Забезпечення міжкінцевої безпеки автоматизованої мультихмари

Лемешко В.О.[1], *студент гр. ТРІКІ-20-1*;
Персіков М.А.[2], *студент гр. Е-94*
[1]Харківський національний університет радіоелектроніки,
[2]Харківський патентно-комп'ютерний коледж, м. Харків, Україна

Технологічне завдання розгортання та забезпечення ефективного функціонування мультихмари (multi-cloud), що не залежить від місця знаходження користувача та програми чи сервісу, що надається множиною незалежних провайдерів (Cloud Service Providers), є актуальним і потребує системного рішення [1]. Зазначається, що незалежно від того, який тип хмар використовується – публічна, приватна чи гібридна (AWS, Azure, edge cloud тощо), політики та контроль мультихмарою повинні бути розподіленими рівномірно [2].

Отже, мультихмарному середовищу необхідна міжкінцева (наскрізна) оркестрація, абстрагована від базових ресурсів, що дозволить операторам зосередитись на головних функціях, а не на семантиці налаштувань. Таким чином, оркестрація є фактично платформою для автоматизації. Крім того, має існувати наскрізний аналітичний рівень, що забезпечуватиме видимість публічних і приватних хмар, фізичних і віртуальних ресурсів, робочіх навантажень на мережу та додатки [1, 2].

Очевидно, що розгортання мультихмари неможливе без наявності вбудованих функцій інформаційної безпеки для забезпечення різноманітного навантаження в будь-якій хмарі, віртуальній машині чи контейнері. Такі політики безпеки повинні бути рівномірно задекларовані та застосовувані. З цього виходить, що інформаційна безпека представляє собою міжкінцеву функцію. Більше того, міжкінцева безпека автоматизованої мультихмари повинна забезпечуватись також зверху вниз: від додатків до фізичних ресурсів.

Керівник: Єременко О.С., *д.т.н., професор*

1. M.V. Kushala, B.S. Shylaja, *Recent Trends on Security Issues in Multi-Cloud Computing: A Survey*, *ICOSEC* (2020).
2. E. Rios, E. Iturbe, et al., *Dynamic security assurance in multi-cloud DevOps*, *CNS* (2017).