АНАЛІЗ МЕТОДІВ ПЕРЕВІРКИ ЦІЛІСНОСТІ ТА АВТЕНТИЧНОСТІ ФАЙЛІВ ЗА ДОПОМОГОЮ ГЕШ-ФУНКЦІЙ

Доленко О.Д., В'юхін Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасних умовах, коли обсяг цифрових даних стрімко зростає, а також відбувається інтенсивний обмін файлами в інформаційних системах, важливим є забезпечення довіри до цифрових даних. Перевірка контрольних сум є одним з найпоширеніших методів підтвердження цілісності та автентичності файлів, що дозволяє швидко виявляти спроби несанкціонованої модифікації, втрати або підміни даних [1, 2].

Метою доповіді є аналіз методів перевірки цілісності та автентичності файлів за допомогою геш-функцій. Вибір алгоритму для розрахування контрольної суми залежить від мети користувача. Швидкі алгоритми – xxHash або Adler32, підходять для виявлення випадкових пошкоджень, а криптографічно стійкі алгоритми, такі як SHA256, SHA512 та новітній BLAKE3 доцільно використовувати для підтвердження автентичності [3]. Дослідження, наведені у [4], показали, що BLAKE3 підтримує багатопотокову обробку, має у 2-3 рази більшу швидкість роботи та потребує у 10 разів меншу кількість оперативної пам'яті для роботи в порівнянні з перерахованими криптостійкими алгоритмами.

Запропонований підхід полягає у першочерговому використанні високошвидкісного алгоритму xxHash для попередньої перевірки даних, а після – криптографічно стійкого BLAKE3 для верифікації критичної частки інформації. У змодельованому експерименті для масиву даних розміром 6 GB використання лише BLAKE3 зайняло близько 1.5 с, тоді як комбінована схема скоротила час до 1.23 с при застосуванні BLAKE3 до 75% даних (економія 18%) та до 0.85 с при застосуванні BLAKE3 до 50% даних (економія 43%). Таким чином, цей метод дає змогу скоротити час перевірки у порівнянні з використанням BLAKE3 для всього об'єму даних.

Проведений огляд підтверджує доцільність застосування каскадних методів, де швидкий алгоритм виконує попередню перевірку, а надійний криптографічний хеш застосовується лише до окремих критичних даних.

Список літератури

1. Моруга Д. І. Методи та алгоритми хешування паролів на платформі .NET: кваліфікаційна робота, пояснювальна записка; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. – Харків, 2022. – 65 с.

2. Голубничий, Д.Ю., Сєвєрінов, О., Коломійцев, О.В., та інш. (2021). Аналіз сучасних загроз в інформаційних системах за складовими загроз: кібербезпеки, інформаційної безпеки та безпеки інформації.

3. Addis M. Which checksum algorithm should I use?. *DPC technology watch guidance note*. 2020. P. 1–5.

4. Pandya M. Performance evaluation of hashing algorithms on commodity hardware. *arXiv.org e-Print archive*. URL: https://arxiv.org/html/2407.08284v1.3.