Секція 1

ОРГАНІЗАЦІЯ ЗАХИСТУ ХМАРНОГО СЕРЕДОВИЩА

Даценко В. А.
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»
Науковий керівник Землянко Г. А.

Актуальність. Хмарні середовища – це зручний сервіс для зберігання та обробки будь-якої інформації користувачів, що тісно інтегровані в сучасні пристрої, це забезпечує доступ до даних і передових обчислювальних ресурсів де завгодно [1]. Проте захист інформації від несанкціонованого доступу, безпека використання хмарних технологій та передбачення ймовірних ризиків, що виникають у процесі їх використання, є пріоритетним напрямком у повсякденні.

Мета. Аналіз технологій захисту інформаційних ресурсів при використанні хмарних технологій.

Основні положення. Хмарна безпека, також відома як безпека хмарних обчислень, складається з набору політик, засобів керування, процедур і технологій, які працюють разом для захисту хмарних систем, даних та інфраструктури від загроз та кібератак.

Компанії хмарних послуг забезпечують комплексний багаторівневий захист, що включає: системи керування доступом, постійний моніторинг загроз, шифрування даних під час передачі та зберігання, захист фізичних центрів обробки даних; захист мережі, захист програм, резервне копіювання даних, постійні перевірки, захист від масового видалення файлів та моніторинг підозрілих дій під час входу [2].

Найбільш ефективні способи захисту у сфері безпеки хмар опублікувала організація Cloud Security Alliance (CSA) [3]. Проаналізувавши матеріли, було виявлено такі рішення:

1. Збереження даних. Шифрування – один із найефективніших способів захисту даних. Провайдер, що надає доступ до даних, повинен шифрувати інформацію клієнта, що зберігається в ЦОД, а також у разі відсутності необхідності безповоротно видаляти.
2. Захист даних під час передачі. Зашифровані дані під час передачі повинні бути доступні лише після аутентифікації. Дані не вдасться прочитати або зробити зміни, навіть у разі доступу через ненадійні вузли. Для цього використовуються провайдерами такі технології: протоколи AES, TLS, IPsec та інші.

3. Аутентифікація – захист паролем. Для забезпечення більш високої надійності використовують такі засоби, як токени та сертифікати. Для прозорої взаємодії провайдера з системою ідентифікації при авторизації також рекомендується використовувати протоколи LDAP та SAML.
4. Ізоляція користувачів. Використання індивідуальної віртуальної машини та віртуальну мережу. Віртуальні мережі повинні бути розгорнуті із застосуванням таких технологій, як VPN, VLAN та VPLS. Часто провайдери ізолюють дані користувачів один від одного за рахунок зміни даних коду в єдиному програмному середовищі [4].

Висновки. Найдієвішими технологіями захисту інформаційних ресурсів при використанні хмарних середовищ на сьогодні є: шифрування, захист даних при передаванні, аутентифікація та ізоляція користувачів. Засоби безпеки потребують постійного вдосконалення і передбачання ризиків, що виникають у процесі користування. Хмарні технології постійно розвиваються, витісняють інші та закорінюються в IT-індустрії, а отже питання безпеки у цьому середовищі завжди актуальне, тому на часі є розробка та впровадження нових методів захисту інформації у хмарі.

Список літератури

1. Безпека хмарних сховищ і технологій: Основні правила. *Datami*. URL: https://datami.ua/bezpeka-hmarnih-shovishh-i-tehnologij-osnovni-pravila/ (дата звернення: 17.11.2022).
2. Paul Diamond. Хмарне сховище чи локальні сервери: 9 критеріїв, які слід врахувати під час вибору. *Microsoft*. URL: https://www.microsoft.com/uk-ua/microsoft-365/business-insights-ideas/resources/cloud-storage-vs-on-premises-servers (дата звернення: 18.11.2022).
3. Guideline on Effectively Managing Security Service in the Cloud. *Cloud Security Alliance*. URL – https://cloudsecurityalliance.org/artifacts/guideline-on-effectively-managing-security-service-in-the-cloud/ (дата звернення: 20.11.2022).
4. Загрози хмарних обчислень та їх методи захисту. *Habr*. URL: https://habr.com/ru/post/183168/ (дата звернення: 26.11.2022).

Відомості про авторів

Даценко Владислав Анатолійович, бакалавр кафедри комп'ютерних систем, мереж і кібербезпеки, v.datsenko@student.csn.khai.edu
Землянко Георгій Андрійович, асистент кафедри комп'ютерних систем, мереж і кібербезпеки, g.zemlianko@csn.khai.edu