УДК 004.056.5:004.738.5

МЕТОДИ ЗАХИСТУ ОСОБИСТИХ ДАНИХ У ХМАРНИХ СЕРВІСАХ

Ольга Українець, Оксана Онищук

METHODS FOR PROTECTING PERSONAL DATA IN CLOUD SERVICES

Olga Ukrainets, Oksana Onyshchuk

Волинський національний університет імені Лесі Українки, просп. Волі, 13, Луцьк, 43025, Україна

Abstract. T*he article examines the functionality of cloud storage systems and the challenges of ensuring their information security. It highlights the evolution of data protection measures — from traditional network tools to advanced approaches such as client-side encryption, containerization, multi-factor authentication, and future directions in quantum cryptography. Special attention is given to the differences between private and corporate cloud usage, as well as issues of authorization and authentication within enterprise IT infrastructures.*

Хмарні сховища — це зручний сервіс для обробки та зберігання інформації користувачів, який тісно інтегрований у мобільні операційні системи смартфонів і настільні ПК. Для підключення до хмарних технологій активно використовуються захищені браузери. Щодня велика кількість користувачів синхронізує свої пристрої з хмарними сервісами, зберігаючи там відео, документи, фотографії, музику та навіть паролі до інших сервісів.

Розвиток хмарних технологій та методів захисту даних став результатом багаторічної еволюції обчислювальних систем і засобів забезпечення безпеки. Спочатку хмарні обчислення були орієнтовані на забезпечення зберігання даних і віддалений доступ до ресурсів. Проте зі зростанням обсягів даних і поширенням хмарних платформ зросла і кількість кіберзагроз. Перші хмарні технології почали активно впроваджуватись у середині 2000-х років, коли великі компанії, зокрема Amazon (Amazon Web Services), Google (Google Compute Engine) і Microsoft (Azure, з 2010 року), почали пропонувати відповідні сервіси.

Однією з основних переваг хмарних технологій є можливість доступу до даних із будь-якої точки світу та з будь-якого пристрою. Водночас це створює потенційні ризики — зокрема, можливість несанкціонованого доступу до даних з боку кіберзлочинців. Початково захист у хмарному середовищі обмежувався традиційними засобами, такими як міжмережеві екрани та VPN. Із зростанням складності систем і кількості користувачів хмарні провайдери зіткнулися з новими загрозами. У відповідь було запроваджено різноманітні протоколи та стандарти шифрування, які стали основою сучасної хмарної безпеки. У 2010-х роках, зокрема, почалося впровадження стандарту шифрування AES (Advanced Encryption Standard) для захисту збережених даних. Подальший розвиток приніс шифрування на стороні клієнта (client-side encryption), що дозволяє користувачам зашифровувати дані перед передачею в хмару, підвищуючи рівень довіри до сервісу — навіть провайдери не мають доступу до ключів.

З упровадженням контейнерних технологій, таких як Docker і Kubernetes, з’явилися нові виклики у сфері безпеки. Контейнери забезпечують швидке масштабування та розгортання додатків, проте через розподіленість даних та високий рівень інтеграції зростають і ризики. У відповідь на це були розроблені додаткові засоби автентифікації, управління доступом та моніторингу, які гарантують цілісність і доступність даних у середовищі контейнеризації.

Окрім протоколів шифрування, активно використовуються й інші технології, зокрема багатоетапна автентифікація (MFA), токени доступу та контроль прав на основі ролей (RBAC).

Також ведеться активна розробка квантових методів захисту й механізмів наскрізного шифрування (end-to-end encryption), які забезпечують стійкість до складніших атак і мають значний потенціал у майбутньому.

Значну роль у забезпеченні безпеки хмарних сервісів відіграє також відповідність нормативним вимогам і стандартам, таким як ISO/IEC 27001, GDPR та NIST. Дотримання цих стандартів є не лише індикатором зрілості інформаційної безпеки компанії, а й важливою умовою довіри користувачів і партнерів. Провайдери хмарних послуг повинні впроваджувати прозорі політики зберігання та обробки даних, а також надавати клієнтам інструменти для аудиту доступу та логування дій. Завдяки цьому організації можуть не лише зменшити ризики витоку інформації, а й оперативно реагувати на потенційні інциденти безпеки.

Для пересічних користувачів використання хмарних сервісів є загалом безпечним — за умови шифрування даних та використання складних паролів. Натомість для компаній питання безпеки ускладнюється через багаторівневу структуру доступу до хмарних IT-інфраструктур. Співробітники можуть працювати з різних місць і пристроїв, тому критично важливими стають механізми автентифікації та авторизації, які забезпечують персоніфікований і контрольований доступ до даних.

Отже, хмарні технології стали невід'ємною складовою цифрового середовища, надаючи зручний доступ до даних. Водночас зростають і загрози безпеці інформації. Еволюція методів захисту — від базових мережевих засобів до шифрування, MFA і контейнеризації — свідчить про послідовне прагнення до посилення конфіденційності та цілісності даних. Особливої уваги потребує корпоративне використання хмар, де акцент зроблено на автентифікації та авторизації як основі безпечного функціонування IT-інфраструктури. У майбутньому ключову роль відіграватимуть квантові технології захисту та наскрізне шифрування даних.

У перспективі хмарні технології будуть дедалі тісніше інтегруватися з такими напрямами, як штучний інтелект, інтернет речей (IoT) та периферійні обчислення (edge computing), що вимагатиме нових підходів до захисту даних у децентралізованих середовищах. Зростатиме роль автоматизованих систем виявлення загроз, заснованих на машинному навчанні, здатних оперативно ідентифікувати аномальні дії та реагувати на інциденти в режимі реального часу. Таким чином, безпека хмарних сервісів трансформується у проактивну модель захисту, де передбачення загроз стане так само важливим, як і їхнє запобігання.

Бібліографія

1. Безпека хмарних сховищ і технологій. Основні правила [Електронний ресурс] //*DataMi*.– 2024.– https://datami.ee/ua/blog/bezpeka-hmarnih-shovish-i-tehnologij-osnovni-pravila/ (30.04.2025).
2. Безпека хмарних сервісів [Електронний ресурс] // *ESKA Global*. – 2024. – Режим доступу: https://eska.global/blog/bezpeka-hmarnih-servisiv (дата звернення: 30.04.2025).
3. Google Cloud. (n.d.). *Google Compute Engine documentation*. https://cloud.google.com/compute/docs
4. ISO/IEC. (2013). *Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001:2013)*. International Organization for Standardization. https://www.iso.org/standard/54534.html
5. National Institute of Standards and Technology. (2020). *Framework for improving critical infrastructure cybersecurity*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf