УДК 004.67
Лупенко А. М., д.т.н., Гарасівка А. В.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

КЛЮЧОВІ ЕЛЕМЕНТИ ІНФОРМАЦІЙНОЇ МОДЕЛІ ХМАРНИХ СХОВИЩ

Lupenko A. M., D.E.Sc., Harasivka A. V.

KEY ELEMENTS OF THE INFORMATION MODEL OF CLOUD STORAGE

Хмарне сховище — це сервіс, який дозволяє користувачам зберігати та отримувати доступ до своїх даних (фотографії, відео, будь-які інші види файлів) зазвичай через всесвітню мережу Інтернет, за допомогою веб-інтерфейсу / консолі чи програми. Замість того, щоб зберігати дані локально на власних пристроях, користувачі завантажують їх на сервери, які належать або управляються постачальником послуг, і мають можливість створення й редагування файлів безпосередньо у хмарному сховищі, керування доступом і ведення спільної роботу з файлами, перегляд історії зміни файлів.

Хмарні сховища є інноваційними інформаційними моделями та технологіями, які дозволяють ефективно управляти даними. Інформаційна модель для хмарних сховищ включає такі ключові аспекти:

- Ідентифікація та автентифікація – для керування доступом.
- Шифрування в сховищі (at rest) – це шифрування, яке використовується для захисту даних, які зберігаються на диску або резервному носії. Наприклад, Усі дані, які зберігає Google, шифруються на рівні зберігання за допомогою алгоритму Advanced Encryption Standard (AES) AES-256. Ми використовуємо загальну криптографічну бібліотеку Tink, яка включає наш перевірений модуль FIPS 140-2.
- Шифрування в пересиланні (in transit) – захист даних під час передачі даних між користувачем і серверами, використовується шифрування TLS/SSL для захисту від перехоплення та несанкціонованого доступу до даних і S/MIME часто використовується для шифрування повідомлень електронної пошти.
- Моніторинг та аудит – ведення систем моніторингу для виявлення незвичайної активності та аудиту подій для визначення хто і що робив в системі. Нагляд 24/7 для глобальної підтримки, керування та відстеження доступу до центру обробки даних,.
- Захист від атак – розробка заходів для запобігання та виявлення атак, таких як DDoS або SQL-ін'єкції, для забезпечення неперервності роботи та цілісності даних.
- Резервне копіювання та відновлення – розробка стратегій резервного копіювання та відновлення для забезпечення можливості відновлення даних у випадку аварій чи втрати інформації.
- Дотримання стандартів безпеки – використання та дотримання міжнародних стандартів безпеки для забезпечення відповідності вимогам та стандартам безпеки даних. У разі пожежі чи будь-яких інших збоїв компанії автоматично й плавно переносять доступ до даних в інший центр обробки даних, щоб користувачі могли продовжувати роботу без перерв. Аварійні резервні генератори продовжать живити центри обробки даних навіть у разі збою електроживлення. Безперервность бізнесу Google підтверджується сертифікацією ISO 22301:2019.
- Фізична безпека дата-центрів – Google дотримується високих стандартів фізичної безпеки в своїх дата-центрах, включаючи контроль доступу, відеоспостереження та інші заходи для запобігання фізичним загрозам.

Ці аспекти допомагають створити повноцінну інформаційну модель, яка забезпечить високий рівень безпеки в хмарному сховищі.