Прим. № 1

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

вул. Солом'янська, 13, м. Київ, 03110,
тел. (044) 281-92-10, факс: (044) 281-94-83, e-mail: info@dsszzi.gov.ua

26.04.2018 № 04/03/02-1799

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 26.04.2018 м. Київ

Виданий: Товариству з обмеженою відповідальністю «САЙФЕР БІС» (код ЄДРПОУ 33349855)

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 17.04.2018 № 339.

Об'єкт експертизи: Програмний виріб «Шифр+» версія 1.0 ТЗ У 72.2 23154898 001:2007.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю «САЙФЕР БІС» (код ЄДРПОУ 33349855).

Експертний заклад: Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» (код ЄДРПОУ 34979237).

Висновки:

1. В об'єкті експертизи правильно реалізовано криптографічні алгоритми, визначені ДСТУ ГОСТ 28147:2009, ДСТУ 4145-2002, ГОСТ 34.311-95.
2. В об'єкті експертизи алгоритм генерації випадкових двійкових послідовностей відповідає додатку А ДСТУ 4145-2002.
3. В об'єкті експертизи правильно реалізовано протокол автономного узгодження ключів в групі точок еліптичної кривої типу Діффі-Геллмана (KANIDH), визначений п. 8.2 ДСТУ ISO/IEC 15946-3:2015.
4. В об'єкті експертизи механізм формування початкових значень генератора випадкових двійкових послідовностей відповідає вимогам документу «Методика ініціалізації генератору випадкових послідовностей. МІ У 72.2 23154898 001:2007».
5. Об'єкт експертизи відповідає вимогам технічного завдання ТЗ У 72.2 23154898 001:2007 із Доповненням № 1 до нього, в частині реалізації функцій криптографічних перетворень.
6. Об'єкт експертизи може бути використаний для 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:

Каталог Java
cipherplus.jar EEE005F1 1EA1A894 060D4739 5E99BF60 4320E861 B43A0EF4 B6089EC8 FA3B560C

Каталог Win32
dstu4145.dll BA19CD8A 2F214C44 8B6F3C9C 318DDA0E 0C63A286 9F80C5F4 5F3FDFB9 51F36408

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 17.04.2023.

Перший заступник Голови Служби О.М. Чаузов