тривалого використання публічних хмар виявив ряд їх недоліків: обмеженість безпеки та контролю, складність з дотриманням нормативних вимог, високі затримки, обмеженість налаштувань, залежність від провайдера та неконтрольовані зростання витрат. А при побудові хмар власними силами на локальних ресурсах організації зіткнулися з нестачею кваліфікованих кадрів для її підтримки, з проблемами обмежень наявної інфраструктури та зі зростанням витрат на обслуговування. Як відповідь на ці виклики світовими та регіональними сервіс-провайдерами були запропоновані послуги по розгортанню приватних хмар в ізольованому середовищі на орендованій або локальній інфраструктурі замовників та гібридних хмар, які дозволяють поєднати переваги приватних і публічних хмар, щоб досягти балансу між гнучкістю, контролем та інноваціями. Впровадження цих хмарних стратегій змінює підходи до побудови корпоративної інфраструктури і стає все більш популярним з року в рік. Але впровадження цих підходів поряд з перевагами також може спричинити компаніям чимало проблем. Проте, проблеми можна подолати, якщо організація добре усвідомлює особливості різних хмарних підходів, має продуману стратегію і архітектурне рішення для розгортання хмари, а також досвідчених партнерів. Дана стаття спрямована на те, щоб допомогти організаціям, які шукають нові рішення для успішності свого бізнесу, зробити правильний вибір.*

**Ключові слова:** хмарні технології, корпоративна інфраструктура, безпека даних, публічна хмара, приватна хмара, гібридна хмара.

**Постановка проблеми.** Хмарні послуги міцно увійшли в наше життя і знаходять широке застосування в корпоративній інфраструктурі організацій. Проте застосування організаціями послуг, пов'язаних з багатохмарним підходом, як у світі, так і в Україні почало поширюватись відносно недавно. Закону України «Про хмарні послуги» [1] був прийнятий тільки у 2022 році. Організації ще не в повному обсязі усвідомлюють, як забезпечити максимальну ефективність від використання різних хмарних послуг, їх переваги і обмеження та шляхи уникнення можливих проблем. В пропозиціях провайдерів можна зустріти різні підходи до реалізації приватних та гібридних хмар та навіть дещо відмінну термінологію. Все це ускладнює вибір організацій, які шукають нові рішення.

**Аналіз останніх досліджень і публікацій.** Хмарні технології сьогодні займають важливе

місце в ІТ галузі, тому актуальний стан ринку їх застосування регулярно аналізується у звітах всесвітньо відомих організацій та компаній таких, як CNCF, Flexera, Mordor Intelligence та ін. [2–5], чий постійні опитування охоплюють сотні підприємств з усього світу.

Всі звіти демонструють постійне зростання використання хмарних проектів у виробництві в опитуваних організаціях незалежно від їх розміру. Організації переходять на хмарні технології через їх масштабованість, економічність, високу доступність і широке охоплення, більш швидке розгортання та підвищення продуктивності праці розробників.

В той же час, серед головних проблем застосування хмарних технологій залишається управління витратами та безпека даних. За даними Flexera управління витратами на хмару вже дру-

гий рік поспіль займає перше місце (як головну проблему її визначили 84% організацій) і випереджає проблеми безпеки (81%).

Серед інших проблем, як і в попередні роки, респонденти відзначають брак ресурсів/експертів, проблеми з урядовими дозволами та погодженнями, з управлінням ліцензіями на ПЗ, з балансом відповідальності між центральною хмарною командою та корпоративною, з управлінням мультихмарою та міграцією в хмару.

Використання публічних хмар продовжує зростати. Провайдери всіх рівнів постійно розширюють набір пропонованих послуг та вдосконалюють існуючі. Проте проблеми і обмеження самого підходу залишаються. Для їх подолання пропонуються інші хмарні стратегії: приватна, багато хмарна та гібридна. Їх впровадження змінює підходи до побудови корпоративної інфраструктури.

Сьогодні в світі стратегія, при якій на підприємствах одночасно використовуються послуги декількох хмар одночасно стала вже нормою. Гнучкість цієї моделі дозволяє організаціям скористатися перевагами різних видів хмар, зменшити ризики, забезпечити масштабованість і оптимізацію ресурсів.

Так, за даними звіту Flexera 2024 року тільки 10% опитаних організацій задовольнялись послугами одного публічного провайдера і лише 1% – тільки власною мережевою інфраструктурою, а 89% застосовували багато хмарні рішення, з яких 73% склали гібридні хмари, 14% – з використанням кількох публічних без приватних та 2% – з використанням кількох приватних без публічних.

