УДК 004.056.5:004.7

Черкаський Олександр Валерійович,

здобувач другого (магістерського) рівня вищої освіти
Харківського національного університету радіоелектроніки

Буслов Павло Володимирович,

к.т.н., старший викладач кафедри безпеки інформаційних технологій
Харківського національного університету радіоелектроніки

БАГАТОРІВНЕВА МОДЕЛЬ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ З ХМАРНИХ СЕРЕДОВИЩ

Анотація. Обґрунтовано багаторівневий підхід до запобігання витоку інформації під час використання хмарних сервісів. Розглянуто розмежування функцій автентифікації та авторизації, криптографічного захисту, перевірки цілісності та відновлення інформаційних об’єктів. Запропоновано архітектуру, що передбачає перевірку одноразового пароля, шифрування даних перед їх розміщенням у хмарному сховищі, відокремлене зберігання ключів і контроль автентичності. Визначено сценарії функціонального оцінювання захисних механізмів та підхід до порівняння продуктивності алгоритмів шифрування. Показано, що ефективність комплексного захисту визначається не лише криптографічним алгоритмом, а й узгодженістю політик доступу, керування ключами та процедур відновлення.

Ключові слова: хмарне середовище, витік інформації, багаторівневий захист, автентифікація, AES-GCM, контроль цілісності, керування ключами.

Перенесення корпоративних інформаційних ресурсів до хмарних середовищ супроводжується зміною меж контролю над даними. Компрометація облікових записів, помилки конфігурації доступу, неправомірне копіювання об’єктів та порушення правил використання криптографічних ключів створюють ризики розголошення інформації. Застосування окремого захисного засобу не охоплює весь життєвий цикл

даних, тому актуальним є поєднання взаємодоповнювальних механізмів безпеки в єдиній архітектурі [1].

Метою дослідження є обґрунтування структури багаторівневої моделі захисту даних у хмарному середовищі та визначення критеріїв перевірки її функціональних властивостей. Особливістю запропонованого підходу є узгодження механізмів доступу, криптографічного перетворення і контролю стану інформаційних об’єктів у послідовному процесі оброблення запитів.

На першому рівні передбачено ідентифікацію та автентифікацію користувача із застосуванням одноразового пароля (OTP) як додаткового фактора. Після перевірки облікових даних система окремо оцінює право суб’єкта на конкретну операцію, що дає змогу реалізувати принцип найменших привілеїв. З метою зменшення ризику перебору необхідні обмеження кількості спроб, контроль строку дії коду та захист від його повторного використання [2].

Другий рівень забезпечує конфіденційність інформаційних об’єктів до їх передавання у віддалене сховище. Як основний криптографічний механізм доцільно використовувати автентифіковане шифрування AES-GCM, яке поєднує приховування вмісту та перевірку автентичності даних [3]. Ключовими умовами коректного застосування є унікальність nonce у межах одного ключа, захищене створення й зберігання ключового матеріалу та недопущення видачі відкритого тексту за невдалої перевірки тегу. При цьому криптографічні ключі мають бути логічно відокремлені від шифротекстів [4].

Третій рівень спрямовано на виявлення несанкціонованого змінення об’єктів, резервування і контрольоване відновлення. На відміну від простого хешування, автентифіковане шифрування дозволяє перевірити цілісність за наявності секретного ключа. Водночас можливість відновлення визначається не лише наявністю резервної копії, а й

доступністю відповідних ключів і перевіреністю процедури відновлення.

Для функціонального оцінювання запропоновано такі контрольні сценарії: відмова в операції за неправильних облікових даних або OTP; відсутність відкритих даних у хмарному сховищі; відхилення зміненого шифротексту чи тегу; неможливість розшифрування без належного ключа; відновлення даних за наявності резервної копії та ключового матеріалу. Ці сценарії дозволяють відокремити перевірку властивостей захисту від вимірювання швидкодії.

У роботі описано експериментальне порівняння алгоритмів RC4, RC6, MARS, AES, DES, 3DES, Twofish і Blowfish у дослідницькому середовищі Amazon EC2 t1.micro, а також аналіз бітових послідовностей за тестами NIST SP 800-22. Таке порівняння характеризує обрану конфігурацію експерименту, проте статистичні властивості послідовностей не є самостійним доказом криптографічної стійкості. DES, 3DES і RC4 розглядаються лише як історичні порівняльні варіанти, а не як рекомендовані засоби захисту.

Організаційний аспект комплексного захисту також потребує врахування управління вразливостями та ризиками протягом експлуатації інформаційної системи. Відповідний взаємозв’язок процедур оцінювання вразливостей і політики інформаційної безпеки розглянуто в дослідженні О. В. Сєвєрінова та співавторів [5].

Таким чином, запропонована модель визначає логічно узгоджену послідовність захисних дій: перевірка користувача й повноважень, шифрування, зберігання шифротексту, перевірка автентичності та відновлення за контрольованих умов. Її практичне значення полягає у формуванні перевірюваних вимог до захищеної взаємодії з хмарними ресурсами. Подальше дослідження має охоплювати незалежне випробування реалізації на типових сценаріях витоку даних, оцінювання витрат на криптографічні операції та перевірку процедур керування ключами.

Список використаних джерел

1. National Institute of Standards and Technology. The NIST Definition of Cloud Computing / P. Mell, T. Grance. NIST SP 800-145. 2011. DOI: https://doi.org/10.6028/NIST.SP.800-145.
2. Temoshok D., Fenton J., Choong Y.-Y., Lefkovitz N., Regenscheid A., Galluzzo R., Richer J. Digital Identity Guidelines: Authentication and Authenticator Management. NIST SP 800-63B-4. 2025. DOI: https://doi.org/10.6028/NIST.SP.800-63B-4
3. Dworkin M. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. NIST SP 800-38D. 2007. DOI: https://doi.org/10.6028/NIST.SP.800-38D.
4. Barker E. Recommendation for Key Management: Part 1 – General. NIST SP 800-57 Part 1 Rev. 5. 2020. DOI: https://doi.org/10.6028/NIST.SP.800-57pt1r5
5. Поддубний В. О., Сєвєрінов О. В., Пустомельник О. С. Менеджмент вразливостей як складова частина політики безпеки ІТС. Системи управління, навігації та зв'язку. 2020. Вип. 4. С. 55–58. DOI: https://doi.org/10.26906/SUNZ.2020.4.055.