УДК 004.056

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ВИКОРИСТНЯ ХМАРНИХ СХОВИЩ ДЛЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Ориник С., Ящук В.
Львівський державний університет безпеки життєдіяльності, м. Львів

Проаналізовано переваги та розглянуто основні тенденції розвитку та впровадження хмарних сховищ. Окреслено характерні ознаки розвитку технології «хмарних обчислень» та визначено головні переваги та недоліки «хмарних» рішень для українських підприємств. Описано принципи та основні вимоги до хмарних сховищ, як сервісу для зберігання та оброблення інформації користувачів. Запропоновано основні правила щодо забезпечення безпеки користування хмарними технологіями.

Ключові слова: *хмарні технології, хмарні сервіси, забезпечення безпеки, інтернет-технології.*

The advantages are analyzed and the main tendencies of development and introduction of cloud storage are considered. The characteristic features of the development of "cloud computing" technology are outlined and the main advantages and disadvantages of "cloud" solutions for Ukrainian enterprises are identified. The principles and basic requirements for cloud storage as a service for storing and processing user information are described. The basic rules for ensuring the safety of using cloud technologies are proposed.

Keywords: *cloud technologies, cloud services, security, Internet technologies.*

Створення нового покоління центрів обробки даних, в яких архітектурна концепція дозволяє зменшити витрати на обчислювальні потужності, ресурси зберігання даних і мережеві ресурси можливо досягнути, використавши концепцію «хмарних обчислень». Сьогодні найпопулярнішими хмарними сховищами є Dropbox, Google Drive (Google Диск), Microsoft OneDrive та ICloud для користувачів технікою Apple. Існують також інші, маловідомі, хмарні сховища даних, та технологія роботи у них приблизно однакова. Важливим питанням є захищеність даних Dropbox, Google Диска чи Microsoft OneDrive, а доступ до них простий та зрозумілий.

Хмарні сховища сьогодні - це зручний сервіс для зберігання та оброблення будь-якої інформації користувачів, що тісно інтегровані в настільні ПК і мобільні операційні системи на смартфонах. На сьогоднішній день активно використовуються захищені браузери для підключення до хмарних технологій. Щодня здійснюється синхронізація з хмарою і зберігається в ній велика кількість фотографій, відео, документів, музики та навіть паролі, збережені в інших сервісах. Розвиток інтернет-технологій позбавив необхідності використання зовнішніх носіїв для збереження великого обсягу даних або обміну файлами. Тепер ці функції делеговані хмарним сховищам.

Принцип роботи будь-якого «хмарного» сховища такий: на персональний комп'ютер або ноутбук ставиться програма-клієнт «хмарного» сховища, прописується шлях до папок розташованим на жорсткому диску, які планується помістити в «хмару». Програма-клієнт копіює інформацію з зазначених папок в сховище, і в подальшому відстежує будь-які зміни в цих папках і автоматично вносить корективи в «хмарне» сховище даних.

При зміні файла, що зберігається в «хмарі», програма внесе правки в копії файлів на комп'ютері. Такий підхід дозволяє мати актуальний набір файлів на будь-якому з пристроїв (смартфоні, комп'ютері, планшеті тощо). Єдина умова, яку потрібно забезпечити для безперебійної роботи сховища з файлами комп'ютера - повна синхронізація. При включенні ПК потрібно дочекатися, поки пройде синхронізація даних. Швидкість здійснення даного процесу багато в чому залежить від швидкості з'єднання з інтернетом. Якщо вимкнути пристрій передчасно, можлива помилка синхронізації даних хмарного сховища.

Володіти доступом до усіх даних з будь-якої точки планети та з будь-якого доступного пристрою є великою перевагою. Але це також відкриває великі можливості для тих, хто так само може отримати файли — для кіберзлочинців.

Наведемо основні правила щодо забезпечення безпеки користування хмарними технологіями:

1. Слід використовувати надійні паролі та двофакторну (чи багатофакторну) аутентифікацію. Обирати довгі й унікальні паролі, які важко відгадати та користуватись менеджером (генерація, зберігання і управління).

