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

30.06.2017 № 04/03/02-2332

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 30.06.2017 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 30.06.2017 № 297.

Об'єкт експертизи: ПРИСТРОЇ ДЛЯ АВТОМАТИЧНОГО ОБРОБЛЕННЯ ІНФОРМАЦІЇ-КЛЮЧІ ЕЛЕКТРОННІ "SECURE TOKEN-337" АЧСА.467369.010, АЧСА.467369.012, АЧСА.467369.014, АЧСА.467369.024.

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).

Висновки:

1. В об'єкті експертизи правильно реалізовано криптографічні алгоритми, визначені ДСТУ ГОСТ 28147:2009 (в режимах простої заміни, гамування із зворотним зв'язком та обчислення імітовставки), ГОСТ 34.311-95, ДСТУ 4145-2002 (при реалізації в поліноміальному базисі).
2. В об'єкті експертизи правильно реалізовано криптографічні алгоритми шифрування DES, TDEA, AES відповідно до ДСТУ ISO/IEC 18033-3:2015 (в режимах ECB, CBC, CFB, визначені ДСТУ ISO/IEC 10116:2014).
3. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування RSA, визначений PKCS#1 v2.1 RSA Cryptography Standard (за схемою RSAES-PKCS1-v1_5 з довжиною ключа 1024, 1536, 2048 біт).
4. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного цифрового підпису RSA, визначений PKCS#1 v2.1 "RSA Cryptography Standard" (за схемою RSASSA-PKCS1-v1_5 з довжиною ключа 1024, 1536, 2048 біт).
5. В об'єкті експертизи правильно реалізовано криптографічний алгоритм гешування SHA-1, визначений в ДСТУ ISO/IEC 10118-3:2005.
6. В об'єкті експертизи правильно реалізовано алгоритм вироблення імітовставки (MAC) згідно алгоритму DES відповідно до FIPS PUB 81 Federal Information Processing Standards Publication 81 (в режимі роботи MAC-CBC).
7. В об'єкті експертизи правильно реалізовано алгоритм вироблення імітовставки (MAC) згідно алгоритму AES відповідно до NIST 800-38A NIST Special Publication (в режимі MAC-CBC).

8. В об'єкті експертизи правильно реалізовано алгоритм вироблення імітовставки (CMAC) згідно алгоритму AES відповідно до NIST Special Publication 800-38B (в режимі CMAC).
9. 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".
10. Протокол автономного узгодження ключів типу Діффі-Гелмана (KANIDH), який реалізовано в об'єкті експертизи, відповідає 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 в Міністерстві юстиції України 14.01.2013 за № 108/22640 (ECDH в поліноміальному базисі, з довжиною ключа 163-509 біт).
11. В об'єкті експертизи забезпечується захист записаних даних від несанкціонованого доступу, від безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання.
12. Об'єкт експертизи відповідає вимогам Технічного завдання ТЗ.АЧСА.467649.041-01 із Доповненням № 1 до нього, в частині реалізації функцій криптографічних перетворень.
13. Об'єкт експертизи (як засіб криптографічного захисту інформації категорії "Ш", "К", "Р", "П") 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".
14. Об'єкт експертизи (як засіб криптографічного захисту інформації категорії "П", "К") може бути використаний для побудови засобів криптографічного захисту з обмеженим доступом (крім інформації, що становить державну таємницю), видів "А" та "Б".

Особливі умови (рекомендації):

1. Ступень обмеження доступу до інформації, захист якої має забезпечуватися об'єктом експертизи, що використовується у складі конкретного комплексу засобів захисту інформації, визначається вимогами до відповідного комплексу, видів "А" та "Б".
2. Дія експертного висновку поширюється на зразки об'єкта експертизи, які виготовлені відповідно до технічних умов ТУ У 30.0-32248356-017:2011 із Сповіщенням АЧСА.02-2013 про зміну № 1 та Сповіщенням АЧСА.03-2016 про зміну № 2.

Термін дії експертного висновку – до 27.10.2021.

Перший заступник Голови Служби О.М. Чаузов