

ФУКС ОЛЕГ

EPAM Systems

<https://orcid.org/0009-0003-1366-7840>e-mail: olegfuks98@gmail.com

ПТАШИНСЬКИЙ МАР'ЯН

EPAM Systems

<https://orcid.org/0009-0009-7461-2740>e-mail: maryan.pt95@gmail.com

МАРІКУЦА УЛЯНА

Національний університет "Львівська політехніка"

<https://orcid.org/0000-0002-9514-7413>e-mail: uliana.b.marikutsa@lpnu.ua

ДОСЛІДЖЕННЯ МЕТОДІВ ОЦІНЮВАННЯ ЯКОСТІ ХМАРНИХ СЕРВІСІВ, ВКЛЮЧАЮЧИ МЕТРИКИ НАДІЙНОСТІ, ПРОДУКТИВНОСТІ ТА БЕЗПЕКИ

Стаття являє собою аналіз різних методів оцінювання якості хмарних сервісів. Зокрема розглядаються метрики надійності, продуктивності та безпеки, а також порівнюються різні моделі оцінювання.

Ключові слова: хмарні послуги, якість хмарних сервісів, оцінка якості хмарних сервісів, метрики хмарних сервісів.

FUKS OLEH, PTASHYNSKYI MARIAN

EPAM Systems

MARIKUTSA ULIANA

Lviv Polytechnic National University

RESEARCH METHODS FOR ASSESSING THE QUALITY OF CLOUD SERVICES, INCLUDING RELIABILITY, PERFORMANCE AND SECURITY METRICS

In today's world, cloud services play an important role in the success of any global business. Evaluating the quality of these services is of paramount importance for companies and individuals who use them for their operations and data management.

This article is an analysis of various methods for assessing the quality of cloud services. Reliability, performance, and security metrics are discussed, and different assessment models are compared.

In the introduction, the authors describe the importance of cloud services and the need to assess their quality. This article provides an overview of cloud service quality assessment methods and shows how they can be applied to different aspects of these services. In the main part of the article, the author describes different methods of assessing the quality of cloud services and compares different assessment models. The author also provides examples of how these methods are used. The methods for assessing the quality of cloud services are discussed, covering reliability, performance, and security. While these metrics provide valuable insights into the performance of cloud services, some counterarguments highlight the potential limitations of using standardized metrics for evaluation. The author also recommends choosing a cloud provider and optimizing cloud services.

It is emphasized that reliability metrics, such as uptime and disaster recovery time, are important to ensure the smooth operation of cloud services. Performance metrics, such as response time and throughput, indicate how quickly and efficiently cloud services can process data and requests. Security metrics, such as data encryption and access control, are important to protect data from unauthorized access and cyber threats.

The author also emphasizes the importance of considering subjective factors such as user experience and customer support when assessing the quality of cloud services. Finally, the author discusses various risk assessment models that can be used to assess the security of cloud services. The author proposes a new approach to assessing the quality of cloud services for educational institutions. This approach is based on using a combination of quantitative and qualitative indicators that consider the reliability, performance, security, and usability of cloud services.

In conclusion, the author recommends choosing a cloud provider and optimizing cloud services. Assessing the quality of cloud services is a complex process that requires a comprehensive and systematic approach. You need to consider various factors such as reliability, performance, and security, as well as your organization's individual needs and requirements.

Keywords: cloud services, cloud service quality, cloud service quality assessment, cloud service metrics.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Характерно, що якість хмарного сервісу є важливим аспектом в сучасному світі для успіху будь-якого глобального бізнесу. При цьому оцінка якості послуг має першорядне значення для компаній і окремих осіб, які покладаються на ці сервіси для своїх операцій і управління даними у середовищі хмарних сервісів, що швидко розвивається. Проблема оцінки якості хмарних сервісів, зокрема, з точки зору показників надійності, продуктивності та безпеки, є критично важливою для сучасних організацій. Оскільки все більше і більше підприємств переносять свої операції в хмару, забезпечення високої якості послуг, на які вони покладаються, стає важливішим. Оскільки поширеність хмарних обчислень продовжує зростати, зростають і пов'язані з ними ризики для безпеки. Хмарні обчислення створюють такі виклики, як безпека та конфіденційність даних, автентифікація, шифрування, інтеграція даних та проблеми доступу.

