ХМАРНІ ТЕХНОЛОГІЇ ТА ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Грішин І.Ю., Рябов А.М.
Кубанський державний технологічний університет, м. Краснодар

В роботі розглянуті різні види загроз хмарних обчислень, а також проведено аналіз можливих видів атак на елементи хмари і рішення щодо протидії таким атакам.

Хмарні обчислення – технологія розподіленої обробки даних, в якій комп'ютерні ресурси і потужності надаються користувачеві як Інтернет-сервіс. Застосування хмарних технологій призвело до нових загроз інформаційної безпеки, що вимагає додаткового опрацювання особливостей хмарних обчислень з метою виявлення вимог до системи їх інформаційного захисту.

В даний час на ринку представлений широкий спектр пропозицій для захисту серверів і центрів обробки даних (ЦОД) від різних загроз. Вони об'єднані орієнтованістю на вузький спектр вирішуваних завдань. Але він зазнав значного розширення внаслідок поступового витіснення класичних апаратних систем віртуальними платформами. До загальновідомих типів загроз (мережеві атаки, уразливості в додатках операційних систем, шкідливе програмне забезпечення) додалися проблеми, пов'язані з контролем середовища (гипервизора), трафіку між гостьовими машинами та розмежуванням прав доступу. Розширилися внутрішні питання і політики захисту ЦОД, а також вимоги зовнішніх регуляторів. Робота сучасних ЦОД в ряді галузей вимагає закриття технічних питань і нюансів, пов'язаних з їх безпекою.

Основні проблеми інформаційної безпеки при використанні хмарних технологій:

– труднощі при переміщенні звичайних серверів в обчислювальну хмару. Вимоги до безпеки хмарних обчислень не відрізняються від вимог безпеки до центрів обробки даних. Але віртуалізація ЦОД і перехід до хмарних середовищ призводять до появи нових загроз;

– динамічність віртуальних машин. Дана мінливість створює додаткові труднощі для забезпечення цілісності системи безпеки;

– вразливість всередині віртуальних середовищ. Для хмарних систем загроза віддаленого злому або зараження шкідливим програмним забезпеченням істотно підвищується;

– захист бездіяльних віртуальних машин. При використанні хмарних обчислень периметр мережі розмивається або зовсім зникає. Для розмежування сегментів з різними рівнями довіри в хмарі віртуальні машини повинні самостійно забезпечити себе захистом, переміщаючи мережевий периметр до самої віртуальної машині.