Сухіх А. С.,
канд. пед. наук,
старший науковий співробітник
відділу хмаро орієнтованих систем інформатизації освіти,
Інститут цифровізації освіти НАПН України, м. Київ

ОСОБЛИВОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ ВИКОРИСТАННІ ХМАРНИХ СЕРВІСІВ

Процеси цифрової трансформації відбуваються у різних сферах суспільної діяльності, тому використання хмарних середовищ з кожним роком стає більш популярним, а в деяких галузях хмарні технології стають необхідною умовою для повноцінного функціонування систем.

На прикладі хмарних технологій у середовищі Google (рис.1) можна ознайомитися з основними складниками та послугами, що надаються хмарними системами.

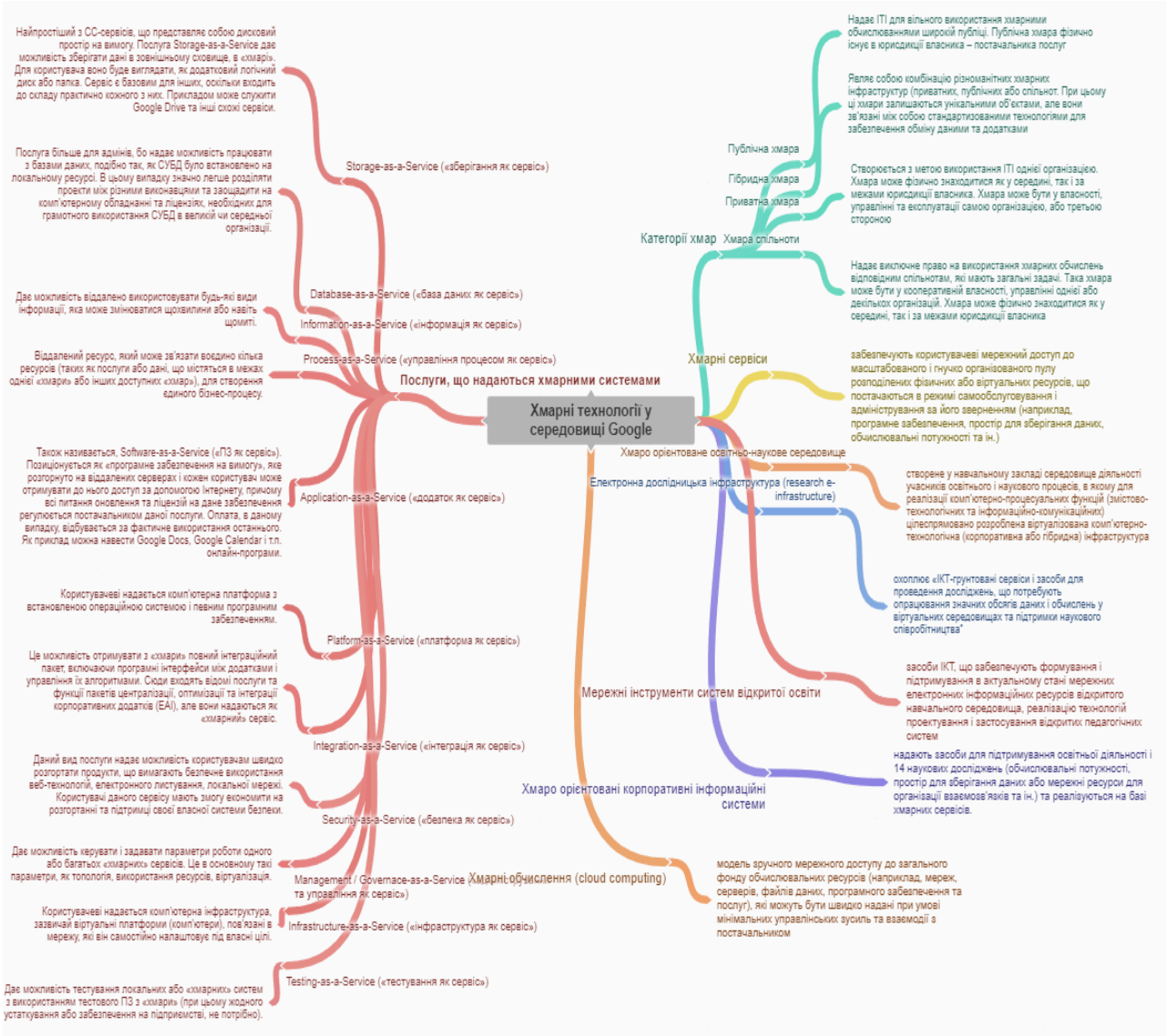

Рис. 1. Хмарні технології у середовищі Google [1]

Хмарні технології є зручним способом зберігання даних та управління ними, що доступні у будь-який час та у будь-якому місці. Однак зберігання будь-яких даних у хмарі потребує їх захисту, тому потреба у забезпеченні інформаційної безпеки та захисту

інформації, що циркулює у хмарній інфраструктурі від внутрішніх та зовнішніх загроз є важливою задачею.

Безпека призначена для захисту усіх фізичних мереж, зокрема маршрутизаторів, електричних систем, даних, накопичувачів, серверів, програм, операційних систем, а також програмного й апаратного забезпечення. Існують певні відмінності між поняттями "безпека хмари" та "безпека у хмарі". Вперше різниця була сформульована Amazon для роз'яснення спільної відповідальності постачальників та користувачів. За безпеку хмари відповідальними є постачальники хмарних послуг, які зазвичай відповідають за фізичну та мережеву інфраструктуру хмарної служби, а користувачі - за налаштування доступу, встановлення паролів та інші питання, які не залежать від сервіс-провайдера [2].

Основними ризиками для користувачів хмарних технологій з точки зору інформаційної безпеки є:

