СИСТЕМИ ЗБЕРІГАННЯ КРИПТОГРАФІЧНИХ КЛЮЧІВ

Щербакова Ю.А., Острижна Є.С.
Національний аерокосмічний університет
«Харківський авіаційний інститут», Харків, Україна

Зберігання криптографічних ключів є важливим аспектом забезпечення безпеки інформаційних систем на державному рівні [1, 2], у фінансовій сфері [3, 4] та у приватному спілкуванні.

Ризики, пов'язані з втратою, компрометацією або неправильним зберіганням ключів, мають значний вплив на цілісність і конфіденційність інформації, тому дослідження критеріїв оптимальності при створенні таких систем, а також вибір параметрів їх функціонування набувають значної актуальності

Метою доповіді є розробка системного підходу до аналізу, проектування та вдосконалення системи зберігання криптографічних ключів для забезпечення конфіденційності, цілісності та доступності даних, а також підвищення рівня захищеності інформації в сучасних інформаційних системах.

Виклики, виявлені в дослідженнях:

- Компрометація ключів,
- Баланс між безпекою та продуктивністю,
- Захист ключів у багатокористувацьких середовищах,
- Відповідність нормативним вимогам.

Перспективи розвитку:

- Інтеграція штучного інтелекту,
- Покращення алгоритмів шифрування,
- Автоматизація управління життєвим циклом ключів.

Можливі критерії оптимізації.

Оптимізація системи зберігання криптографічних ключів спрямована на підвищення її ефективності, безпеки та надійності. Критерії оптимізації поділяються на три основні категорії: продуктивність, захищеність і економічна ефективність.

1. Продуктивність системи.

Оптимізація продуктивності спрямована на зменшення затримок, підвищення швидкості роботи системи і забезпечення її масштабованості.

Критерії:

– Час доступу до ключів (мінімізація часу, необхідного для обробки запиту на отримання ключа),

– Швидкість генерації ключів (зменшення часу, потрібного для створення криптографічного ключа),

– Пропускна здатність системи,

– Масштабованість (можливість обробляти зростаючий обсяг даних).

2. Захищеність системи

Оптимізація захищеності спрямована на мінімізацію ризиків компрометації ключів, забезпечення стійкості системи до атак.

Критерії:

– Рівень безпеки зберігання ключів(гарантія, що ключі захищені від фізичного та логічного доступу неавторизованих користувачів),

– Контроль доступу до ключів (ефективність політик доступу, що регулюють права користувачів),

– Стійкість до компрометації ключів (мінімізація ризиків витоку ключів та впливу їх компрометації на систему),

– Відмовостійкість системи (здатність системи продовжувати роботу у разі збоїв або атак.).

–

3. Економічна ефективність

Оптимізація витрат на розробку, впровадження та обслуговування.

Критерії:

– Вартість розгортання системи (мінімізація витрат на встановлення обладнання та програмного забезпечення),

– Вартість обслуговування системи (зменшення витрат на підтримку та оновлення системи),

– Ефективність використання ресурсів (оптимізація використання обчислювальних ресурсів для роботи системи).

Методи реалізації оптимізації

– Автоматизація управління ключами: Ротація, архівація, створення та видалення ключів виконуються без участі адміністратора,

– Модульність: Поділ системи на окремі компоненти (зберігання, авторизація, резервне копіювання), які можна оптимізувати незалежно,

– Моніторинг продуктивності: Регулярний аналіз роботи системи для виявлення вузьких місць,

– Інтеграція штучного інтелекту

Список літератури

1. Інструкція про порядок генерації ключів програмного комплексу «Варта». https://uakey.com.ua/files/uploads/ba58cdbb8a1dcb8b96c7d426de177ab8.pdf

2. GDPR — Загальний регламент захисту даних (General Data Protection Regulation): https://eur-lex.europa.eu/legal

3. Порядок роботи з криптографічними ключами модулів безпеки Національної платіжної системи “Український платіжний простір” https://bank.gov.ua/admin_uploads/law/Decision_Prostir_28062024_57-13_Crypto_Keys_Procedure

4. PCI DSS — Стандарт безпеки даних індустрії платіжних карт: https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1

Посібник з SSL-сертифікату Exchange Server https://www.ssl.com/guide/exchange-server-ssl-certificate-guide/