УДК 004.056.5:004.73](043.2)

Ласкавчук М. А., здобувач вищої освіти;
Загоруйко Л. В., канд. техн. наук, доцент,
доцент кафедри прикладної математики та кібербезпеки,
Донецький національний університет імені Василя Стуса

ОГЛЯД МЕТОДІВ ОБРОБКИ ІНФОРМАЦІЇ ДЛЯ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ У КЕРУВАННІ ХМАРНИМ СЕРВІСОМ

Ключові слова: системи безпеки, засоби захисту, програмні засоби захисту, хмарний сервіс.

Вступ. Забезпечення безпеки у хмарних обчисленнях стає важливим завданням для компаній будь-якого масштабу, оскільки використання хмарних послуг має багато переваг, але включає в себе також значний рівень ризику. Щоб зменшити можливі загрози безпеці, пов’язані з використанням хмарних ресурсів, компанії повинні бути свідомими різних видів ризиків та вміти ефективно ними управляти.

Актуальність. У сучасному світі для підтримки ухвалення рішень у процесі управління хмарним сервісом є надзвичайно важливим, оскільки швидкий розвиток цифрових технологій та збільшення обсягів інформації створюють нові виклики та загрози для безпеки та ефективності операцій.

Під час керування хмарним сервісом безпека та конфіденційність даних є однією з головних проблем у хмарних обчисленнях. Постачальники хмарних послуг повинні забезпечити захист контенту від різних шкідливих програм, і для цього існують різні політики та механізми постачальників хмарних послуг [1].

В узагальненій схемі процесу гарантування безпеки хмарного сервісу можна виокремити кілька множин, незалежно від того, які ресурси надають хмарні платформи (рис. 1) [2–4]:

– існує безліч небезпек, які можуть втілюватися в хмарі $X = \{x_i \mid i = 1, N\}$. Під небезпекою можна розуміти намір особи, що порушує правила з метою завдати фізичної, матеріальної або іншої шкоди, яка призведе до порушення цілісності та конфіденційності інформації;

– кожна загроза може характеризуватися: $P_{заг}$ – імовірністю появи та реалізації *i*-ї загрози; $C_{заг}$ – значущістю під час завдання збитків;

– хмарний сервіс являє собою множину $Y = \{y_j \mid j = 1, L\}$ з низкою сервісів, що надаються. Множина характеризується показниками: $P_{зах}$ – коефіцієнт надійності сервісу або ресурсу, $V_{сер}$ – цінність сервісу, що надається, $H_{рес}$ – коефіцієнт надійності (безвідмовної роботи) апаратних ресурсів для надання сервісів, $S_{рес}$ – коефіцієнт надійності (безвідмовної роботи) програмних ресурсів для надання послуг хмарних сервісів;

– множина користувачів хмарних сервісів $P = \{p_j \mid j = 1,K\}$ (внутрішні, зовнішні користувачі сервісу);

– множина потоків інформації P(N,L), $PL = \{PL_j | \{PL_j | j = 1, M\}, PN = \{PN_j | j = 1,K\}$ (PL – безпечні потоки, PN – потенційно небезпечні потоки інформації, що несуть різного виду загрози безпеці);

– множина доступу $R = \{r_j | j = 1,N\}$(містить монітор безпеки) відповідає за персоніфікованість користувачів, аутентифікацію та ідентифікацію користувачів, здійснює управління доступом і контроль доступу до сервісів з урахуванням розробленої політики безпеки;

– безліч засобів захисту в хмарному сервісі, що надається хмарному сервісі $Z = \{z_k | k = 1,M\}$, які виконують функції виявлення та блокування загрози безпеки хмарної платформи;

– встановлені засоби захисту характеризуються $A_j A_i$ – здатністю протидіяти реалізації загрози, цю функцію в хмарних обчисленнях виконує агент безпеки, який відповідає за моніторинг і адекватність запитів користувачів у системі хмарних обчислень, надає можливі варіанти запитів у разі неправильно обраних дій або спроби несанкціонованого доступу до ресурсів системи хмарних обчислень, так само відповідає за безпечну взаємодію системи загалом.

