МОДЕЛІ ПРЕДСТАВЛЕННЯ, ТИПИ ТА ОСНОВНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ХМАРНИХ ОБЧИСЛЕНЬ

Гришин І.Ю., Скидан Р.А.

Кубанський державний технологічний університет, м. Краснодар

Хмарні обчислення засновані на трьох основних моделях: інфраструктура як послуга (IaaS), платформа як сервіс (PaaS) та програмне забезпечення як послуга (SaaS).

Відповідно до класифікації Національного інституту стандартів і технології США (NIST) виділяються три основних види хмарних обчислень: приватні, гібридні та публічні.

Питання безпеки та конфіденційності є одними з найбільш важливих проблем в області хмарних обчислень, так як велика кількість особового контенту і інші конфіденційні дані розташовуються в хмарі.

Забезпечення безпеки і конфіденційність в цьому контексті вимагає прийняття рішень для захисту, які істотно відрізняються від тих, які передбачені діючими практиками в області забезпечення безпеки в «традиційної інфраструктурі».

У традиційній IT-інфраструктурі організація повністю контролює свою інфраструктуру. Коли інфраструктура організації повністю або частково мігрувала в хмару, то така інфраструктура, включаючи відповідні додатки та збережені дані розташовується в середовищі, яка відокремлена, управляється і підтримується поза організації. Звідси випливає проблема фізичної безпеки інфраструктури, яка розпилюється поза територією організації, і яка може відрізнятись від очікуваної. Для приватної хмарної інфраструктури ризики фізичної безпеки практично аналогічні ризикам, характерним для традиційної інфраструктури.

Безпека і доступність хмарних сервісів – від аутентифікації і управління доступом до шифрування й активності моніторингу – залежить від безпеки API. Ризик збільшується третіми сторонами, які покладаються на API, і на основі цих інтерфейсів розробляють додатки, що надають додатковий функціонал для організації, якій, можливо, буде потрібно надати облікові дані третій стороні. API-інтерфейси та інтерфейси, як правило, в найбільшою мірою схильні до злому і атакам, тому що вони, як правило, доступні з мережі Інтернет.

Перед перенесенням служб, даних й додатків в «хмари», організації повинні чітко розуміти і контролювати питання, які можуть представляти будь-які потенційні ризики, пов'язані з використанням середовищ хмарних обчислень. Безпека і конфіденційність питань безпеки, загроз й вразливості можуть бути різними для різних типів розгортання хмарних моделей.