В термінології щодо видів розгортання хмарних послуг будемо орієнтуватись на визначення всесвітніх організацій і провідних провайдерів.

**Публічна хмара.** Загальнодоступні хмари є стандартним способом розгортання хмарних обчислень (cloud computing) [6]. У загальнодоступній хмарі обчислювальні ресурси, сховища даних, програмне забезпечення та мережева інфраструктура знаходяться у володінні та управлінні постачальника хмарних служб. Користувачі керують лише основними параметрами послуг. Провайдер відповідає за обслуговування ресурсів та гарантує доступність, надійність та безпеку за допомогою угод про рівень обслуговування SLA (Service Level Agreement).

Послуги надаються великій кількості незалежних користувачів на вимогу у міру потреби через Інтернет. В основі хмарного підходу лежить

віртуалізація загальнодоступних ресурсів, які динамічно перерозподіляються між споживачами в умовах постійної зміни запиту на потужності, чим забезпечується швидке автоматичне масштабування обчислювальної системи. Ресурси можуть бути розміщені в одному або декількох дата-центрах. Служби надаються постачальником на основі трьох базових моделей: IaaS, (Infrastructure-as-a-Service) – інфраструктура як послуга, PaaS (Platform-as-a-Service) – платформа як послуга та SaaS (Software-as-a-Service) – програмне забезпечення як послуга.

**Приватна хмара.** Приватна хмара створюється тільки для потреб однієї організації і використовується тільки нею. Інфраструктуру приватної хмари можна побудувати на базі локальних ресурсів підприємства чи орендувати у спеціалізованих постачальників хмарних послуг (або їх комбінації).

**Віртуальна приватна хмара.** Послуга Virtual Private Cloud (VPC) з'явилась не так давно. Проте це послуга публічної хмари. Вона дозволяє розгорнути програмно-ізольовану мережеву інфраструктуру на загальнодоступних обчислювальних ресурсах провайдера (наприклад, в хмарі AWS [7]). В порівнянні з IaaS послуга VPC пропонує клієнту побудувати програмним способом мережу традиційного вигляду з віртуальними комутуючими пристроями, серверами, ПЗ та самостійно налаштувати звичні засоби контролю та безпеки даних.

**Мультихмара.** Хоча цей термін не є загальноприйнятим, проте ця стратегія розгортання сьогодні не є рідкісною, і варто того, щоб бути окремо виділеною. Мультихмарним будемо називати підхід, при якому організація використовує не інтегровані послуги кількох публічних хмар без приватних або в доволі рідких випадках – кількох приватних хмар без публічних.

Стратегію роботи з кількома публічними хмарами підприємства можуть вибирати з різних причин. Наприклад, потреба в розміщенні даних і доступу до ресурсів у різних регіонах, забезпечення безперервності роботи бізнесу (уникнення потенційного ризику блокування постачальника, аварійне відновлення/перемикання при відмові). Також різні хмари можуть застосовуватися для різних завдань бізнесу, оскільки зазвичай один постачальник не може бути універсальним рішенням для всіх потреб.

**Гібридна хмара.** Ця стратегія розгортання передбачає комбінацію з двох або більше різних хмарних інфраструктур (приватних, публічних). На відміну від моделі з кількома публічними хма-

рами, які використовуються паралельно, гібридна модель пропонує інтегровану мережу, що включає приватну, публічну хмару та локальну інфраструктуру в різних комбінаціях. При цьому створюється сегментована, але єдина загальна мережева інфраструктура. В гібридній інфраструктурі забезпечується можливість спільного розміщення, управління та надання послуг, а також уніфікований моніторинг та управління. Як наслідок, зберігання даних та запуск програм може відбуватись прозоро в різних середовищах, наприклад, приватні хмарні програми можуть звертатися до ресурсів публічної хмари під час тимчасових сплесків трафіку.

**Постановка завдання.** Метою статті є порівнянню можливостей, переваг та обмежень різних хмарних підходів до побудови сучасної корпоративної інфраструктури, аналіз проблем впровадження цих підходів та шляхів їх подолання.

**Виклад основного матеріалу.** До переваг класичних публічних хмарних сервісів належать:

- Масштабування за потребами.
- Оплата в міру використання ресурсів та відсутність потреби у підтримці власної інфраструктури.
- Широкий спектр послуг.
- Постійний доступ до інновацій та оновлень.
- Висока доступність та надійність.

