Прим. № 1

# ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

вул. Солом'янська, 13, м. Київ, 03680,
тел. (044) 281-92-10, факс: (044) 281-94-83, e-mail: info@dsszzi.gov.ua

19.06.2015 № 05/02/02-2597

## ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 19.06.2015 м. Київ

Виданий: Товариству з обмеженою відповідальністю "САЙФЕР ЛТД" (код ЄДРПОУ 23154898)

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 19.06.2015 № 196.

Об'єкт експертизи: Програмний виріб "Шифр" (Бібліотеки функцій криптографічних перетворень. Версія 1.0) UA.23154898.00001-01.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю "САЙФЕР ЛТД" (код ЄДРПОУ 23154898).

Експертний заклад: Державний науково-дослідний інститут спеціального зв'язку та захисту інформації Державної служби спеціального зв'язку та захисту інформації України (код ЄДРПОУ 34732331).

Висновки:
1. В об'єкті експертизи правильно реалізовано криптографічні алгоритми, які визначені ДСТУ ГОСТ 28147:2009, ГОСТ 34.310-95, ГОСТ 34.311-95.
2. Об'єкт експертизи відповідає вимогам технічного завдання UA. 23154898.00001-01 90 01 та Доповнення № 1 до нього, в частині реалізації функцій криптографічних перетворень.
3. Об'єкт експертизи може бути використаний для побудови засобів криптографічного захисту інформації з обмеженим доступом (крім службової інформації та інформації, що становить державну таємницю) та відкритої інформації, вимога щодо захисту якої встановлена законом, видів А та Б.

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:

| | |
|---|---|
| c32csp.dll* | EBF94554 84F826A2 62FD3CC3 0519E8C3 DF202D49 DD600B5B 4AA08D7F B561A4B6 |
| c32csp.h* | 47DD1029 4FB5D573 C361949F 80099EEC 0B9C3FCA 792E730B C3DCFFED 1EABBE59 |
| c32csp.lib* | E4D33201 5078E49F 81806951 E1DC45CA 13576178 A2BABE86 F1481967 49EA69A0 |
| c32cspimp.lib* | 9864DEC1 C6D4E7EC DBC8C6BF D27C7B3F 0CC3CFC4 FE97AB19 EDBBFDFF E3B8ED93 |
| c32csp.zip* | 1A733D6A 7D84ADD5 9CA67683 8926CD85 B6553003 51416B00 17EE0F0F 93BCE928 |

Розрахунок геш-функцій здійснено відповідно до ГОСТ 34.311-95 з урахуванням значення нульового стартового вектора та ДКЕ № 1 з додатка № 1 до Інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації, затвердженої наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 12.06.2007 № 114, зареєстрованої в Міністерстві юстиції України 25.06.2007 за № 729/13996.

Термін дії експертного висновку – до 19.06.2020.

Перший заступник Голови Служби О.В. Корнейко