Аналіз досліджень та публікацій

Важливі аспекти висвітлюються такими українськими ученими як Л.В. Борисова, Н.В. Гришина, Н.В. Дженюк, І.І. Надточій, Л.О. Нікітіна, І.С. Крамаренко, І.В. Малярчук, М.А. Смолинець та інші. В роботі Л.О. Нікітіна, Н.В. Дженюк, Л.В. Борисова [1] описується експертна система для оцінки ризиків хмарних сервісів. Автори обговорюють виклики, з якими стикаються організації при виборі хмарних сервісів. Запропонована

система використовує нечітку логіку для оцінки ризиків. І.В. Малярчук, М.А. Смолинець [2] акцентують увагу на безпеці ефективності використанні хмарних технологій під час бізнес-процесів. І.І. Надточій, І.С. Крамаренко, Н.В. Гришина [3] описують хмарні технології як інструмент для ефективного управління фінансово-економічною безпекою та HR-технологіями. Автори доводять, що хмарні технології є корисним інструментом для управління фінансовою інформацією та безпекою даних. І. Данилюк, І. Будник [4] обговорюють важливість моніторингу IT-інфраструктури для виявлення проблем і забезпечення безперервної роботи. І.І. Малярчук, М.А. Смолинець [5] коректно визначають становище застосування хмарних технологій в умовах воєнного стану. Однак наявні публікації приділяють незначну увагу методам оцінювання якості наданих послуг хмарними провайдерами.

Формулювання цілей статті

Метою роботи є: надати огляд методів оцінювання якості хмарних сервісів і показати, як їх можна застосувати до різних аспектів хмарних послуг.

Виклад основного матеріалу

За словами Л.О. Нікітіної, Н.В. Дженюк, Л.В. Борисової: «Хмарний сервіс – послуга з надання хмарних ресурсів за допомогою технологій хмарних обчислень» [1, с. 146].

На думку І.В. Малярчук, М.А. Смолинець: «Сьогодні, глобальне розширення бізнесу потребує наявності надійної інфраструктури, здатної підтримувати операції у різних місцях та часових поясах. Хмарні технології полегшують безперешкодний доступ до даних та спільну роботу між географічно розосередженими командами, гарантуючи, що всі учасники мають у своєму розпорядженні актуальну інформацію та інструменти, незалежно від їхнього фізичного місцезнаходження. Така глобальна доступність як підвищує операційну ефективність, а й сприяє інноваціям з допомогою використання різноманітних точок зору і досвіду всередині організації. Крім того, зростаюча увага до прийняття рішень на основі даних наголошує на важливості хмарних технологій. Ці платформи надають розширені можливості аналітики та обробки великих даних, дозволяючи компаніям отримувати корисну інформацію з величезних обсягів даних. Використовуючи хмарну аналітику, компанії можуть оптимізувати свою діяльність, покращити якість обслуговування клієнтів та розробити цільові стратегії, що сприяють зростанню та прибутковості» [2, с. 2].

Автори дотримуються наступної точки зору: «Хмарні технології пропонують надійні рішення для зберігання, резервного копіювання та відновлення даних, забезпечуючи безперервність бізнесу та зводячи до мінімуму ризик втрати даних через кібератаки. Акцент на оптимізації витрат у сьогоднішніх економічних умовах також наголошує на важливості хмарних технологій. Впроваджуючи хмарні технології, підприємства можуть скоротити капітальні витрати на обладнання та інфраструктуру, перейшовши до більш передбачуваної моделі операційних витрат. Це не лише вивільняє капітал для стратегічних інвестицій, а й знижує загальну вартість IT-ресурсів. Крім того, хмарні сервіси часто включають автоматичні оновлення та обслуговування, що знижує навантаження на IT-персонал і гарантує, що підприємства зможуть використовувати новітні технології без значних додаткових інвестицій» [2, с. 2].

Як стверджують І.І. Надточій, І.С. Крамаренко, Н.В. Гришина: «Доступ до інформаційних технологій стає не просто конкурентною перевагою, а необхідною умовою функціонування суб'єктів господарювання. Швидке вдосконалення та поширення хмарних технологій є одним з тих ключових трендів. Використання хмарних сервісів є зручним інструментом забезпечення доступу до інформації з будь-якого пристрою та здатних забезпечити її безпеку» [3, с. 187].

Натомість зручність наданих хмарних послуг визначається за допомогою системи моніторингу та спеціальних методів та метрик. Зокрема, І. Данилюк, І. Будник зазначають: «Агент-базований моніторинг застосовують для моніторингу комп'ютерних систем й мереж та включає в себе встановлення додаткових агентів/програмного забезпечення на цільові пристрої. Його перевагою є те, що такий вид моніторингу дає більше можливостей у плані гнучкості й деталізації у збиранні інформації, може виконувати локальний аналіз та опрацювання даних. Однак встановлення й керування агентами на кожному цільовому пристрої може вимагати регулярного оновлення» [4, с. 46].

Як пишуть І. Данилюк та І. Будник є й інший підхід: «Агент-лесс моніторинг - процес моніторингу комп'ютерних систем і мереж, який не вимагає встановлення додаткових агентів/програмного забезпечення на цільові пристрої, і в цьому є його перевага (простота та гнучкість, відсутність додаткових витрат). Моніторинг здійснюється за допомогою запитів та отримання відповідей через існуючі мережеві протоколи. Агентлесс моніторинг дозволяє виявляти проблеми зі збоєм системи, відстежувати метрики продуктивності, виявляти збої безпеки та забезпечувати відповідну реакцію на них» [4, с. 46].

