ДОСЛІДЖЕННЯ МОДЕЛІ БЕЗПЕКИ ПРИ ВИКОРИСТАННІ ХМАРНИХ СЕРВІСІВ

Рудий С.В., Сєвєрінов О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

В роботі розглянута модель безпеки розташування файлів у хмарному сховищі на основі використання двофакторної автентифікації та симетричного шифруванням.

Об'єктом дослідження є моделі безпеки при використанні хмарних сервісів.

Предмет дослідження – процес двофакторної автентифікації користувачів хмарних сервісів з використанням шифрування файлів при розміщенні у хмарному сервісі.

На сьогодні, сформувалося три основні моделі розгортання хмарних сервісів IaaS, PaaS та SaaS. Основним питанням, на сьогодні, є безпека даних користувача, що взаємодіє з хмарним сервісом [1, 2].

Для підвищення безпеки при використанні хмарних сервісів запропонована модель безпеки, що складається з двох складових:

використання двофакторної автентифікації (2FA) із застосуванням одноразового паролю (OTP);

шифрування файлів при розміщенні у сховищах хмарних сервісів.

Для визначення ефективності запропонованою моделі було проведено порівняння одноразового паролю, ПІН-коду та статичного паролю у якості системи автентифікації с розрахунком ентропії методів автентифікації [2]. Також, було проведено тести NIST для визначення ефективності алгоритмів шифрування AES, RC6, 3DES, MARS, DES, Blowfish, RC4, Twofish для запропонованої моделі.

В результаті проведеного дослідження було встановлено, що ентропія one-time password у більше ніж 2 рази краща ніж у статичного пароля, та 8 разів – ніж у ПІН коду. По результатам дослідження методів шифрування файлів найкращі показники має алгоритм AES.

Таким чином, запропонована модель безпеки даних вирішує проблеми захисту інформації користувачів хмарних сервісів і допомагає постачальнику хмарних послуг вибрати найбільш підходящий алгоритм шифрування.

Список літератури

1. National Institute of Standards and Technology [Електронний ресурс] – Режим доступу до ресурсу://www.nist.gov..

2. V. Prakash, A. Infant, J. Shobana, Eliminating vulnerable attacks using One-Time Password and PassText—Analytical study of blended schema, Universal Journal of Computer Science and Engineering Technology 1 (2010) 133-140.

3. Andrew Rukhin,Juan Soto,James Nechvatal and others. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST, Special Publication 800-22 Revision 1a, April2010, 131 p.