УДК 514.18 : 004.056

# ЗБЕРІГАННЯ ГРАФІЧНОЇ ІНФОРМАЦІЇ В ХМАРІ

Гумен О.М., д.т.н.,
Сич Д.А., студент.
*Національний технічний університет України*
*«Київський політехнічний інститут імені Ігоря Сікорського»*
*(Україна, м. Київ)*

***Анотація*** *– у статті йдеться про хмару як онлайн місце для надійного зберігання з легким доступом до нього. Хмарні системи є відносно недорогим та зручним способом зберігання даних та управління ними з мінімальними витратами. Є великий вибір хмарних сервісів, вони володіють вбудованими засобами аварійного відновлення та доступні в будь-який час та в будь-якому місці. Рекомендується шифрування даних, щоб збереження на віддалених серверах було безпечним. Розглядається широкий асортимент форматів для зберігання, а також стиснення – без втрати та з втратою якості графічної інформації в хмарі.*

***Ключові слова*** *– безпечна хмара, формати графічних файлів, зберігання графічної інформації.*

**Постановка проблеми.** Усю кількість зображень, що використовуються на комп'ютерах, можна розділити на три великі групи. Насамперед, 2D-графіка. До цієї групи відносяться растрова та векторна графіка. Потім 3D-графіка та анімаційна графіка. Для зберігання таких зображень на сьогодні є лише два способи – офлайн і онлайн. Актуальною в наш час є проблема безпечного збереження файлів з легким доступом, вибір зручної програми для шифрування, а також хмари та формату.

**Аналіз останніх досліджень.** Історія персональних хмарних сховищ почалася ще в 2007 році, коли Дрю Х'юстон, генеральний директор Dropbox, втомився постійно губити свій USB-накопичувач. Таким чином, він створив перший індивідуальний хмарний сервіс зберігання даних для малого бізнесу [1]. Це була радикальна ідея свого часу, і всім вона сподобалася. Сьогодні існують десятки дешевих або безкоштовних сервісів хмарного сховища. Але – окрім того, що всі вони надають послуги зі зберігання даних – вони дуже різняться. Сьогоденна проблема користувачів є неправильне налаштування хмари та бази даних, що загрожує їх безпеці. Зокрема після цього їх можна легко знайти за допомогою інструментів для Інтернет-сканування [2]. Ситуація погіршується через використання складних корпоративних хмарних середовищ. Більшість організацій поєднують локальні та загальнодоступні чи приватні хмари, при цьому використовуючи рішення різних

постачальників, щоб мінімізувати ризики компрометації [3]. За даними нещодавнього звіту, 92% користувачів використовують мультихмару, а 82% – гібридну хмару [4].

**Формулювання цілей (постановка завдання).** ІТ-спеціалістам складно підтримувати належну функціональність рішень різних постачальників хмарних послуг. Зокрема виникають труднощі у розробників, які часто не мають спеціальної підготовки з питань безпеки. Тому метою даного дослідження є хмара як онлайн місце для безпечного збереження графічної інформації у відповідному форматі.

**Основна частина.** Під час проведення досліджень, спираючись на власний досвід та інформаційні джерела, було виділено основні поради в роботі з хмарою:

1. Формати графічного файлу та при необхідності їх стиснення.
2. Шифрування інформації.
3. Сервіси для збереження даних.

Під форматом графічного файлу слід розуміти сукупність інформації про зображення та спосіб її запису у файл. Загалом усі графічні формати можна розділити на дві групи. Формати загального призначення містять лише саме зображення та призначені для зберігання, перенесення або перегляду зображень (gif, tiff, jpeg та ін.) та специфічні формати, призначені для зберігання проміжних результатів редагування зображень (cdr, cpt, psd, ai та ін.).

Стиснення файлів. Оскільки графічні файли, як правило, мають великий розмір, корисною є можливість стиснення (упаковки) інформації. В даний час відомі два способи стиснення – без втрати та з втратою якості. Алгоритми стиснення без втрат аналогічні алгоритмам стандартних архіваторів (LZH, PKZIP, ARJ). Найвідоміший із них LZW (LZ84) широко використовується в популярних растрових форматах GIF, TIFF. Алгоритми стиснення із втратою якості відкидають інформацію, що не сприймається людиною (JPEG, PCD). Ступінь упаковки в цьому випадку набагато вищий, але відбувається повільніше і може призвести до погіршення якості (залежно від обраного ступеня стиснення). Головний недолік цього алгоритму полягає у неможливості перестискання без значної втрати вихідної якості зображення.

Шифрування, яке застосовуватиметься до файлів на нашому боці, і вже в зашифрованому вигляді дані відправлятимуться в хмару, гарантуючи, що тільки ви зможете розшифрувати ваші файли. Ні хмарному провайдеру, ні зловмисникам не буде доступний вміст ваших файлів.

Для організації процесу локального шифрування і завантаження на віддалений сервіс існує кілька пропозицій, тому кожен може обрати ту програму, яка більш підходить для постійного використання. Наприклад: Veracrypt, Boxcryptor, Cryptomator. Шифрування в рази знижує ризик того, що хтось сторонній отримає доступ до вмісту ваших файлів, оскільки в

разі використання надійного алгоритму і ключа шифрування розшифрувати дані, а відповідно і використати, на сьогодні практично неможливо.

Тримати інформацію на веб-сховищі надійніше. Якщо раптом злетіла оперативна система, зламався вінчестер або просто користувач купив новий лептоп – не важливо – в такому сервісі для зберігання даних все залишиться.

Але хмар в Інтернеті багато. Одні з найбільш популярних (рис. 1):

1. Amazon Drive
2. OneDrive
3. Box
4. Dropbox
5. Google Drive
6. Nextcloud
7. pCloud

Рис. 1. Логотипи хмар

Підсумуємо:

- Універсальний офіс / хмара / робочий процес: Box, Google Drive, Nextcloud або OneDrive
- Користувачі Apple: Dropbox або Google Drive
- Простота використання та декілька пристроїв: Dropbox
- Користувачі Google: Google Drive
- Користувачі Linux: Nextcloud
- Конфіденційність: pCloud
- Користувачі, які високо цінують контроль даних: Box або Nextcloud
- Користувачі Windows: OneDrive

**Висновки.** Існує дуже багато безкоштовних та недорогих сервісів, що надають послуги хмарного сховища, використання яких є досить зручним і практичним. Забезпечується постійний доступ з будь-якого пристрою там, де є Інтернет. Не доводиться хвилюватись про те, що флешка або диск будуть загублені чи вийдуть з ладу. Також потрібно пам'ятати про шифрування файлів, що допомагає надійно зберігати графічну інформацію. Тому майбутнє за хмарним зберіганням.

***Бібліографічний список***

1. https://www.unian.ua/techno/zberigannya-danih-kompaniy-u-hmarnomu-shovishchi-naskilki-ce-narazi-bezpechno-11812803.html
2. https://cybercalm.org/novyny/najkrashhi-hmarni-shovishha-2021-roku-porivnyannya-i-tsini
3. https://androidas.ru/formats-of-storage-of-graphic-information-graphic-file-formats
4. https://imi.org.ua/advices/bezpechna-hmara-pravyla-zberigannya-informatsiyi-dlya-medijnykiv-i39936