УДК 004.056(075)
Ковальов І.Є.[1], Козіна Г.Л.[2]
[1] студ. гр. БК-813м НУ «Запорізька політехніка»
[2] канд. фіз.-мат. наук, доц. НУ «Запорізька політехніка»

# ОГЛЯД КРИТЕРІЇВ ОЦІНКИ ВЛАСТИВОСТЕЙ ФУНКЦІЙ ХЕШУВАННЯ

Всі геш функції можна розділити та порівняти за наступними характеристиками: довжина гешу, довжина блоку обробки даних.

Це характеристики, які відомі і без дослідження, можна дізнатися з документації функції. А також, є властивості, функції які слід встановлювати вже методом аналізу, серед них швидкість обчислення, стійкість до 0000-0002-4787-6865, аваланшний ефект.

При дослідженні властивостей функцій гешування дуже важливо, щоб умови виконання цих функцій, а також спосіб їх реалізації був максимально однаковим.

Для цього було обрано саме бібліотечну реалізацію цих функцій, а саме бібліотеку Bouncy Castle.

Для порівняння було обрано функцію гешування «Купина», яка описана в ДСТУ 7564:2014, також було розповсюджені функції, так і національні стандарти інших країн: SM3, MD5, родина SHA, BLAKE2, Whirlpool (табл.1).

Таблиця 1 – Загальна характеристика

| Функ-ція | Купи-на | SM 3 | Whirlpo ol | BLAKE2 | MD 5 | SHA3 | SH A | SHA 1 |
|---|---|---|---|---|---|---|---|---|
| Дов-жина гешу (біт) | 256/51 2 | 256 | 512 | 256/384/5 12 | 128 | 256/ 384/51 2 | 256 / 512 | 160 |
| Дов-жина блоку (біт) | 1024 | 512 | 512 | 512-1024 | 512 | 512-1024 | 512 - 102 4 | 512 |

Вимір характеристик відбувався за допомогою програми, яка написана на мові C# і використовує бібліотеку BouncyCastle для реалізації цих функцій. Результати було зведено до таблиці 2.

За даними таблицями можна зробити висновки що до вибору хеш-функцій для різних ситуацій.

Купина-256/512 – як національний стандарт України, найкраще підходить саме для внутрішнього ринку, де потрібна досить висока швидкість та надійність.

Таблиця 2. Результати вимірювання

| Функція | Швидкість обчислення (біт/с) | Стійкість до колізій (спроб до колізії) | Аваланшний ефект (біт) |
|---|---|---|---|
| Купина-256 | 84450,84 | 2545517993 | 127,97 |
| Купина-512 | 2612244,89 | 4247515242 | 255,95 |
| SM3 | 247701,98 | 3754245964 | 127,985 |
| Whirlpool | 363946,54 | 4154245697 | 255,98 |
| BLAKE2-256 | 9350759,13 | 2456795431 | 127,95 |
| BLAKE2-384 | 9434889,43 | 2705943256 | 191,99 |
| BLAKE2-512 | 9578638,94 | 3654245678 | 255,97 |
| MD5 | 110382,89 | 137729200 | 63,68 |
| SHA3-256 | 247056,55 | 3245117215 | 127,98 |
| SHA3-384 | 25430463,57 | 3821954021 | 191,98 |
| SHA3-512 | 26806282,72 | 4651256780 | 255,96 |
| SHA-256 | 372147,11 | 155289240 | 128,00 |
| SHA-512 | 542085,75 | 253256975 | 255,99 |
| SHA-1 | 298340,48 | 11564249 | 79,98 |

Функція гешування SM3 оптимальна для цілісності та цифрових підписів.

Функція гешування Whirlpool – повільна.

Функція гешування BLAKE2 оптимальна для швидкості та безпеки.

Функція гешування MD5 застаріла та небезпечна.

Функція гешування SHA3 надає баланс швидкості та безпеки.

Функція гешування SHA-256/512 широко використовуються; а SHA-1 не рекомендується.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Євсеєв С. П., Йохов О. Ю., Король О. Г., Гешування даних в інформаційних системах: монография — К.: «ХНЕУ», 2013. — 312 с.

2. ДСТУ ISO 7564:2014 Інформаційні технології. Криптографічний захист інформації. Функція гешування [Чинний від 2015-04-01]. Київ, 2015. 39 с. (Інформація та документація).