Публічні сервіси в компаніях застосовують у різних сценаріях, але найпопулярнішими серед них є вирішення завдань аналітики, розширення інфраструктурних можливостей, а також завдання штучного інтелекту та машинного навчання. Коли для компанії важливими є простота використання, швидкість розгортання сервісів без витрат на підтримку власної платформи і оплата в міру використання ресурсів, модель публічної хмари є кращою. Поширений приклад – середовища тестування чи розробки.

Однак досвід тривалого використання публічних хмар виявив ряд їх недоліків:

- Обмеженість безпеки та контролю.
- Складність з дотриманням нормативних вимог та стандартів безпеки та конфіденційності.
- Залежність від Інтернету.
- Обмеженість налаштувань.
- Залежність від провайдера.
- Неконтрольовані зростання витрат.

В першу чергу з цими проблемами зіткнулись державні органи, фінансові установи та іншими організації з важливими для бізнесу операціями, які потребували вищого рівня контролю над своїм середовищем.

А побудова приватних хмар власними силами організацій зіткнулася з проблемами обмежень наявної інфраструктури, нестачею кваліфікованих кадрів для операційної підтримки та зростанням витрат на обслуговування. Локальна хмара вимагає великих початкових інвестицій та поточних витрат, необхідності забезпечувати її безпеку, обслуговування, модернізацію, підтримку та управління ресурсами приватної хмари.

Як відповідь на ці виклики з'явилися послуги від хмарних провайдерів по побудові приватних і гібридних хмар для клієнтів, які пропонують сьогодні як хмарні гіганти AWS, Microsoft Azure, Google Cloud Platform та інші, так і численні регіональні та локальні постачальники хмарних послуг. Наприклад, в Україні послуги приватної хмари пропонують компанії: Denovo, onecloudplanet, Gigacloud, Colobridge, Ucloud [8–12].

Але будь-які переваги приватної хмарної інфраструктури залежать від її реалізації та мають багато відмінностей, які варто розглянути детальніше.

#### *Послуги приватних хмар*

Регіональні та локальні постачальники хмарних послуг зазвичай пропонують варіанти рішень, реалізованих в їх публічних хмарах, але адаптовані під вимоги клієнта та налаштовані на відокремлених фізичних ресурсах (власних або клієнта). Це можуть бути, моделі хмарних служб типу IaaS та PaaS (наприклад, KaaS, Kubernetes-as-a-Service). Але на відміну від публічної хмари IaaS/PaaS у приватній хмарі обчислювальні ресурси не розподіляються між замовниками, а виділяються для єдиного замовника, утворюючи і фізично і програмно ізольоване середовище.

При створенні приватної хмари можуть варіюватись моделі розподілу обов'язків з її обслуговування, які розрізняються вартістю, зручністю, ступенем відповідальності та контролю, що беруть на себе постачальник і організація. Якщо клієнт орендує всі компоненти інфраструктури (сервери, порти необхідного типу та ємності, IP-адреси, сховища даних та ліцензії), то в зону відповідальності провайдера входить забезпечення працездатності цих компонентів, їх заміна в терміни, обумовлені в SLA, закупівля та розширення ресурсів на вимогу замовника. За обслуговування компонентів власної інфраструктури замовник відповідає самостійно.

Обов'язки з управління та обслуговування програмними компонентами хмари можуть також розподілятися між сторонами від повної відповідальності замовника за управління системою віртуалізації та її компонентами (налаштування,

оновлення та моніторинг всіх хмарних служб, керування віртуальними машинами, контроль виділення ресурсів та адмініструванням операційних систем) до мінімальної, коли замовник керує лише операційними системами віртуальних машин.

Причини і умови для застосування компаніями приватних хмар.

**Безпека даних.** Завдяки більшому контролю та високому рівню безпеки, приватні хмарні сервіси допомагають знизити ризики, пов'язані з компрометацією даних, включаючи їх розкриття та витік, атаками та іншими подіями, які можуть вплинути на бізнес.

Наприклад, відповідно до щорічного звіту Identity Theft Resource Center (ITRC) про витік даних за 2023 рік кількість випадків компрометації даних у США збільшилася на 78% (3205) порівняно з 2022 роком (1801) та на 72% за попередній рекордний максимум у 2021 році (1860) [13].

Приватні хмари часто вибирають організації, яким необхідно забезпечити відповідність своїх методів хмарних обчислень законам про конфіденційність даних та галузевим стандартам, нормативним корпоративним вимогам або вимогам до збереження даних в певній географії. До них відносяться урядові, військові, фінансові установи та інші організації, які мають чутливі для бізнесу дані.

