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 № 04/03/02-3682

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: Засіб криптографічного захисту інформації "BitLocker Driver Encryption" операційної системи Microsoft Windows 10 Pro.

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-256) відповідно до ДСТУ ISO/IEC 18033-3:2015, FIPS PUB 197 (в режимі CBC, що визначений NIST SP 800-38A; в режимі XTS, що визначений NIST SP 800-38E; в режимі CCM, що визначений NIST SP 800-38C).
2. В об'єкті експертизи правильно реалізовано криптографічний алгоритм ускладнення "Elephant diffuser" згідно опису, який наведено в документі Niels Ferguson "AES-CBC+ Elephant diffuser. A Disk Encryption Algoritm for Windows Vista".
3. В об'єкті експертизи правильно реалізовано алгоритм захисту ключових даних, що 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).
4. Об'єкт експертизи може бути використаний для криптографічного захисту конфіденційної інформації та відкритої інформації, вимога щодо захисту якої встановлена законом.

Особливі умови (рекомендації): дія експертного висновку поширюється на зразки об'єкта експертизи у складі операційної системи Microsoft Windows 10 Pro, версії 1511, збірки 10586.104 від 13.02.2016, образ *iso якої має наступні значення геш-функцій:

для 32-х розрядних операційних систем MS Windows

A091E1DF B2E1C33E F0DD16B3 47766A2E E4C166BB BA258CDF AD24DE27 F064BB56

для 64-х розрядних операційних систем MS Windows

3D921141 6CA395EB DAA9D029 4B9B656E 9E9BB185 09C134D3 2D252C93 E1DC5C85,

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

для 32-х розрядних операційних систем MS Windows

fvevol.sys 39A8B590 33B922DC 9D8ABC2D FFDB3C0E 0A126FB3 F7012F4C 5880C2A0 B425BF4E

для 64-х розрядних операційних систем MS Windows

fvevol.sys F2E72AB3 A05BB357 665E833B 2EB22801 6E393C28 EC0E5CC9 2C1EB6ED 530C1C31

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