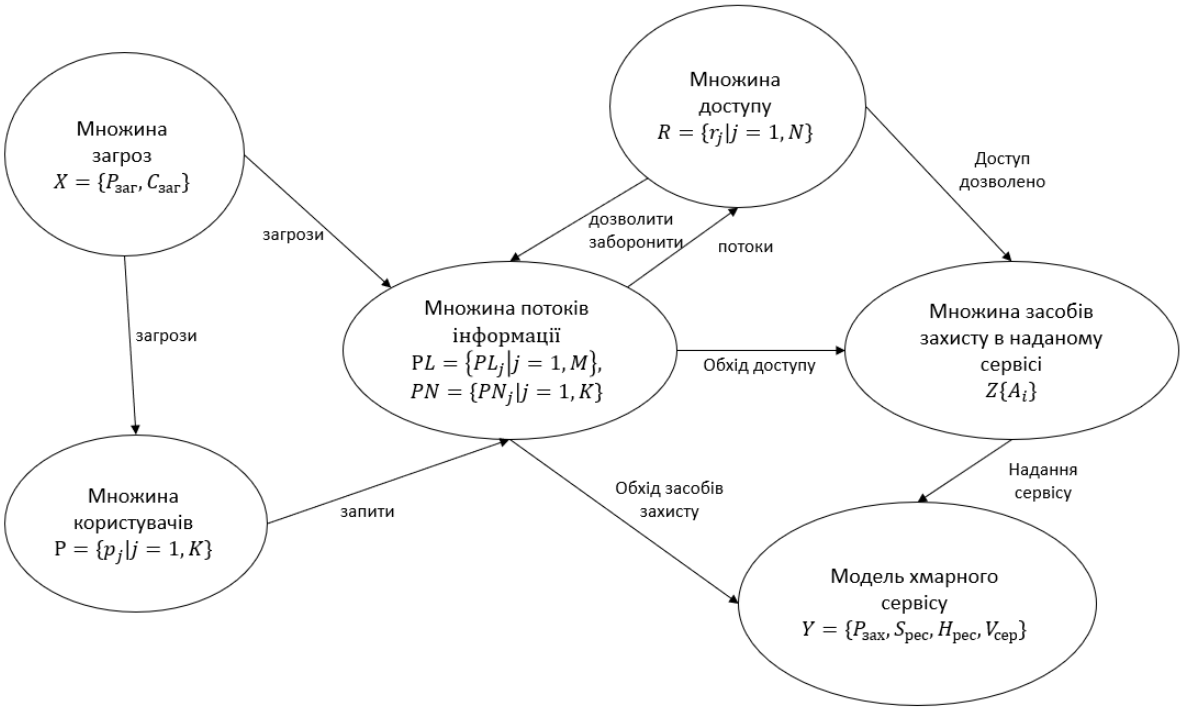

Рисунок 1 – Узагальнена схема процесу забезпечення безпеки хмарного сервісу

Для підтримки прийняття рішень щодо вибору засобів захисту в процесі функціонування хмарного сервісу експертні знання застосовуються для визначення [5]:

– оцінок можливості одержання доступу *i*-го потоку інформації до хмарного сервісу;

– оцінок рівня протидії загрозі, доступу *i*-го потоку інформації до хмарного сервісу;

– оцінок імовірності реалізації *i*-ї загрози в потоці інформації стосовно *j*-го елементу хмарного сервісу;

– оцінок рівня реалізації загрози;
– оцінок ефективності використання засобу захисту.

За отриманими оцінками здійснюється ухвалення рішення щодо вибору засобів захисту для елемента хмарного сервісу. Що вища оцінка, то більша ефективність застосування цього засобу захисту.

Висновки

Наведено узагальнену схему процесу забезпечення безпеки хмарного сервісу. На схемі показано процес взаємодії виділених множин з потоками інформації від кожної множини, схема дає чітке розуміння взаємозв'язку множини користувачів і хмарного сервісу з можливістю обходу різноманітних засобів захисту хмарного сервісу. Зазначена схема також підкреслює важливість прийняття рішень щодо захисту інформації в хмарному сервісі.

Розглянуто процеси прийняття рішень під час керування хмарним сервісом, виділено основні оцінки, за якими здійснюється ухвалення рішень. Для ефективного ухвалення рішень із забезпечення безпеки потрібно уважно аналізувати і враховувати ризики, використовувати відповідні засоби захисту та розробляти стратегії управління ризиками.

Список використаних джерел

1. Cloud computing security challenges URL: https://cutt.ly/EwU6kHNw (дата звернення: 07.11.2023).

2. Хмарні обчислення та безпека хмарних сховищ: як забезпечити безпеку сховищ у хмарі. URL: https://ts2.space/uk/%D1%85%D0%BC%D0%B0%D1%80%D0%BD%D1%96-%D0%BE%D0%B1%D1%87%D0%B8%D1%81%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F-%D1%82%D0%B0-%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0-%D1%85%D0%BC%D0%B0%D1%80%D0%BD%D0%B8%D1%85-4/ (дата звернення: 08.11.2023).

3. What is cloud security? URL: https://www.ibm.com/topics/cloud-security (дата звернення: 08.11.2023).

4. Cloud Data Security: Guidelines to Ensure Strong Protection of Sensitive Data in Cloud Environments. URL: https://gowombat.team/blog/posts/cloud-data-security (дата звернення: 08.11.2023).

5. Підтримка прийняття рішень про реалізацію додатків в гібридній хмарній інфраструктурі / Л. А. Волощук, О. І. Розновець, Д. Д. Волощук. Одеський національний університет імені І. І. Мечнікова. 2018. URL: http://immm.op.edu.ua/files/archive/n1_v8_2018/2018_1(9).pdf (дата звернення: 08.11.2023).