Вибір площадки для розгортання хмари (власна чи провайдера) залежить від конкретних вимог організації. Приватні хмарні послуги надаються в ізольованому середовищі, до якого мають доступ лише уповноважені користувачі. Проте критично важливі для бізнесу операції вимагають посиленого контролю над середовищем на власній інфраструктурі, оскільки до інфраструктури в дата центрі (ЦОД) провайдера в принципі можуть отримати несанкціонований доступ його співробітники. Для додаткового захисту локальних даних корпоративний IT-відділ може налаштувати інструменти керування ідентифікацією та доступом (IAM) та захисту периметру безпеки для додаткового захисту локальних даних.

Рівень безпеки даних користувачів в дата центрах провайдерів розрізняється і залежать від конкретного постачальника послуг. Хоча сертифіковані провайдери можуть забезпечити високі стандарти безпеки, організація все одно несе відповідальність за контроль доступу до ресурсів, хмарну безпеку та шифрування даних (всі конфіденційні дані в публічній хмарі повинні шифруватися), а також за надійність зберігання даних.

Наприклад, в травні 2024 року крупний інцидент стався на платформі Google Cloud, в резуль-

таті якого зникли дані більш ніж півмільйона користувачів приватного пенсійного фонду. Через неправильне налаштування провайдера хмарний обліковий запис захищеної приватної хмари, розміщеної відразу на двох майданчиках, було видалено. Ситуацію частково врятував бекап в іншого провайдера [14].

**Контроль.** Організації мають повний контроль над своїми даними, додатками та інфраструктурою для адміністрування на апаратному рівні та на рівні гіпервізора. Це дозволяє оперативно виявляти на реагувати на проблеми у додатках, використовувати аналітику для прогнозування простоїв та вибирати найкращі політики для контролю доступу.

**Гнучкість налаштування і задоволення специфічних вимог.** Публічні дата центри обмежують можливості вибору типів віртуальних обчислювальних вузлів та не дозволяють їх ручного налаштування.

Тоді як певні додатки можуть мати специфічні вимогами до ресурсів, наприклад, певна частота процесора чи кількість ядер на одну віртуальну машину, модель графічного процесору чи вимоги до системи зберігання даних. Деякі компанії орієнтуються на обладнання конкретного вендора за вимогами якості, надійності та рівня гарантійного обслуговування.

Організація може очікувати певної продуктивності роботи серверів чи системи зберігання даних, наприклад, для додатків із високим постійним навантаженням. Приватна хмара на відміну від публічної може забезпечити на виділених ресурсах ізоляцію від впливу інших користувачів.

Якщо потрібна максимальна швидкість додатку, то зберігання змінних його стану в пам'яті або на диску виділеного сервера з традиційним налаштуванням буде набагато ефективніше, ніж побудова додатку в публічній хмарі із залученням ВааS сервісів баз даних.

Приватна хмара дає змогу реалізувати проекти з обладнанням будь-якої конфігурації від будь-якого виробника, а контроль над інфраструктурою на апаратному рівні та на рівні гіпервізора дозволяє точно налаштувати ресурси та керувати ними відповідно до конкретних вимог і задач компанії.

Але, якщо певні види робіт організації з додатками вимагають мінімально можливої затримки та відсутності залежності від Інтернет, то скоротити час звернення до IT-ресурсів до абсолютного мінімуму можна, зберігаючи їх в локальному центрі обробки даних. Також при побудові систем



Інтернету речей стратегія прикордонних обчислень є домінуючим підходом, який дозволяє підвищити автономність системи, час її відгуку та знизити накладні витрати на взаємодію з хмарним сервером.

Незалежність від провайдера. Публічні хмарні сервіс-провайдери зазвичай пропонують зручні власні рішення, які спрощують використання, управління та обслуговування певних технологій, оскільки весь технологічний стек інтегрований та сумісний між собою. Це дозволяє користувачам економити час і ресурси на навчання та підтримку різних технологій.

Проте, залежність від одного постачальника послуг публічної чи приватної хмари може обмежити гнучкість і призвести до більш високих витрат у довгостроковій перспективі. Не виключено, що сам постачальник може зіткнутися з проблемами у своїй діяльності. Він може підвищувати ціни або змінювати умови контракту. Його пропозиції можуть перестати відповідати потребам компанії, обмежити її у виборі нових технологій та інновацій, нових пропозицій ринку. Відсутність можливості легко перейти до іншого постачальника без високих витрат, юридичних обмежень чи технічної несумісності може створити серйозні ризики для бізнесу.

