Вакалюк Т. А., д-р.пед.наук, проф., професор кафедри ІПЗ,
Гнип М. В., магістрант групи ІСТм-20-1
Державний університет «Житомирська політехніка»

ОРГАНІЗАЦІЯ ЗАХИСТУ ХМАРНОГО СЕРЕДОВИЩА

Усуваючи проблеми масштабованості, хмарні обчислення забезпечують практично необмежену потужність. Вони надають розробникам доступ до апаратних та програмних активів, які більшість користувачів малого і навіть середнього бізнесу не змогли б собі дозволити.

Для виконання хмарних обчислень використовують центри обробки даних (ЦОД), що являють собою сукупність серверів, які розміщені на одному майданчику. Метою створення ЦОД є підвищення ефективності та захищеності. Для захисту центрів обробки даних використовується мережевий та фізичний захист. Крім того, важливо забезпечити відмовостійкість і надійне електроживлення ЦОДу. На даний момент ринок багатий рішеннями щодо захисту серверів і ЦОД від різноманітних заг-роз, які об'єднує орієнтованість на конкретні задачі. Проте, кількість цих завдань значно збільшилась внаслідок поступової заміни апаратних систем, що вважались класичними, на віртуальні платформи. У зв'язку з цим, до вже відомих типів загроз додалися складності, пов'язані з контролем хмарного середовища, трафіку між гостьовими машинами та розмежуванням прав доступу. З'явились більш суворі вимоги зовнішніх регуляторів, а також розширилися внутрішні питання щодо політики захисту ЦОД. На сьогодні до роботи ЦОД висуваються суворі вимоги щодо закриття технічних питань та питань, пов'язаних з їх безпекою. Наразі практично всі компанії, що використовують дані системи, на серйозному рівні зайнялися питаннями посилення безпеки в них, хоча ще декілька років назад інтерес був лише теоретичний. Особливо гостро питання безпеки постають для бізнес-систем та додатків.

Головною причиною масштабного перенесення більшості систем на хмарні сервіси стала віртуалізація. Звісно ж, разом з цим, постає ряд завдань щодо забезпечення безпеки в новому середовищі. Це вимагає особливого підходу. Більшість загроз вже достатньо вивчені та для них розроблені заходи протидії. Однак, слід провести адаптацію цих заходів для використання в хмарному середовищі.

Одною з перших проблем з безпеки, яка виникає – це контроль та управління хмарними сервісами. Адже відслідкувати всі ресурси сервісів, віртуальних машин, процесів – досить важка справа. Даний тип загроз є високорівневим, так як він пов'язаний з керуванням безпосередньо хмарним середовищем, як єдиною інформаційною системою, отже для нього необхідно налагоджувати індивідуальну систему захисту. Для цього використовують модель управління ризиками для хмарних інфраструктур.

За основу забезпечення фізичної безпеки взятий суворий контроль фізичного доступу до всіх елементів даної інфраструктури. Основою мережевого захисту є міжмережевий екран та захист від вторгнень. Під використанням міжмережевого екрану розуміють роботу з фільтрації, метою якої є розмежування внутрішніх мереж ЦОД на підмережі з різним рівнем довіри.

До наявних атак на хмарне середовище відносять наступні:

- традиційні атаки на програмне забезпечення;
- функціональні атаки на елементи хмарної інфраструктури;
- атаки, що спрямовані на клієнта хмарного середовища;
- атаки на контролер середовища (гіпервізор);
- атаки на системи керування.

Ефективна архітектура безпеки хмарного середовища має визначати та боротись з цими атаками. Вирішенням проблем безпеки стають такі рішення:

- шифрування даних, що зберігаються;
- захист даних при передачі;
- аутентифікація користувачів;
- ізоляція користувачів один від одного.

Таким чином, хмарні технології – це дуже перспективний напрямок, що постійно розвивається та надає великого прискорення майбутньому вдосконаленню інформаційних технологій. А отже і питання безпеки в цьому середовищі завжди актуальне. Основними способами захисту інформації в хмарних технологіях є: шифрування, поділ даних і аутентифікація. Тільки при належному ставленні до захисту даних у хмарні обчислення можна стверджувати, що дані захищені.

Список використаних джерел

1. Бердник А. Угрозы облачных вычислений и методы их защиты [Електронний ресурс] / Алексей Бердник. – 2013. – Режим доступу до ресурсу: https://habr.com/ru/post/183168/.
2. Маньшин Г. Г. Парадигма безопасности облачных вычислений [Електронний ресурс] / Г. Г. Маньшин, В. А. Артамонов, Е. В. Артамонова // МАИТ. – 2020. – Режим доступу до ресурсу: http://itzashita.ru/oblachnyie-vyichisleniya/paradigma-bezopasnosti-oblachnyih-vyichisleniy.html.