Натомість І.І. Малярчук, М.А. Смолинець виділяють особливу увагу застосуванню хмарних технологій в умовах воєнного стану: «В Україні, особливо в умовах воєнного стану, хмарні обчислення стали критично важливими для безперервності та стійкості бізнесу. Складне середовище підкреслює необхідність для бізнесу підтримувати роботу в умовах перебоїв, захищати важливі дані від кіберзагроз та адаптуватися до мінливих умов. Українські компанії використовують хмарні технології для забезпечення безперервності бізнесу, надаючи можливість працювати віддалено. Українські компанії покладаються на хмарні рішення для резервного копіювання та аварійного відновлення для захисту безперервності бізнесу в умовах фізичної та кібервійни. Хмарні технології забезпечують безпрецедентну операційну стійкість, що є найважливішою характеристикою у воєнний час. Можливість доступу до даних і додатків з будь-якого місця і в будь-який час

уможливило безперервність бізнесу, навіть якщо фізичні об'єкти скомпрометовані» [5, с. 468].

При цьому переходячи до методів оцінювання зауважимо, що методи оцінювання якості хмарних сервісів можуть бути різноманітними. Існує безліч меж метрик надійності, продуктивності та безпеки, які можна застосовувати для оцінки надаваних послуг.

По-перше, надійність (reliability). Це найважливіший критерій для оцінки хмарних сервісів, оскільки без надійності всі інші переваги є безглуздими. Метрики надійності можуть включати відсоток часу, протягом якого сервіс працює безперебійно, або відсоток часу, протягом якого були зареєстровані помилки. Ключовими показниками надійності є також відмовлення та час відновлення сервісів після відмови.

По-друге, продуктивність (performance). Продуктивність оцінюється за часом відповіді на запити, швидкістю доступу до даних та швидкістю виконання обробок. Методи оцінювання продуктивності можуть включати дослідження затримок відповіді на запити, вимірювання пропускну здатності сервера чи мережі та оцінку часу виконання різних операцій.

По-третє, продуктивність обробки даних (data processing efficiency). Ця метрика оцінює швидкість та ефективність обробки даних всередині хмарного сервісу. Методи оцінювання включають вимірювання часу потрібного для виконання різних операцій обробки даних, таких як вставка, оновлення, видалення чи пошук.

По-четверте, безпека (security). Безпека хмарних сервісів є ключовим фактором для підтримки довіри клієнтів. Методи оцінювання безпеки включають тестинг системного доступу, перевірку реагування на спроби несанкціонованого доступу та оцінку безпеки передачі даних.

По-п'яте, співпраця (collaboration). Методи оцінювання співпраці можуть включати вимірювання часу відповіді на запити з боку клієнтів, швидкості передачі даних між сервісами та ступінь взаємодії між розробниками та користувачами.

По-шосте, співпраця (interoperability). Це показник, який оцінює здатність хмарних сервісів співпрацювати між собою та інтегруватися з існуючими системами клієнтів. Методи оцінювання включають перевірку підтримки відповідних протоколів, форматів даних та програмних інтерфейсів.

Нарешті по-сьоме, масштабовність (scalability). Це показник, який оцінює здатність хмарних сервісів працювати ефективно при зростанні навантаження. Методи оцінювання включають перевірку можливості розширення та модифікації системи під час навантаження, а також оцінку часу потрібного для введення нових ресурсів. Зупинимось детальніше на методах і метриках щодо оцінювання наданих хмарних послуг стосовно надійності, продуктивності та безпеки (рис. 1).

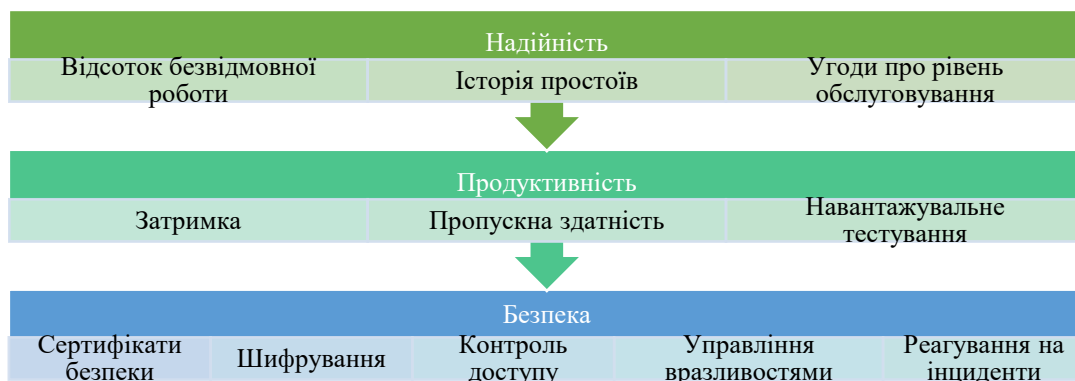


Рис. 1. Метрики оцінки хмарних сервісів щодо надійності, продуктивності та безпеки (розроблено автором [6, 7, 8])

Оцінка якості хмарних сервісів, особливо щодо надійності, продуктивності та безпеки, вимагає комплексного та систематичного підходу. Розглянемо методи дослідження та метрики, які можна використовувати для оцінки хмарних сервісів.