Власна приватна хмара на локальних ресурсах повністю позбавляє залежності від сервіс-провайдерів. Однак, її недоліками є висока вартість та складність обслуговування і обмежена гнучкість. Проте, запобігти прив'язки до одного постачальника можна і при використанні послуг публічних та приватних хмар провайдерів. Умовами для цього є побудова продуктів компанії на основі відкритих стандартів. Це дозволить легко переключатися між різними постачальниками, використовувати відкриті API та інтегруватися з іншими системами. А для приватної IaaS/PaaS хмари варто обирати або відкриті хмарні стеки (наприклад, OpenStack та Kubernetes), або ті комерційні стеки, що поширені серед різних провайдерів (наприклад, стек VMware, або продукти на базі MS Hyper-V).

Економія витрат. На початковому етапі використання перевагами публічних хмарних є економія коштів на власній інфраструктурі та обслуговуючому персоналі. Однак, із збільшенням використання витрати на хмарні послуги поступово зростають, і більшості організацій, особливо великих, важко утримати ці витрати під контролем.

Приватні хмари вимагають більше вкладень на початкових етапах, але з часом можуть бути вигіднішими, ніж публічні хмари з оплатою в міру використання. Розвивати приватну хмару

вигідніше, якщо бізнес-процеси компанії створюють відносно рівномірне постійне навантаження ресурсів.

Варто також зазначити, що використання публічних хмар не відмінює повністю операційних дій з боку компанії, хоча і дозволяє зменшити розмір і кваліфікаційні вимоги до ІТ-команди. Між тим, високі витрати приватної хмари на ІТ-команду також можна зменшити, делегуючи частину рутинних робіт по налаштуванню та обслуговуванню постачальнику цієї послуги.

Приватна хмара може зменшити витрати на переміщення даних, а популярні сьогодні моделі штучного інтелекту в ній можуть бути меншими і швидшими залежно від варіанту використання, отже споживати менше ресурсів.

За даними опитувань найбільшої економії та ефективності витрат для приватних хмар організації досягають за допомогою автоматизації, інструментів планування потужності, гнучких ліцензійних механізмів, регулярної перевірки контрактів з постачальниками на відповідність актуальним потребам та інструментів управління витратами та бюджетом. В добре спланованих під задачі організації і робочі навантаження (додатки, служби та ресурси), автоматизованих та інструментованих мережах можна досягти ефективного використання коштів.

Таким чином, перевагами приватних хмар є:

- Можливість забезпечити рівень безпеки даних, що відповідає будь-яким нормам, законам і стандартам.

- Повний контроль над даними, додатками та інфраструктурою.

- Можливість вибору специфічного обладнання та гнучкість налаштувань відповідно до конкретних вимог бізнес-завдань.

- Можливість забезпечити високу продуктивність додатків.

- Можливість забезпечити високий рівень SLA клієнтів – доступність, продуктивність, масштабованість додатків при високому постійному навантаженні за рахунок виділених ресурсів.

- Можливість уникнути прив'язки до постачальника за рахунок вибору відкритих стандартів та стандартних стеків технологій.

В порівнянні з публічною хмарою приватна хмара налаштовується для задоволення унікальних потреб бізнесу та безпеки організації. Вона надає більше контролю над інфраструктурою, програмами та даними, і дозволяє управляти робочими навантаженнями відповідно до вимог організації, без втрати безпеки та продуктивності, що раніше досягалося лише спеціальними локальними ЦОД. Тому, якщо організація має критичні

для бізнесу системи, для яких важливо врахування індивідуальних вимог, зниження ризиків, безпека, а також організація має фінансові ресурси на розвиток інфраструктури у міру потреби, то вибір на користь приватної хмари буде кращим варіантом.

До недоліків приватної хмари можна віднести:

- Високі початкові фінансові витрати на обладнання та програмне забезпечення, а в подальшому витрати на навчання та утримання персоналу для підтримки хмари власними силами.

- Масштабованість обмежується виділеними обчислювальними ресурсами, а додавання ресурсів для задоволення непередбачуваних вимог потребує певного часу і зусиль.

- Обмеження доступу до нових технологій та інновацій, які надають постачальники публічних хмарних послуг.

### *Послуги гібридних хмар*

На подолання проблем, пов'язаних з приватними хмарами спрямована стратегія гібридних хмар. Інтегруючи загальнодоступні, приватні та локальні ресурси, компанії можуть отримати більше гнучкості та оптимізувати ресурси і витрати.

Переваги гібридної хмари:

- Доступ до інновацій. Організації можуть отримати гнучкість та інновації загальнодоступних хмар та задовольнити потреби різних бізнес-завдань в залежності від унікальних пропозицій постачальників.

- Керування ризиками. Організації можуть розподілити ризики, розподіляючи ресурси або резервні копії між різними хмарами, в тому числі, між хмарами різних постачальників.

- Розподіл контролю. Організації можуть перемістити некритичні додатки в загальнодоступну хмару, а конфіденційні дані та додатки в залежності від галузевих вимог або залишити на власних локальних ресурсах або на ресурсах приватної інфраструктури.

- Гнучкість масштабування. Організації можуть використовувати додаткові ресурси на вимогу в загальнодоступній хмарі під час короткострокових сплесків навантаження, а ресурси приватної хмари – для стабільних робочих навантажень, щоб не витрачати кошти на оплату надлишкових виділених ресурсів під час їх простою.

- Ефективне використання апаратних ресурсів. Для бізнес-завдань, що потребують високопродуктивних обчислень, в залежності від частоти та тривалості їх виконання організації можуть користуватися послугами або приватних або публічних хмар провайдерів, а робочі навантаження, для яких потрібна низька затримка, виконувати на власних локальних ресурсах.

- Економічність. Інтеграція різних типів хмар дозволяє оптимізувати витрати, вибираючи найбільш економічно ефективну платформу для кожного робочого навантаження.

Популярність гібридного підходу полягає в можливості поєднати в загальній інфраструктурі зручність та масштабованість публічних хмар з додатковим контролем, безпекою даних та оптимізацією швидкодії, які можуть надати приватні хмари та власна інфраструктура. Такий підхід дозволяє швидко реагувати на мінливі потреби бізнесу, оптимізувати витрати та ресурси, ефективно розподіляючи їх там, де це є найбільш доцільним.

Однак, впровадження гібридних хмарних сервісів пов'язано з рядом проблем.

- Складність наскрізного управління. Типові операційні завдання такі, як управління ресурсами та додатками, моніторинг, ведення журналу та усунення несправностей, безпека та технічна підтримка. у гібридному середовищі стає більш складним через різноманітність систем та інструментів. Може знадобитися залучення різних спеціалістів – для управління публічними та приватними хмарними ресурсами.

- Комплексність безпеки. Передача даних між публічною та приватною частинами потребує надійних та безпечних мережеских з'єднань. Складнощі у забезпеченні єдиних стандартів безпеки для обох середовищ можуть становити ризик безпеки.

- Підтримка стабільного рівня обслуговування SLA. Відмінності в архітектурі конфігурації між публічною та приватною частинами а також різні стратегії забезпечення продуктивності можуть створювати ризики сумісності та впливати на ефективність роботи систем.

- Управління витратами. Необхідність реалізації стратегій з оптимізації витрат на підставі аналізу за політик окремих провайдерів.

- Штат кваліфікованих фахівців для операційної підтримки хмари. Організації необхідно утримувати та дбати про підвищення кваліфікації персоналу з обслуговування та регулярного оновлення гібридної хмарної інфраструктури. Причому, потрібні окремі експерти по кожному напрямку технологій: для приватної, локальної та кожної з публічних хмар (наприклад, зі знанням нюансів в організації VMware, MS Azure або AWS).

- Прив'язка до постачальника. Така прив'язка виникає при використанні специфічних сервісів або технологій, які тісно інтегровані з конкретним постачальником хмарних послуг.

Між тим, добре розуміючи потреби і проблеми компаній, світові постачальники, розробники

хмарних рішень та регіональні сервіс-провайдери прагнуть забезпечити сумісність своїх платформ для надання послуг гібридних хмар.

Прикладами гібридних хмарних платформ для власних стеків технологій можуть слугувати AWS Outposts, VMware Cloud on AWS [15], Azure Stack, Azure Arc, Azure VMware Solution [16], Google Anthos [17], VMware Cloud Foundation [18]. А у травні 2023 року IBM представила IBM Hybrid Cloud Mesh – універсальну SaaS-пропозицію, покликану допомогти підприємствам керувати своєю інфраструктурою в гібридних, багатохмарних та гетерогенних середовищах [19]. Як приклади пропозицій для управління гібридною інфраструктурою в Україні можна привести: Hybrid Cloud Management X (HCMX) від компанії Micro Focus [20], рішення від Sim-networks, Colobridge, Ucloud [21, 11, 12].

