УДК 004.056.5:004.75

Трофімов О.С., аспірант
Київський столичний університет імені Бориса Грінченка

МЕТОД КОМБІНОВАНОГО ШИФРУВАННЯ ДАНИХ В ХМАРНИХ СЕРЕДОВИЩАХ

Перенесення корпоративних інформаційних систем до хмарних середовищ актуалізує проблему забезпечення конфіденційності, цілісності та доступності даних за умов високої інтенсивності операцій, жорстких вимог до продуктивності та обмежень на допустиму затримку. У таких умовах криптографічний захист має відповідати не лише вимогам інформаційної безпеки, а й експлуатаційним характеристикам високонавантажених систем. Концептуальну основу такого підходу формують керування інформаційною безпекою та архітектура «Повної недовіри», у межах якої жоден компонент інфраструктури не вважається довіреним за замовчуванням [1], [2].

Побудова ефективного захисту даних у корпоративних хмарних системах потребує поєднання кількох вимог: формалізованої моделі загроз, розмежування рівнів довіри, керованого життєвого циклу ключового матеріалу та узгодження криптографічних механізмів із часовими обмеженнями хмарних сервісів [1], [2]. За таких умов критичні криптографічні перетворення доцільно виконувати на стороні клієнта або в межах окремого довіреного домену керування ключами, не покладаючись на безпечність інфраструктури провайдера.

Особливу увагу слід приділяти визначенню місця гомоморфного шифрування в архітектурі захисту. Його перевага полягає в можливості виконання обчислень над зашифрованими даними без розкриття відкритого тексту, що є перспективним для приватної аналітики та спеціалізованих сервісів обробки конфіденційної інформації [4]. Водночас значні обчислювальні накладні витрати, збільшення обсягу даних і зростання часу обробки обмежують використання таких схем у ролі базового механізму захисту хмарних сховищ. Тому гомоморфне шифрування доцільно розглядати як окремий сервісний рівень для вибіркових сценаріїв, а базовий захист реалізовувати за допомогою симетричних автентифікованих механізмів.

Архітектура криптографічного захисту має передбачати розмежування транспортного рівня, рівня сховищ і рівня реалізації, при цьому саме рівень сховищ є центральним для забезпечення основних криптографічних гарантій. Для об'єктних і файлових сховищ доцільним є підхід AEAD-first, за якого автентифіковане шифрування поєднує конфіденційність і контроль цілісності. До додаткових автентифікованих даних мають включатися стабільні параметри

контексту, зокрема ідентифікатор орендаря, ресурсу, версія політики та позиція фрагмента, що дає змогу виявляти атаки повтору, перестановки та відкату [2], [3].

Для мережевих блочних сховищ доцільно використовувати або профіль AEAD-на-сектор, або режим XTS-AES лише у поєднанні з окремим механізмом автентифікації, оскільки сам по собі XTS-AES не забезпечує контролю цілісності. Не менш важливою складовою є керування ключовим матеріалом, яке має охоплювати генерацію, детерміновану деривацію, ротацію, зберігання та знищення ключів. Контекст деривації повинен однозначно визначати призначення ключа, домен безпеки, ресурс і версію криптографічної політики, забезпечуючи ізоляцію між орендарями та ресурсами [1], [5].

Отже, ефективний криптографічний захист даних у корпоративних хмарних системах доцільно реалізовувати шляхом поєднання архітектури «Повної недовіри», автентифікованого симетричного шифрування, формалізованого криптографічного контексту та керованого життєвого циклу ключів. Такий підхід узгоджує криптографічну стійкість із вимогами до продуктивності, масштабованості та прогнозованості затримок.

Список використаних джерел

1. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT). [Чинний від 2023-08-22]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2023. 16 с.

2. Rose S., Borchert O., Mitchell S., Connelly S. Zero trust architecture. Gaithersburg, MD : National Institute of Standards and Technology, 2020. 59 p. (NIST Special Publication 800-207). DOI: 10.6028/NIST.SP.800-207.

3. ДСТУ ISO/IEC 27017:2017. Інформаційні технології. Методи захисту. Звід практик стосовно заходів інформаційної безпеки, що ґрунтуються на ISO/IEC 27002, для хмарних послуг (ISO/IEC 27017:2015, IDT). [Чинний від 2019-01-01]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2017.

4. Marcolla C., Sucasas V., Manzano M., Bassoli R., Fitzek F. H. P., Aaraj N. Survey on fully homomorphic encryption, theory, and applications. Proceedings of the IEEE. 2022. Vol. 111, no. 3. P. 317–345. DOI: 10.1109/JPROC.2022.3205665.

5. Chen L. Recommendation for Key Derivation Using Pseudorandom Functions. Gaithersburg, MD : National Institute of Standards and Technology, 2022. 34 p. (NIST Special Publication 800-108 Rev. 1). DOI: 10.6028/NIST.SP.800-108r1.