УДК 004.75:004.05

А.В. КОЗИКОВ, ст. викладач, К.С. РОСОХАТИЙ, студент,
Криворізький національний університет

БЕЗПЕКА ХМАРНИХ ОБЧИСЛЕНЬ

Збільшення популярності хмарних обчислень посилило попит на її використання. Згідно з даними Міжнародної компанії IDC і дослідженням Forbes, в 2018 році сумарні витрати організацій на інфраструктуру і послуги, пов'язані з хмарними обчисленнями, досягли рівня $ 154 млрд. Подібна популярність технології, перш за все, обумовлена її функціональністю, яка надає не тільки широкі можливості для обробки і зберігання даних, але і є способом уникнути витратних інвестицій. У зв'язку з актуальністю цієї технології необхідно зосередити увагу на її переваги і недоліки, особливе місце займає питання безпеки.

Згідно з визначенням NIST, хмарні обчислення представляють собою модель повсюдного та зручного мережевого доступу на вимогу до загального пулу конфігуруємих обчислювальних ресурсів (наприклад, мереж передачі даних, серверів, пристроїв зберігання даних, додатків і сервісів - як разом, так і окремо), які можуть бути оперативно надані і звільнені з мінімальними експлуатаційними витратами і / або зверненнями до провайдера.

Існує три моделі надання послуг хмарних обчислень (SaaS - Software-as-a-Service, PaaS - Platform-as-a-Service, IaaS - Infrastructure-as-a-Service) і чотири моделі розгортання (Public Cloud, Private Cloud, Community Cloud, Hybrid Cloud). Незалежно від моделі хмарні обчислення характеризуються рядом загальних переваг: можливістю спільного доступу до ресурсів і послуг, гнучкістю управління послугами та можливістю динамічного масштабування ресурсів, зручною системою оплати використовуваних сервісів (pay-per-usage model) [1-4].

Але є проблемні сторони даної технології. Головне місце займає безпека. Порушення функціонування хмари може бути спровоковано атаками зловмисників так і збоями самої хмарної інфраструктури. Головною проблемою в безпеці є втрата даних. Певні рішення в даних складнощах вносить відсутність стандарту безпеки хмарних обчислень. В більшості випадків безпека в хмарі досягається за рахунок контролю третьої сторони, або реалізацією провайдерами хмарних сервісів своїх власних стандартів і моделей безпеки.

Загрози безпеці хмари відрізняються в залежності від моделі надання послуг. Існують типи загроз, які є загальними для всіх моделей. Їх можна класифікувати за впливом на ознаки, що характеризують дані і послуги хмарних обчислень: конфіденційність (Загроза доступу зловмисних інсайдерів до призначених для користувача даних, що зберігається в хмарі; загроза несанкціонованого доступу до даних; загроза компрометації або несправності апаратного забезпечення), цілісність (надання частини користувачів в рамках однієї інфраструктури несправних або неправильно сконфігурованих компонент), доступність[3].

Статистика загроз і аналіз ринку хмарних обчислень показують, що актуальність вироблення методів і розробки засобів захисту хмарного середовища дуже висока. Однак на сьогоднішній день єдиного механізму і єдиної моделі захисту хмар від існуючих загроз (аномалій) безпеки немає.

Одним з підходів забезпечення безпеки хмарної середовища є використання розподіленої системи моніторингу і виявлення вразливостей[2]. Таке рішення характеризуються розподіленістю і самоорганізацією, що адаптує їх для роботи в хмарному середовищі.

Однак проблемною стороною в питанні використання подібної системи є оцінка її ефективності, оскільки багаторівнева структура середовища вносить складності в використання стандартних методів оцінки.

Список літератури

1. Облачный провайдинг 2015-2020: экономика, стратегии, бизнес-модели. [Електроний ресурс]. – Режим доступу: http://www.iksmedia.ru/news/ 5331917-Novyj-otchet-iKSConsulting-oblachny.html.

2. Security and Privacy Issues in Cloud Computing. Jaydip Sen [Електроний ресурс]. – Режим доступу: https://arxiv.org/ftp/arxiv/papers/1303/ 1303.4814.pdf.

3. Хмарні технології. Переваги і недоліки. [Електроний ресурс]. – Режим доступу: https://valtek.com.ua/ua/system-integration/it-infrastructure/clouds/cloud-technologies.

4. Grace Lewis, Basics About Cloud Computing. Software Engineering Institute, Carnegie Mellon University [Електронний ресурс]. – Режим доступу: http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=28873.