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

14.09.2016 № 04/03/02-3685

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 14.09.2016 м. Київ

Виданий: Товариству з обмеженою відповідальністю "Майкрософт Україна" (код ЄДРПОУ 32383277)

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 09.09.2016 № 256.

Об'єкт експертизи: Криптографічний сервіс провайдер "Microsoft Enhanced RSA and AES Cryptographic Provider" операційної системи Microsoft Windows Server 2012 R2 Datacenter 9600.

Розроблений (виготовлений): Корпорація Microsoft.

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

Висновки:

1. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування AES (AES-128, AES-192, AES-256) відповідно до ДСТУ ISO/IEC 18033-3:2015, FIPS PUB 197 (в режимах ECB, CBC, CFB, OFB, CTR, що визначені NIST SP 800-38A; в режимі CMAC, що визначений NIST SP 800-38B; в режимі CCM, що визначений NIST SP 800-38C).
2. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування DES відповідно до FIPS PUB 46 (в режимах ECB, CBC, CFB, що визначені NIST SP 800-38A).
3. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування TDEA (з довжиною ключа 112 та 168 бітів) відповідно до ДСТУ ISO/IEC 18033-3:2015, ANSI X9.52-1998 (в режимах ECB, CBC, CFB, що визначені NIST SP 800-38A).
4. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування RC2 відповідно до IETF RFC 2268 (в режимах ECB, CBC, CFB, що визначені NIST SP 800-38A).
5. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування RC4 згідно опису, який наведено в документі R.L. Rivest "The RC4 Encryption Algorithm".
6. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування RSA, визначений PKCS#1 v.2.2 "RSA Cryptography Standart" (за схемою RSAES-PKCS1-v1_5).
7. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування MD2, MD4, MD5, які визначені в IETF RFC 1319, IETF RFC 1320, IETF RFC 1321 відповідно.
8. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-1, SHA-256, SHA-384, SHA-512, які визначені в ДСТУ ISO/IEC 10118-3:2005, FIPS PUB 180.
9. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного цифрового підпису RSA, визначений PKCS#1 v.2.2 "RSA Cryptography Standart" (за схемами RSASSA-PKCSl-vl_5 та RSASSA-PKCS-PSS).

10. В об'єкті експертизи правильно реалізовано коди автентифікації повідомлень HMAC-MD5, HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, визначені FIPS PUB 198, IETF RFC 2104.
11. В об'єкті експертизи правильно реалізовано генератор псевдовипадкових чисел, який визначений в документі "Криптографічні сервіси операційних систем Microsoft Windows ® Server 2012 R2 та Microsoft Windows ® 10 та їх додатків. "Роз'яснення щодо генерації ключових даних та управління ключами" (до вх. № 3820 від 05.08.2016).
12. В об'єкті експертизи правильно реалізовано алгоритм генерації ключових даних, який визначений в документі "Криптографічні сервіси операційних систем Microsoft Windows ® Server 2012 R2 та Microsoft Windows ® 10 та їх додатків. "Роз'яснення щодо генерації ключових даних та управління ключами" (до вх. № 3820 від 05.08.2016).
13. В об'єкті експертизи правильно реалізовано протокол SSL v.3.0 відповідно до IETF RFC 6101.
14. Об'єкт експертизи може бути використаний для криптографічного захисту конфіденційної інформації та відкритої інформації, вимога щодо захисту якої встановлена законом, при побудові засобів криптографічного захисту інформації видів "А" та "Б".

Особливі умови (рекомендації): дія експертного висновку поширюється на зразки об'єкта експертизи у складі операційної системи Microsoft Windows Server 2012 R2 Datacenter 9600, образ *iso якої має наступне значення геш-функції:

```
8CF082C4 2E415AF1 C079DDB2 5DA90C7B 9BFD9288 4F1C917D D1A80F7A DB407BCC,
```

у складі якої низькорівневі функції криптографічних перетворень реалізовано у програмних модулях, які мають наступні значення геш-функцій:

```
bcrypt.dll              1DACB763 09542FE5 D1967EF9 1B159409 479459E7 FC383C1F B0E30F43 8BFA2376
bcryptprimitives.dll    71B87A10 B6D365B2 A2179B86 048E4411 2EA66E28 C075E2F8 D7940765 5AD79234
cng.sys                 72CDCFBE 23544C3F E0FD9A93 E9A4102A 81AC4E45 11EBD7EC 0554BCBA 03A06B37
ksecdd.sys              AA70D6ED C285ED88 D0377FEE B228083C 448E8991 375A5B5B 4C2893C3 504F9FF5
ncrypt.dll              BA0DF5EA 4C47D408 921F1011 4D0C1430 1BE98443 409B0160 654FC044 AC0BE81E
```

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 09.09.2021.

Перший заступник Голови Служби О.М. Чаузов