УДК 618.31.05

ЗАХИСТ ДАНИХ В «ХМАРНИХ» ТЕХНОЛОГІЯХ ОБЧИСЛЕНЬ

Титарчук Є. О.
Науковий керівник – д.т.н., проф. Квєтний Р. Н.

Розповсюдження мереж з високою потужністю, низька вартість комп'ютерів і пристроїв зберігання даних, а також широке впровадження віртуалізації, сервіс-орієнтованої архітектури привели до величезного зростання хмарних обчислень.

Хмарні обчислення — це модель забезпечення зручного доступу на вимогу через мережу до обчислювальних ресурсів, які можуть бути оперативно надані та звільнені з мінімальними управлінськими затратами та зверненнями до провайдера.

Кінцеві користувачі мають доступ до власних даних і можуть не перейматися роботою обладнання технологічної інфраструктури (а в залежності від моделі обслуговування і програмним забезпеченням) "хмари", яка їх підтримує. Проте в цьому проявляється головний недолік хмари – приватна інформація користувача фактично стає доступна третій стороні – провайдеру, крім цього данні можуть стати вразливими під час їх передачі по каналам зв'язку. Після аналізу відомих недоліків хмарної моделі обчислень можна виділити такі її основні вразливості:

- Незахищені програмні інтерфейси (API)
- Неправомірне використання хмарних технологій
- Внутрішні порушники
- Вразливості в технологіях віртуалізації
- Втрата даних
- Кража персональних даних
- Інші вразливості.

Для захисту даних великі провайдери, такі як Amazon та Azure, дають змогу користувачам шифрувати інформацію яку вони зберігають на сервісах, проте таке шифрування відбувається вже на стороні провайдера і не може забезпечити збереження інформації при деяких з вище перерахованих сценаріях. При необхідності виконання обрахунків у хмарі може бути використана модель гомоморфного шифрування, проте сучасні алгоритми такого шифрування не забезпечують достатній рівень продуктивності обчислень. Програма «Клієнт», що розробляється, буде використовувати шифрування на клієнтській стороні та надсилатиме в хмару вже зашифровані дані, роблячи їх недоступними для третьої сторони. Проте умовою використання такого рішення є необхідність застосування спеціалізованої клієнтської програми та збереження ключа шифрування, втрата якого однозначно призведе до втрати усієї зашифрованої інформації.