Спростити інтеграцію також може підхід, при якому компанії прагнуть до уніфікації платформ у межах власної IT-інфраструктури для приватної та публічної хмари. При виборі стеку для побудови приватної хмара, наприклад, VMware, організація буде орієнтуватись на провайдерів сервісів IaaS/PaaS, які також використовують цю платформу.

Досвідчені сервіс провайдери з міцними позиціями на ринку хмарних послуг завжди мають в своєму штаті кваліфікованих фахівців. Вони надають допомогу організаціям у виборі архітектурних рішень для гібридного чи мультихмарного середовища, в тому числі із залученням сторонніх сервісів, в розрахунку витрат та економічного ефекту від впровадження, в налаштуванні комплексної безпеки та ефективної роботи додатків, а також в інших питаннях побудови, підтримки та розвитку хмарної інфраструктури компанії. Це особливо актуально для малого та середнього бізнесу, у якого бракує власних досвідчених спеціалістів.

#### *Хмарна стратегія*

Подолання проблем при побудові гібридної, приватної чи мультихмари вимагає від організації продуманої стратегії, гарного архітектурного рішення, залучення відповідних технологій та досвідчених партнерів.

Спочатку компанія має оцінити існуюче програмне забезпечення, визначити свої завдання та цілі, рівень ризику, який вона готова прийняти щодо своєї IT-інфраструктури та даних.

Для ефективного використання всіх переваг гібридного або мультихмарного підходу та успішного керування складною інфраструктурою, організація має розробити стратегію хмари. Стратегія повинна визначати, які програми та дані будуть розміщуватися локально, а які – у хмарі, які додаткові сервіси на стороні провайдера необхідні компанії.

Хороша хмарна стратегія повинна містити чітке економічне обґрунтування, оцінку витрат та зусиль, пов'язаних з її реалізацією, оцінку економічних, організаційних та технічних переваг, які отримає компанія від використання хмари. Плануючи міграцію у хмару, важливо розробити план поетапного та своєчасного виведення з експлуатації застарілого обладнання, обслуговування якого постійно вимагає коштів.

На наступному етапі слід розглянути різні хмарні стеки. Якщо завдання не надто критичні, можна обирати open source платформи, для важливих бізнес-додатків та середовищ краще використовувати комерційні платформи.

Стратегія застосування відкритих або широко підтримуваних комерційних платформ в основі хмари та програмних продуктів компанії, постійний аналіз нових пропозицій ринку та стану технологій дозволить уникати прив'язки до одного постачальника послуг та адаптувати корпоративну інфраструктуру до мінливих потреб бізнесу.

Подальшим кроком буде вибір базового хмарного провайдера, що міг би забезпечити максимальні переваги щодо набору сервісів, вартості, продуктивності та безпеки. Слід звертати увагу на клас хмарної платформи, яку пропонує провайдер, наприклад, корпоративний – Hyper-V або операторський – VMware vCloud, MS Azure Stack. Причому, рішення на Hyper-V більш орієнтовані на використання у власній корпоративній мережі та підтримку успадкованих додатків ніж на побудову нових на основі мікросервісної архітектури та концепції DevOps.

Також має значення наявність сертифікатів та статусів, які підтверджують компетенції провайдера, наявність технічної підтримки від вендорів.

Доцільно вибрати поетапний підхід до переходу на модель гібридної хмари та почати з менш складних робочих навантажень, перш ніж переходити до більш важливих систем, поступово переносючи робочі навантаження одну за одною.

**Висновки.** В сучасному конкурентному світі, де компанії прагнуть до цифрової трансформації, щоб отримати максимум ринкових переваг, хмарні технології стають невід'ємною частиною успішного бізнесу. Наряду з широким використанням загальнодоступних хмарних сервісів компанії все більше впроваджують приватні, гібридні та мультихмарні рішення, щоб досягти балансу між гнучкістю, контролем та інноваціями. Комбінування різних хмарних платформ, розподіл даних та навантаження між ними дозволяє оптимізувати витрати, зменшити ризики, пов'язані з виходом з ладу або змінами політики одного постачальника послуг, забезпечити відповідність галузевим



стандартам конфіденційності та безпеки, підвищити надійності та гнучкості в управлінні своєю ІТ-інфраструктурою.