1. Надійність:

а. Відсоток безвідмовної роботи. Цей показник вимірює відсоток часу, протягом якого хмарний сервіс доступний для користувачів. Високий відсоток безвідмовної роботи (наприклад, 99,9% або вище) свідчить про надійність сервісу.

б. Історія простоїв. Вивчення історичних записів про простої постачальника хмарних послуг може дати уявлення про його надійність. Шукайте закономірності або причини простоїв і оцінюйте, наскільки добре провайдер їх усував.

с. Угоди про рівень обслуговування (SLA). Провайдери хмарних сервісів часто пропонують SLA, які гарантують мінімальний рівень безвідмовної роботи та якості послуг. Перегляньте ці угоди і переконайтеся, що вони відповідають вимогам вашої організації.

2. Продуктивність:

а. Затримка. Цей показник вимірює час, необхідний для передачі даних від пристрою користувача до хмарного сервісу і назад. Низька затримка має вирішальне значення для додатків, які вимагають взаємодії в режимі реального часу, таких як відеоконференції або онлайн-ігри.

б. Пропускна здатність. Цей показник вимірює обсяг даних, який може бути оброблений або

переданий хмарним сервісом за певний проміжок часу. Висока пропускна здатність важлива для додатків, які обробляють великі обсяги даних, таких як аналітика великих даних або мережі доставки контенту.

с. Навантажувальне тестування. Проведення симуляцій тестування навантаження може допомогти оцінити продуктивність хмарного сервісу за різних умов, наприклад, при збільшенні трафіку користувачів або попиту на ресурси. Це може дати уявлення про потенційні вузькі місця або області для вдосконалення.

3. Безпека:

а. Сертифікати безпеки. Провайдери хмарних сервісів можуть мати сертифікати, такі як ISO 27001, SOC 2 або PCI DSS, які свідчать про те, що вони відповідають певним стандартам безпеки. Переконайтеся, що провайдер, якого ви розглядаєте, має відповідні сертифікати для вашої галузі.

б. Шифрування. Переконайтеся, що постачальник хмарних послуг використовує надійні алгоритми шифрування для захисту даних як під час передачі, так і в стані спокою.

с. Контроль доступу. Оцініть політику та процедури контролю доступу провайдера, щоб переконатися, що лише уповноважений персонал має доступ до ваших даних і систем.

д. Управління вразливостями. Перегляньте програму управління вразливостями провайдера, щоб зрозуміти їхній процес виявлення, виправлення та зменшення вразливостей безпеки.

е. Реагування на інциденти. Оцініть план реагування на інциденти та можливості провайдера, щоб переконатися, що він може ефективно реагувати на інциденти безпеки та мінімізувати збитки [6].

Не викликає заперечення, що надійність є наріжним каменем для оцінки якості хмарних сервісів, забезпечення постійного та безперебійного надання послуг. Показники, зосереджені на надійності, наприклад відсоток безвідмовної роботи, забезпечують кількісне вимірювання того, як часто послуга доступна користувачам. Вищий відсоток безвідмовної роботи вказує на більш надійну службу, що має вирішальне значення для підприємств, яким потрібен безперервний на запити користувачів. Швидший час відгуку сприяє більш плавній роботі користувача та підвищенню ефективності. Крім того, заходи стійкості до відмов, такі як резервування та механізми відновлення після збоїв, підвищують надійність хмарних служб шляхом мінімізації впливу потенційних збоїв.

Хоча стандартизовані показники надійності пропонують цінну інформацію, універсальні показники можуть не врахувати нюанси різних хмарних служб. Різні галузі мають різні вимоги та пріоритети, що вимагає індивідуальних критеріїв оцінки. Наприклад, фінансова установа може надавати перевагу безпеці даних над відсотком безвідмовної роботи, вимагаючи індивідуальних показників для оцінки. Індивідуальні показники можуть запропонувати більш повну оцінку хмарних служб, узгоджуючи її з конкретними галузевими потребами та характеристиками послуг. Надмірна увага до стандартизованих показників може надто спростити процес оцінювання, потенційно не звертаючи уваги на важливі аспекти якості, унікальні для кожної послуги.

Постачальник хмарних послуг має можливість аварійного відновлення для організацій-клієнтів. Хмарні сервіси, що використовуються в організації, є надійними, тобто завжди надають однаковий результат для одного і того ж запиту, якщо немає змін у базових даних. Хмарні системи, які ви використовуєте, є стійкими / відмовостійкими, тобто якщо одна система виходить з ладу, інша доступна. Хмарні системи надають точні та безпомилкові послуги, транзакції та записи. Постачальник хмарних послуг надає послуги, які він обіцяв організації

За словами S. Pare, F. Paci, J. Jürjens, F. Massacci: «Надійність (reliability) – означає, як хмарна служба працює без збоїв за певних умов роботи протягом певного періоду часу. Розраховується як добуток обіцяного середнього часу до відмови постачальника хмарних послуг та ймовірності відмови служби протягом визначеного часу. У контексті SaaS це означає, наскільки надійним є примірник програмного забезпечення, для PaaS вона пов'язана з надійністю платформи, а для IaaS – це надійність віртуальних машин або служб зберігання даних» [6].

