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

12.03.2019 № 04/03/02-690

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 12.03.2019

м. Київ

Виданий: Товариству з обмеженою відповідальністю «Інститут комп'ютерних технологій» (код ЄДРПОУ 21541987)

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 06.03.2019 № 389.

Об'єкт експертизи: Бібліотека процедур криптографічного захисту інформації «Тайфун-PKI PKCS#11» Версія 1.02 UA.21541987.00016-01 90 03.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю «Інститут комп'ютерних технологій» (код ЄДРПОУ 21541987).

Експертний заклад: Товариство з обмеженою відповідальністю «ДОЛЯ І КО.ЛТД» (код ЄДРПОУ 01043342).

Висновки:

1. В об'єкті експертизи правильно реалізовані криптографічні алгоритми ДСТУ ГОСТ 28147:2009, ГОСТ 34.311-95, ДСТУ 4145-2002.
2. Об'єкт експертизи відповідає вимогам технічного завдання UA.21541987.00016-01 90 03, в частині реалізації функцій криптографічних перетворень (п. 4.2, 4.3.2, 4.8.1 – 4.8.9 ТЗ).
3. Формат посиленого сертифіката відкритого ключа, структура об'єктних ідентифікаторів для криптоалгоритмів, що є державними стандартами, формат списку відкликаних сертифікатів, формат підписаних даних, протокол фіксування часу, протокол визначення статусу сертифіката, які реалізовані та використовуються в об'єкті експертизи, відповідають вимогам наказу Міністерства юстиції України та Адміністрації Держспецзв'язку від 20.08.2012 № 1236/5/453 «Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису», зареєстрованого в Міністерстві юстиції України 20.08.2012 за № 1398/21710.
4. Формати криптографічних повідомлень, що реалізовані та використовуються в об'єкті експертизи, відповідають вимогам наказу Адміністрації Держспецзв'язку від 18.12.2012 № 739 «Про затвердження Вимог до форматів, криптографічних повідомлень», зареєстрованого в Міністерстві юстиції України 14.01.2013 за № 108/22640.
5. Об'єкт експертизи (як засіб криптографічного захисту інформації категорій «К» та «Ш») може бути використаний 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.
6. Ступень обмеження доступу до інформації, цілісність та підтвердження автентичності якої забезпечується об'єктом експертизи (як засобом криптографічного захисту інформації категорії «П»), визначається вимогами до засобів КЗІ видів «А» та «Б» або автоматизованих систем, у складі яких він використовується.