Прим. № 1

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

вул. Солом'янська, 13, м. Київ, 03110, тел. (044) 281-92-10, факс: (044) 281-94-83,
e-mail: info@dsszzi.gov.ua, сайт: www.dsszzi.gov.ua, код згідно з ЄДРПОУ 34620942

08.07.2020 № 04/03/02-1762 На № _____ від _____

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 08.07.2020 м. Київ

Виданий: Товариству з обмеженою відповідальністю «САЙФЕР ПРО» (код ЄДРПОУ 42125815)

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 08.07.2020 № 460.

Об'єкт експертизи: Криптомодуль мережний «Шифр-HSM» МКМ: 42125815.ТД – 01.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю «САЙФЕР ПРО» (код ЄДРПОУ 42125815).

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

Висновки:

1. В об'єкті експертизи правильно реалізовано криптографічні алгоритми, визначені ДСТУ ГОСТ 28147:2009 (в режимі простої заміни, гамування та гамування зі зворотнім зв'язком), ДСТУ 7624:2014 (в режимах ECB, OFB, CFB, CBC, CTR), ДСТУ 7564:2014, ДСТУ 4145-2002 (у поліноміальному базисі), 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 правильно реалізовано криптографічні алгоритми шифрування TDEA, AES, визначені ДСТУ ISO/IEC 18033-3:2015 (в режимах ECB, OFB, CFB, CBC, CTR, визначених ДСТУ ISO/IEC 10116:2019).
5. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування RSA, визначений IETF RFC 3447 (за схемами RSAES-PKCS1-v1.5, RSAES-OAEP).
6. В об'єкті експертизи правильно реалізовано криптографічний алгоритм електронного цифрового підпису RSA, визначений IETF RFC 3447 (за схемами RSASSA-PKCS1-v1_5, RSASSA-PSS).
7. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного цифрового підпису ECDSA, визначений ДСТУ ISO/IEC 14888-3:2015.
8. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-1, SHA-256, SHA-384, SHA-512, визначені ДСТУ ISO/IEC 10118-3:2005.
9. В об'єкті експертизи правильно реалізовано криптографічні алгоритми обчислення кодів автентифікації (імітовставки), визначені ДСТУ ГОСТ 28147:2009, ДСТУ 7624:2014, ДСТУ ISO/IEC 18033-3:2015.

10. В об'єкті експертизи криптографічний алгоритм формування початкових значень генератора випадкових двійкових послідовностей реалізовано відповідно до вимог документу «Методика ініціалізації генератора випадкових двійкових послідовностей UA.33349855.00001 – 01 94 01».
11. В об'єкті експертизи криптографічний алгоритм зберігання особистих ключових даних реалізовано відповідно до вимог документу «Методика захисту ключа шифрування ключових даних МКМ 42125815.ТД – 08».
12. Об'єкт експертизи відповідає вимогам технічного завдання ТЗ У.72.2-42125815-001:2019 із Доповненням № 1 ТЗ У.72.2-42125815-001:2019-1 до нього, в частині реалізації функцій криптографічних перетворень (п. 6.2 – 6.5 ТЗ).
13. 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.

Особливі умови (рекомендації): дія експертного висновку поширюється на зразки об'єкта експертизи, виготовлені відповідно до технічних умов ТУ У 26.2-42125815-001:2020.

Термін дії експертного висновку – до 08.07.2025.

Голова Служби Валентин ПЕТРОВ