Звернемо увагу, що показники продуктивності відіграють важливу роль в оцінці ефективності та продуктивності хмарних служб, впливаючи на загальну взаємодію з користувачем. Такі показники, як швидкість обробки даних, дають зрозуміти, наскільки швидко служба може обробляти та керувати даними, що впливає на швидкість операцій для користувачів. Показники масштабованості вказують на здатність служби адаптуватися та розширюватися відповідно до вимог користувачів, забезпечуючи безперебійну роботу навіть у періоди підвищеного навантаження. Крім того, оцінка показників використання ресурсів допомагає оптимізувати розподіл ресурсів у хмарному середовищі, підвищуючи ефективність і економічність для користувачів [7].

Хоча показники продуктивності пропонують кількісну оцінку ефективності, оцінка хмарних служб виключно на основі показників може не враховувати суб'єктивний характер досвіду користувача. На задоволеність користувачів, важливий аспект якості послуг, впливають фактори, що не входять до кількісних показників. Взаємодія з користувачем є суб'єктивною та може залежати від таких факторів, як дизайн інтерфейсу, простота використання та якість підтримки клієнтів, які можуть не повністю відобразитися показниками продуктивності. Таким чином, цілісна оцінка хмарних послуг повинна враховувати як кількісні показники, так і якісні аспекти, щоб забезпечити комплексну оцінку якості послуг.

Натомість показники безпеки є фундаментальними для забезпечення безпеки та цілісності даних, що зберігаються й обробляються в хмарі, захисту від потенційних кіберзагроз і несанкціонованого доступу. Протоколи шифрування служать критично важливим показником безпеки, шифруючи дані для запобігання

несанкціонованому перехопленню та забезпечуючи конфіденційність. Заходи контролю доступу, такі як контроль доступу на основі ролей (RBAC), обмежують доступ до конфіденційних даних на основі ролей користувачів, зменшуючи ризик витоку даних. Крім того, механізми виявлення загроз, включаючи системи виявлення вторгнень (IDS) і моніторинг подій безпеки, покращують безпеку хмарних служб, забезпечуючи раннє виявлення та пом'якшення інцидентів безпеки [7].

Суворе покладання на показники безпеки для оцінки хмарних служб може знехтувати людським фактором у якості послуг, охоплюючи аспекти, що виходять за межі кількісних вимірювань. Людське спілкування та підтримка відіграють важливу роль у забезпеченні якісного надання послуг, зміцненні довіри та впевненості серед користувачів. Емоційний інтелект і емпатія, необхідні для вирішення занепокоєнь користувачів і вирішення проблем, не можуть бути кількісно визначені традиційними показниками безпеки. Зосереджуючись виключно на кількісних показниках безпеки, існує ризик не помітити цілісну якість хмарних сервісів, яка охоплює як технічні заходи безпеки, так і орієнтовані на людину аспекти надання послуг.

Варто погодитись з S. Pape, F. Paci, J. Jürgens, F. Massacci: «Безпека (security) – важлива характеристика, коли йдеться про збереження важливих даних компанії в хмарі. Безпека хмарних обчислень – це набір технологій і політик на основі контролю, призначених для дотримання правил відповідності нормативним вимогам і захисту інформації, програм та інфраструктури, пов'язаних із використанням хмарних обчислень. Найчастіше постачальники хмарних послуг мають декілька стандартів заходів безпеки. Функція безпеки дає змогу обмежити доступ до ресурсів і допомагає захистити дані від зловмисників. Це важливий якісний показник, який визначається згідно із шкалою від 1 до 10 і оцінюється користувачем послуги» [6].

Не секрет, що хмарні обчислення стикаються з більшою кількістю загроз безпеці, що вимагає кращих заходів безпеки. Хмарний хостинг критично важливих даних вимагає надійної системи безпеки, здатної адаптуватися до навколишнього контексту, залучати відповідні ресурси та ефективно управляти ризиками. Моделі OCTAVE Allegro, COBIT 5 і CORAS рекомендуються для хмарного хостингу, оскільки вони враховують тріаду ЦПУ, акцентуючи увагу на зберіганні, обробці та передачі інформації. Однак моделі ISO27005, NIST SP 800-30 і CRAMM, хоча і є всеосяжними, не можуть запропонувати конкретних і точних рекомендацій щодо аналізу та оцінки ризиків, пов'язаних з хмарними технологіями. Моделі CORAS, OCTAVE та COBIT5 надають чітку процедуру оцінки ризиків, пов'язаних як з внутрішніми, так і з зовнішніми системами та програмними ресурсами, включаючи специфічну інфраструктуру хмарних обчислень [7].

