Прим. № 1

АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ
(АДМІНІСТРАЦІЯ ДЕРЖСПЕЦЗВ'ЯЗКУ)

вул. Солом'янська, 13, м. Київ, 03110, тел. (044) 281-93-08, факс: (044) 281-94-83,
e-mail: info@cip.gov.ua, сайт: www.cip.gov.ua, код згідно з ЄДРПОУ 34620942

15.05.2024 № 04/05/02-8119/ВН На № _____ від _____

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 15.05.2024 м. Київ

Виданий: Товариству з обмеженою відповідальністю «ДОЛЯ І КО. ЛТД» (код ЄДРПОУ 01043342)

на підставі рішення Експертної комісії з питань проведення державної експертизи в сфері криптографічного захисту інформації Державної служби спеціального зв'язку та захисту інформації України, протокол від 13.05.2024 № 611.

Об'єкт експертизи: Програмний виріб обчислення геш-функції «HashCalc» UA.01043342.00002-01.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю «ДОЛЯ І КО. ЛТД» (код ЄДРПОУ 01043342).

Експертний заклад: Товариство з обмеженою відповідальністю «ЗАХИСТ.ЮЕЙ» (код ЄДРПОУ 42292899).

Висновки:
1. В об'єкті експертизи правильно реалізовано криптографічний алгоритм гешування, визначений ДСТУ 7564:2014 (у режимах «Купина-256», «Купина-384», «Купина-512») та ГОСТ 34.311-95.
2. Об'єкт експертизи відповідає вимогам технічного завдання UA.01043342.00002-01 90 01 в частині реалізації функцій криптографічних перетворень.
3. Об'єкт експертизи може бути використаний для здійснення контролю цілісності даних шляхом обчислення та перевірки значень геш-функцій для набору файлів.

Особливі умови (рекомендації): дія експертного висновку поширюється на зразки об'єкта експертизи, у яких криптографічні перетворення здійснюються програмними модулями, що мають наступні значення геш-функцій:

```
Gost34311HashCalc.dll  F2AF20A2 0FAF5CCE BD5F0B05 C24B3E3B ACE38B7B AE1358CA 840E4A97 5D95E295
KupynaHashCalc.dll     C6694870 A1FD7F86 53A7BF29 5E234015 122A9A29 57720549 6F3EFAEB 898C8BCD
```

Розрахунок геш-функцій здійснено відповідно до ДСТУ 7564:2014 (у режимі роботи «Купина-256» з використанням нульового вектора ініціалізації).

Термін дії експертного висновку – до 13.05.2029.

Голова Служби Юрій МИРОНЕНКО