



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 № 04/03/02-3684

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 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-256) відповідно до ДСТУ ISO/IEC 18033-3:2015, FIPS PUB 197 (в режимі CBC, що визначений NIST SP 800-38A; 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 Algorithm for Windows Vista".
3. В об'єкті експертизи правильно реалізовано алгоритм захисту 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).
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 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 програмному модулі, який має наступне значення геш-функції:

fvevol.sys 7F6C82C2 DE69B3F9 914DF574 88DA9268 45025553 48C41771 CF57673D C1F895F3

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