Тільки авторизовані користувачі можуть отримати доступ до послуг, що надаються постачальником хмарних послуг. Дані вашої організації захищені від вірусів/шкідливого програмного забезпечення/атак, поки вони знаходяться в хмарі. Дані вашої організації захищені від стихійних лих, оскільки вони розміщені в хмарі. Співробітники постачальника хмарних послуг не використовують і не поширюють дані організації без письмового дозволу.

У хмарних транзакціях використовується шифрування даних [8]. Міграція до хмари зростає, що ставить перед нею нові виклики та складнощі. Зберігання даних у хмарі не є ані простим, ані традиційним; навпаки, воно стає дедалі складнішим через багатогранність та обсяг даних [9].

Як зазначають J. Alonso, L. Ogue-Echevarria, V. Casola: «Хоча хмарні обчислення є ефективним способом отримання обчислень і зберігання даних як послуги для багатьох додатків, вони можуть не підходити для обробки нескінченних даних, що генеруються пристроями Інтернету речей. Деякі з обмежень традиційної хмарної парадигми особливо стосуються додатків, які повинні відповідати суворим вимогам реагування в режимі реального часу і низької затримки, або тих, що підтримують критично важливу інфраструктуру» [10].

Оцінка якості хмарних служб за допомогою показників надійності, продуктивності та безпеки дає цінну інформацію про їх продуктивність і можливості. Хоча стандартизовані показники пропонують кількісні оцінки, важливо визнати обмеження універсальних показників і потенційні недогляди, покладаючись виключно на кількісні оцінки. Розглядаючи як аргументовану, так і контраргументативну точки зору, зацікавлені сторони можуть прийняти збалансований підхід до оцінки хмарних сервісів, охоплюючи як кількісні показники, так і якісні аспекти для забезпечення комплексної оцінки якості послуг.

Коли справа доходить до оцінки якості хмарних сервісів, дослідники і практики використовують цілий ряд методів і метрик для оцінки надійності, продуктивності та безпеки. Ці методи та показники можуть відрізнятися залежно від конкретної моделі хмарного сервісу (інфраструктура як послуга, платформа як послуга, програмне забезпечення як послуга), типу програми або сервісу, що розміщується, а також потреб та очікувань кінцевих користувачів.

Ось деякі з ключових методів дослідження та метрик, що використовуються для оцінки якості хмарних сервісів:

По-перше, аудит SLA (Угоди про рівень обслуговування). Постачальники хмарних послуг зазвичай пропонують SLA, які гарантують певний рівень надійності та продуктивності. Дослідники можуть провести аудит цих SLA, щоб переконатися, що вони чітко визначені, досяжні і послідовно виконуються. Поширені показники SLA включають відсоток безвідмовної роботи, час відгуку і доступність.

По-друге, тестування продуктивності. Дослідники можуть використовувати різноманітні інструменти та методології тестування продуктивності для моделювання реальних сценаріїв використання та виявлення потенційних вузьких місць або проблем у хмарній інфраструктурі. Це може включати

навантажувальне тестування, стрес-тестування, тестування масштабованості та тестування на витривалість.

По-третє, оцінка безпеки. Хмарні сервіси часто обробляють конфіденційні дані, тому дуже важливо забезпечити їхню безпеку. Дослідники можуть проводити оцінку безпеки, використовуючи тестування на проникнення, сканування вразливостей та інші методи для виявлення потенційних вразливостей і оцінки ефективності заходів безпеки хмарного провайдера.

По-четверте, опитування задоволеності клієнтів. Збір відгуків від реальних користувачів хмарних сервісів може надати цінну інформацію про їхній досвід роботи з надійністю, продуктивністю та безпекою. Дослідники можуть розробляти і розповсюджувати опитування для збору цієї інформації безпосередньо від клієнтів.

По-п'яте, бенчмаркінг. Порівнюючи продуктивність і функції безпеки різних постачальників хмарних послуг, дослідники можуть виявити найкращі практики і встановити еталони якості. Це може включати використання стандартних галузевих інструментів бенчмаркінгу та порівняння результатів у різних постачальників.

По-шосте, моніторинг та аналітика. Постійний моніторинг продуктивності, доступності та безпеки хмарних сервісів може допомогти виявити тенденції, потенційні проблеми та сфери для вдосконалення. Дослідники можуть використовувати різноманітні інструменти моніторингу та аналітичні платформи для збору та аналізу цих даних.

По-сьоме, сертифікація та відповідність. Багато постачальників хмарних послуг добровільно проходять незалежний аудит і сертифікацію, щоб продемонструвати свою відповідність галузевим стандартам і правилам, пов'язаним з безпекою, конфіденційністю та іншими аспектами якості. Дослідники можуть переглянути ці сертифікати та аудиторські звіти, щоб оцінити прихильність провайдера до якості.