- отримання несанкціонованого доступу до системи;
- блокування доступу до програмного забезпечення, ключів доступу, окремих файлів;
- порушення цілісності інформаційного масиву, що зберігається в хмарі;
- обмеження використання програми через проникнення в систему вірусів, хакерських програм;
- збої в технічному обслуговуванні системи.

Для захисту розміщення даних у хмарних середовищах необхідною умовою є дотримання вимог безпеки, а саме:

1. Використання надійних паролів та двофакторної (чи багатофакторної) аутентифікації.
2. Перевірка файлів та загальних папок.
3. Перевірка підключених додатків та облікових записів.
4. Надання іншим користувачам доступу до потрібних їм ресурсів лише з мінімальними правами.
5. Захист апаратних засобів.

На думку експертів та за даними аналітичних компаній, світовий ринок хмарних послуг продовжує динамічно рости – приблизно на 15-20 % щорічно. У звіті Cloud Security Alliance «Конфіденційні дані у хмарі» [3] зазначено, що 89 відсотків опитаних компаній зберігають конфіденційні дані у хмарі. При цьому 67 відсотків з них розміщують конфіденційні дані у публічних хмарах, а 45 відсотків – у приватних. Згідно з поданою інформацією у звіті, лише 4 % опитаних експертів з IT та безпеки вважають, що дані, які зберігаються в хмарі, належним чином захищені.

Потрібно розмежовувати відповідальність за інформаційну безпеку між постачальниками хмарних послуг та користувачами, знати про ризики та дотримуватися правил безпеки для їх запобігання.

Список використаних джерел:

1. Хмарні технології у середовищі Google. URL: https://cutt.ly/B3B74I3
2. Хмарна безпека: ключові поняття, загрози та рішення – результати дослідження. URL: https://cloudsecurityalliance.org/artifacts/understanding-cloud-data-security-and-priorities/
3. Understanding Cloud Data Security and Priorities in 2022 URL: https://cloudsecurityalliance.org/artifacts/understanding-cloud-data-security-and-priorities/