***Ліщинський О.А. магістрант групи ІСТм-21-2,***

*Державний університет «Житомирська політехніка»,*

[*ipzm212\_loa@student.ztu.edu.ua*](mailto:ipzm212_loa@student.ztu.edu.ua)

**ОРГАНІЗАЦІЯ ЗАХИСТУ ХМАРНОГО СЕРЕДОВИЩА**

Усуваючи проблеми з масштабованістю, хмарні обчислення надають майже необмежені можливості. Вони дають розробникам доступ до апаратних і програмних засобів, які не можуть собі дозволити більшість користувачів малого та середнього бізнесу. Хмарні обчислення виконуються за допомогою центру обробки даних (ЦОД), який являє собою групу серверів, розташованих на сайті. Метою створення дата-центру є підвищення ефективності та безпеки. Для захисту ЦОД використовуються мережа та фізичний захист.

Крім того, важливо також забезпечити відмовостійкість і надійне електропостачання ЦОД. В даний час на ринку існує безліч рішень для захисту серверів і центрів обробки даних від різноманітних загроз, і ці рішення поєднують зосередженість на конкретних завданнях. Однак кількість цих завдань значно зросла за рахунок поступової заміни того, що вважається класичною апаратною системою, на віртуальну платформу.

У зв'язку з цим відомі типи загроз ускладнюють контроль над хмарним середовищем, трафіком між гостьовими комп’ютерами та розрізненням дозволів доступу. Більш жорсткі вимоги до зовнішніх регулюючих органів та розширення питань внутрішньої політики захисту даних.

Сьогодні до центрів обробки даних висуваються жорсткі вимоги щодо технології вимкнення та проблем безпеки. Зараз майже всі компанії, які використовують ці системи, серйозно працюють над підвищенням їх безпеки, хоча ще кілька років тому цей інтерес був лише теоретичним. Для бізнес-систем і програм проблеми безпеки є особливо серйозними. Основною причиною масштабної міграції більшості систем на хмарні сервіси є віртуалізація. Звичайно, водночас є багато завдань щодо забезпечення безпеки в новому середовищі. Для цього потрібен спеціальний метод. Більшість загроз повністю вивчені та розроблено проти них контрзаходи. Однак ці заходи повинні бути придатними для використання в хмарі.

Однією з перших проблем безпеки, яка виникла, був контроль і керування хмарними сервісами. Зрештою, відстеження всіх ресурсів сервісів, віртуальних машин і процесів – непросте завдання. Ця загроза має високий рівень, оскільки передбачає управління хмарним середовищем як єдиною інформаційною системою, тому необхідно створити окрему систему захисту. Для цього використовуйте модель управління ризиками хмарної інфраструктури.

Суворий контроль фізичного доступу до всіх елементів цієї інфраструктури є основою для забезпечення фізичної безпеки. Основою захисту мережі є брандмауер і захист від вторгнень. Використання брандмауера означає фільтрацію, а його мета — розрізняти внутрішню мережу ЦОД на підмережі різних рівнів довіри.До наявних атак на хмарне середовище відносять наступні:

-Традиційні програмні атаки;

-Функціональні атаки на елементи хмарної інфраструктури;

-Атаки на стороні клієнта хмарного середовища;

-Атаки на екологічного контролера (програма управління);

-Атаки на систему управління. Ефективна архітектура хмарної безпеки повинна розпізнавати ці атаки та боротися з ними. Рішення безпеки стають Наступні рішення:

-Зашифроване зберігання даних;

-Захист даних під час передачі;

-Аутентифікація користувача;

-Користувачі ізольовані один від одного.

Тому хмарні технології є дуже перспективною галуззю, яка постійно розвивається і забезпечує значне прискорення для майбутнього вдосконалення інформаційних технологій. Тому питання безпеки в цьому середовищі завжди актуальні. Основними методами захисту інформації в хмарних технологіях є: шифрування, обмін даними та аутентифікація. Тільки за умови правильного ставлення до захисту даних у хмарних обчисленнях дані можна вважати захищеними.