Висновки з даного дослідження

і перспективи подальших розвідок у даному напрямі

Підсумовуючи, оцінюючи хмарні сервіси на предмет надійності, продуктивності та безпеки, враховуйте відсоток безвідмовної роботи, історію простоїв, угоди про рівень обслуговування, затримки, пропускну здатність, тестування навантаження, сертифікати безпеки, шифрування, контроль доступу, управління вразливостями та можливості реагування на інциденти. Ретельно проаналізувавши ці фактори, ви зможете прийняти обґрунтоване рішення про те, який постачальник хмарних послуг найкраще відповідає потребам вашої організації.

Таким чином, використовується комбінація методів і метрик для оцінки надійності, продуктивності та безпеки хмарних сервісів. Ретельно вивчивши ці фактори, надається цінна інформація та рекомендації, які допоможуть організаціям приймати обґрунтовані рішення при виборі постачальника хмарних послуг.

Література

1. Нікітіна Л.О., Дженюк Н.В., Борисова Л.В. Експертна система для оцінки ризиків хмарних сервісів. Системи управління, навігації та зв'язку. Збірник наукових праць. Полтава: ПНТУ, 2024. Т. 1 (75). С. 146-151. DOI <https://doi.org/10.26906/SUNZ.2024.1.146>. URL: <https://journals.nupp.edu.ua/sunz/article/view/3287> (дата звернення: 13.06.2024).
2. Малярчук І.В., Смолинець М.А. Підвищення ефективності бізнес-процесів через застосування хмарних технологій: безпековий аспект. Економіка та суспільство. 2024. № 60. 5 с. DOI <https://doi.org/10.32782/2524-0072/2024-60-3> URL: <https://economyandsociety.in.ua/index.php/journal/article/view/3546/3476> (дата звернення: 12.06.2024).
3. Надточій І.І., Крамаренко І.С., Гришина Н.В. Хмарні технології як інструмент ефективного управління фінансово-економічною безпекою та HR-технологіями в умовах цифровізації. Економічний простір. 2024. № 190. С. 187-191. DOI <https://doi.org/10.32782/2224-6282/190-34> URL: <http://prostir.pdaba.dp.ua/index.php/journal/article/view/1473> (дата звернення: 12.06.2024).
4. Данилюк І., Будник І. Технологія проведення комплексного ІТ-моніторингу компанії. Галицький економічний вісник. 2024. № 2 (87). С. 40-49. DOI https://doi.org/10.33108/galicianvisnyk_tntu2024.02.040 URL: https://elartu.tntu.edu.ua/bitstream/lib/45113/2/GEJ_2024v87n2_Danylyuk_I-Technology_of_carryng_out_40-49.pdf (дата звернення: 13.06.2024).
5. Малярчук І.І. Смолинець М.А. Використання хмарних технологій для оптимізації бізнес процесів на підприємстві: виклики воєнного стану. Наукові інновації та передові технології. 2024. № 3(31). С. 465-473. DOI [https://doi.org/10.52058/2786-5274-2024-3\(31\)-465-473](https://doi.org/10.52058/2786-5274-2024-3(31)-465-473) URL: <http://perspectives.pp.ua/index.php/nauka/article/view/9727/9780> (дата звернення: 13.06.2024).
6. Pape S., Paci F., Jürjens J., Massacci F. Selecting a Secure Cloud Provider—An Empirical Study and Multi Criteria Approach. Information. 2020; 11(5):261. <https://doi.org/10.3390/info11050261> URL: <https://www.mdpi.com/2078-2489/11/5/261> (date of access: 14.06.2024).
7. Ali, T., Al-Khalidi, M., & Al-Zaidi, R. Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review. Journal of Computer Information Systems, 2024. 1–28. DOI <https://doi.org/10.1080/08874417.2024.2329985> URL: <https://www.tandfonline.com/doi/full/10.1080/08874417.2024.2329985> (date of access: 14.06.2024).
8. Agarwal R., Dhingra S. Factors influencing cloud service quality and their relationship with customer

satisfaction and loyalty. *Heliyon*, 2023. Volume 9, Issue 4, DOI <https://doi.org/10.1016/j.heliyon.2023.e15177> URL: <https://www.sciencedirect.com/science/article/pii/S2405844023023848> (date of access: 14.06.2024).

9. Alzahrani, A., Alyas, T., Alissa, K., Abbas, Q., Alsaawy, Y., & Tabassum, N. Hybrid Approach for Improving the Performance of Data Reliability in Cloud Storage Management. *Sensors* (Basel, Switzerland), 2022. 22(16), 5966. DOI <https://doi.org/10.3390/s22165966> URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9412250/> (date of access: 14.06.2024).

10. Alonso, J., Orue-Echevarria, L., Casola, V. et al. Understanding the challenges and novel architectural models of multi-cloud native applications – a systematic literature review. *J Cloud Comp*. 2023. 12, 6. DOI <https://doi.org/10.1186/s13677-022-00367-6> URL: <https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-022-00367-6#citeas> (date of access: 14.06.2024).

