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

10.01.2020 № 04/03/02-133 На № _____ від _____

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 10.01.2020 м. Київ

Виданий: Товариству з обмеженою відповідальністю «АВТОР» (код ЄДРПОУ 32248356)

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 17.01.2020 № 438.

Об'єкт експертизи: КЛЮЧІ ЕЛЕКТРОННІ «SECURE TOKEN-338».

Розроблений (виготовлений): Товариством з обмеженою відповідальністю «АВТОР» (код ЄДРПОУ 32248356).

Експертний заклад: Адміністрація Державної служби спеціального зв'язку та захисту інформації України (код ЄДРПОУ 34620942).

1. В об'єкті експертизи криптографічні алгоритми реалізовано відповідно до вимог ДСТУ ГОСТ 28147:2009, ДСТУ 7624:2014 (Калина-128/128, Калина-128/256) у режимах ECB, CFB, CMAC, CBC, KW), ДСТУ 7564:2014 (у режимах Купина-384, Купина-512), ГОСТ 34.311-95, ДСТУ 4145-2002 (у поліноміальному та оптимальному нормальному базисах, з довжиною ключа 163-509 біт).
2. В об'єкті експертизи алгоритм генерації випадкових послідовностей відповідає додатку А ДСТУ 4145-2002.
3. В об'єкті експертизи правильно реалізовано криптографічні алгоритми шифрування TDEA, AES, DES, визначені ДСТУ ISO/IEC 18033-3:2015 (в режимах CBC, ECB і CFB, визначених ДСТУ ISO/IEC 10116:2015).
4. В об'єкті експертизи правильно реалізовано криптографічний алгоритм гешування SHA-1, SHA-256, визначені ДСТУ ISO/IEC 10118-3:2005.
5. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування RSA, визначений в PKCS#1 v2.1 RSA Cryptography Standard (за схемою RSAES-PKCS1-v1_5).
6. В об'єкті експертизи правильно реалізовано криптографічний алгоритм електронного цифрового підпису RSA, визначений PKCS#1 v2.1 «RSA Cryptography Standard» (за схемами RSASSA-PSS, RSASSA-PKCS1-v1_5, з довжиною ключа 1024-4096 біт).
7. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного цифрового підпису ECDSA, визначений ДСТУ ISO/IEC 14888-3:2015, з довжиною ключа 192-521 біт.
8. В об'єкті експертизи алгоритм вироблення імітовставки (MAC) згідно алгоритму DES, TDES реалізовано відповідно до FIPS PUB 81 Federal Information Processing Standards Publication 81 (в режимі MAC-CBC).

9. В об'єкті експертизи алгоритм вироблення імітовставки (MAC) згідно алгоритму AES реалізовано відповідно до NIST 800-38A NIST Special Publication (в режимі MAC-CBC).
10. В об'єкті експертизи правильно реалізовано алгоритм вироблення імітовставки (CMAC) згідно алгоритму AES відповідно до NIST Special Publication 800-38B (в режимі CMAC).
11. Порядок вироблення сеансових ключів для шифрування даних в об'єкті експертизи реалізовано відповідно до документа «Засоби КЗІ. Методика вироблення сеансового ключа, автентифікації, генерування випадкових послідовностей та контролю засобів КЗІ АЧСА.460709.001».
12. В об'єкті експертизи обчислення спільного секрету для криптографічного протоколу Діффі-Геллмана, що базується на криптографічних перетвореннях у групі точок еліптичної кривої (ECDH), що реалізовані та використовуються в об'єкті експертизи, відповідають вимогам наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 18.12.2012 № 739 «Про затвердження Вимог до форматів криптографічних повідомлень», зареєстрованого у Міністерстві юстиції України 14.01.2013 за № 108/22640, та ДСТУ ISO/IEC 15946-3:2006.
13. Об'єкт експертизи відповідає вимогам технічного завдання ТЗ.АЧСА.467649.062-01 із Доповненням № 1 до нього в частині реалізації функцій криптографічних перетворень.
14. Об'єкт експертизи, як засіб криптографічного захисту виду «В» (категорій «Ш», «К», «Р», «П») може бути використаний як складова частина при побудові засобів криптографічного захисту інформації видів «А» та «Б», призначених 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.
15. Об'єкт експертизи, як засіб криптографічного захисту виду «В» (категорії «П») може бути використаний як складова частина при побудові засобів криптографічного захисту інформації видів «А» та «Б», призначених для криптографічного захисту інформації з обмеженим доступом (крім 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 26.2-32248356-029:2020.

Термін дії експертного висновку – до 17.01.2025.

Голова Служби Валентин ПЕТРОВ