А добре усвідомлення переваг та обмежень різних підходів до розгортання хмарних послуг,

розробка продуманої стратегії та архітектурного рішення, залучення досвідчених партнерів дозволять організаціям уникнути поширених помилок і забезпечити максимальну ефективність від використання корпоративної хмари.

### Список літератури:

1. Закон України “Про хмарні послуги”, <https://zakon.rada.gov.ua/laws/show/2075-20#Text>
2. Flexera: State of the Cloud Report. <https://info.flexera.com/CM-REPORT-State-of-the-Cloud-2024>
3. CNCF 2023 Annual Survey. April 2024. <https://www.cncf.io/reports/cncf-annual-survey-2023/>
4. Mordor Intelligence. Cloud Computing Market Size & Share Analysis - Growth Trends & Forecasts (2024-2029) <https://www.mordorintelligence.com/industry-reports/cloud-computing-market>
5. Mordor Intelligence. Hybrid Cloud Market Size - Industry Report on Share, Growth Trends & Forecasts Analysis (2024 - 2029). <https://www.mordorintelligence.com/industry-reports/hybrid-cloud-market>
6. Mell, Peter and Grance, Timothy. The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology. NIST (20 жовтня 2011). <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>
7. AWS. What is a Private Cloud? <https://aws.amazon.com/what-is/private-cloud/>
8. De Novo, <https://denovo.ua/>
9. OneCloudPlanet, <https://onecloudplanet.com>
10. Gigacloud, <https://gigacloud.ua/>
11. COLOBRIDGE, <https://blog.colobridge.net/2024/02/multicloud-and-hybrid-cloud-solutions-by-azure/>
12. Ucloud. Хмарні послуги, <https://ucloud.ua/services/>
13. ITRC Annual Data Breach Report <https://www.idtheftcenter.org/publication/2023-data-breach-report/>
14. The Guardian. Google Cloud accidentally deletes UniSuper’s online account due to ‘unprecedented misconfiguration’. <https://www.theguardian.com/australia-news/article/2024/may/09/unisuper-google-cloud-issue-account-access>
15. AWS, <https://aws.amazon.com/hybrid-multicloud/>
16. Microsoft, <https://azure.microsoft.com/solutions/hybrid-cloud-app>
17. Google Cloud, Anthos, <https://cloud.google.com/anthos>
18. VMware, Introducing VMware Cloud Foundation 9, <https://blogs.vmware.com/cloud-foundation/2024/08/27/vmware-cloud-foundation-9/>
19. IBM, IBM Hybrid Cloud Mesh, <https://www.ibm.com/products/hybrid-cloud-mesh>
20. Elko, <https://www.elko.ua/produkty/hybrid-cloud-management-x>
21. Gibrud Cloud Solutions, <https://www.sim-networks.com/en/cloud/hybrid-cloud>

### **Hiorhizova-Hai V.S., Kyriusha B.A. CLOUD SERVICES IN CORPORATE INFRASTRUCTURE**

*The article analyzes marketing reports of world-famous organizations and companies on the state of cloud technologies implementation, analyzes the proposals of global and regional service providers offering services in Ukraine. Based on this analysis, the article compares the capabilities, advantages and limitations of various cloud approaches to building a modern corporate infrastructure of organizations, considers the problems of implementing private, hybrid and multi-cloud technologies and ways to overcome them.*

*Modern companies are expanding their use of cloud technologies to gain competitive advantages in the market. Long-term experience with public clouds has revealed a number of their disadvantages: limited security and control, difficulty in complying with regulatory requirements, high latency, limited customization, service provider dependency, and uncontrolled cost growth. When organizations build clouds by our own efforts on-premises, they faced a shortage of qualified personnel to support them, problems with the limitations of existing infrastructure, and rising maintenance costs. In response to these challenges, global and regional service providers have offered services to deploy private clouds in an isolated environment on customers' leased or local infrastructure and hybrid cloud services that combine the benefits of private and public clouds to balance agility, control and innovation. According to various surveys, the vast majority of companies in the world choose a hybrid approach to deploying a corporate cloud. These cloud strategies are changing approaches to building corporate infrastructure and are becoming more popular year by year. But the implementation of these approaches, along with the benefits, can also lead to many problems for companies. However, challenges can be overcome if an organization has a good understanding of the different cloud approaches, a sound strategy and architecture for cloud deployment, and experienced partners.*

*This article aims to help organizations that are looking for new solutions for their business success to make the right choice.*

**Key words:** cloud technologies, corporate infrastructure, data security, public cloud, private cloud, hybrid cloud.