References

1. Nikitina L.O., Dzheniuk N.V., Borysova L.V. (2024). Ekspertna systema dlia otsinky ryzykiv khmarnykh servisiv [Expert system for risk assessment of cloud services]. *Systemy upravlinnia, navihatsii ta zviazku. Zbirnyk naukovykh prats. Poltava: PNTU - Control, navigation and communication systems. Collection of scientific papers. Poltava: PNTU*. 1(75), 146-151. DOI <https://doi.org/10.26906/SUNZ.2024.1.146>. Retrieved from: <https://journals.nupp.edu.ua/sunz/article/view/3287> [in Ukrainian].

2. Maliarchuk I.V., Smolynets M.A. (2024). Pidvyshchennia efektyvnosti biznes-protseviv cherez zastosuvannia khmarnykh tekhnolohii: bezpekovyi aspekt [Increasing the efficiency of business processes through the use of cloud technologies: security aspect]. *Ekonomika ta suspilstvo - Economy and society*. 60, 5. DOI <https://doi.org/10.32782/2524-0072/2024-60-3> Retrieved from: <https://economyandsociety.in.ua/index.php/journal/article/view/3546/3476> [in Ukrainian].

3. Nadochii I.I., Kramarenko I.S., Hryshyna N.V. (2024). Khmarni tekhnolohii yak instrument efektyvnoho upravlinnia finansovo-ekonomichnoi bezpekoiu ta HR-tekhnolohiiamy v umovakh tsyfrovizatsii [Cloud technologies as a tool for effective management of financial and economic security and HR technologies in the context of digitalization]. *Ekonomichniy prostir - Economic space*. 190, 187-191. DOI <https://doi.org/10.32782/2224-6282/190-34> Retrieved from: <http://prostir.pdaba.dp.ua/index.php/journal/article/view/1473> [in Ukrainian].

4. Danyliuk I., Budnyk I. (2024). Tekhnolohiia provedennia kompleksnoho IT-monitorynhu kompanii [Technology of comprehensive IT monitoring of the company]. *Halytskyi ekonomichniy visnyk - Galician Economic Herald*. 2 (87). 40-49. DOI https://doi.org/10.33108/galicianvisnyk_tntu2024.02.040 Retrieved from: https://elartu.tntu.edu.ua/bitstream/lib/45113/2/GEJ_2024v87n2_Danylyuk_I-Technology_of_carryng_out_40-49.pdf [in Ukrainian].

5. Maliarchuk I.I., Smolynets M.A. (2024). Vykorystannia khmarnykh tekhnolohii dlia optymizatsii biznes protseviv na pidpriemstvi: vyklyky voiennoho stanu [Using cloud technologies to optimize business processes at an enterprise: challenges of martial law]. *Naukovi innovatsii ta peredovi tekhnolohii - Scientific innovations and advanced technologies*. 3(31). 465-473. DOI [https://doi.org/10.52058/2786-5274-2024-3\(31\)-465-473](https://doi.org/10.52058/2786-5274-2024-3(31)-465-473) Retrieved from: <http://perspectives.pp.ua/index.php/nauka/article/view/9727/9780> [in Ukrainian].

6. Pape S., Paci F., Jürjens J., Massacci F. (2020). Selecting a Secure Cloud Provider—An Empirical Study and Multi Criteria Approach. *Information*. 11(5):261. <https://doi.org/10.3390/info11050261> Retrieved from: <https://www.mdpi.com/2078-2489/11/5/261> [in English].

7. Ali, T., Al-Khalidi, M., & Al-Zaidi, R. (2024). Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review. *Journal of Computer Information Systems*, 1–28. <https://doi.org/10.1080/08874417.2024.2329985> Retrieved from: <https://www.tandfonline.com/doi/full/10.1080/08874417.2024.2329985> [in English].

8. Agarwal R., Dhingra S. (2023). Factors influencing cloud service quality and their relationship with customer satisfaction and loyalty. *Heliyon*, Volume 9, Issue 4, DOI <https://doi.org/10.1016/j.heliyon.2023.e15177> Retrieved from: <https://www.sciencedirect.com/science/article/pii/S2405844023023848> [in English].

9. Alzahrani, A., Alyas, T., Alissa, K., Abbas, Q., Alsaawy, Y., & Tabassum, N. (2022). Hybrid Approach for Improving the Performance of Data Reliability in Cloud Storage Management. *Sensors* (Basel, Switzerland), 22(16), 5966. DOI <https://doi.org/10.3390/s22165966> Retrieved from: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9412250/> [in English].

10. Alonso, J., Orue-Echevarria, L., Casola, V. et al. (2023). Understanding the challenges and novel architectural models of multi-cloud native applications – a systematic literature review. *J Cloud Comp* 12, 6. DOI <https://doi.org/10.1186/s13677-022-00367-6> Retrieved from: <https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-022-00367-6#citeas> [in English].