2. Перевірка файлів та загальних папок. Сервіси хмарного зберігання підходять для обміну файлами з іншими людьми — від членів сім'ї до колег по роботі, але вони можуть залишити дані відкритими для несанкціонованого доступу. Якщо хтось знайде ці посилання, то зможе отримати доступ до облікового запису людини, з якою ви поділились цими файлами.

3. Необхідно очистити "вже видалені" файли. Багато хмарних сервісів зберігання використовують так звану корзину, зберігаючи протягом певного часу видалені файли на випадок, якщо виникне потреба їх відновити. Необхідно впевнитися, що важливі конфіденційні файли будуть цілком знищені та ніхто більше не зможе їх відновити.

4. Перевіряйте підключені додатки та облікові записи. Навіть, якщо хакери не зможуть увійти у облікові записи звичними способами, вони можуть спробувати отримати доступ "через бокове вікно з двору" — наприклад, з допомогою іншого облікового запису, що підключений до вашого поточного хмарного сховища.

5. Увімкніть сповіщення та повідомлення про дії в акаунті. Більшість хмарних сервісів зберігання даних можуть відправляти вам сповіщення про різні події в обліковому записі, такі як нові входи, зміни в файлах та доступі до них. Тому важливо переконатися, що ці сповіщення увімкнені.

6. Необхідно деактивувати старі пристрої, на яких все ще є доступ до акаунту. Більшість хмарних сервісів зберігання дозволяють синхронізувати файли з декількома пристроями, тому, якщо оновлюєте (або купуєте новий) телефон чи користуєтесь новим ноутбуком, важливо правильно вимкнути та деактивувати старі пристрої.

7. Виходити з облікових записів, якщо не працюєте в них. Для зручності ми не виходимо з облікових записів хмарного сховища навіть коли не працюємо в них. Проте, коли ми закінчуємо в них працювати, важливо вийти з системи, щоб ніхто інший не отримав доступу до ваших файлів.

8. Захистити свої пристрої так добре, як і акаунти. Фізична безпека також важлива. Тримайте телефони, ноутбуки та інші пристрої, на яких користуєтеся обліковими записами хмарних сховищ, захищеними від стороннього доступу.

Хмарне сховище даних - це віртуальний носій інформації, який зберігає і обробляє дані на численних серверах, розкиданих у всесвітній павутині. Причин для розміщення даних в хмарі може бути досить багато, і для різних користувачів вони можуть мати різний пріоритет. Наприклад, для приватних осіб важливіша буде можливість доступу до даних з різних місць інтернету і з різних пристроїв, а для корпоративних користувачів більш істотними можуть виявитися надійність і вартість зберігання.

Література

1. Безпека хмарних сховищ і технологій. Основні правила. 25 August 2020 [Електронний ресурс] – Режим доступу:https: //datami.ua/bezpeka-hmarnih-shovishh-i-tehnologij-osnovni-pravila/https://datami.ua/bezpeka-hmarnih-shovishh-i-tehnologij-osnovni-pravila/.
2. Як забезпечити захист інформації та інформаційну безпеку конфіденційних даних, використовуючи хмарні технології [Електронний ресурс] – Режим доступу: http://www.dut.edu.ua/ua/news-1-569-9733-yak-zabezpechiti-zahist-informacii-ta-informaciynu-bezpeku-konfidenciynih-danih-vikoristovuyuchi-hmarni-tehnologii_kafedra-cistem-tehnichnogo-zahistu-informacii
3. Ящук В. І. Тренди використання технології «хмарних обчислень» в ІТ-сфері України / В. І. Ящук // Торгівля, комерція, підприємництво : збірник наукових праць / [редакц. кол.: Апопій В. В., Дайновський Ю. А., Скибінський С. В. та ін.]. – Львів : Львівська комерційна академія, 2012. – Вип. 14. – С. 104-108.
4. Що таке хмарні сховища та як вони працюють 10 Вересня, 2021 [Електронний ресурс] – Режим доступу:https: https://info.nic.ua/uk/blog-uk/cloudstorage-2/
5. Хмарні сховища [Електронний ресурс] – Режим доступу: https://sites.google.com/site/karnasiyk1course/home/hmarni-shovisa.
6. Хмарне зберігання даних. 7 квітня 2020 [Електронний ресурс] – Режим доступу: https://compbest.com.ua/ua/oblachnoe-khranenie-dannykh/.