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 № 04/03/02-691

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: Комплекс програмних засобів реалізації інфраструктури відкритих ключів «Тайфун-РКІ» версія 1.02 UA.21541987.00016-01 90 04.

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. Програмний засіб криптографічного захисту інформації, що входить до складу об'єкта експертизи, відповідає Бібліотеці процедур криптографічного захисту інформації «Тайфун-РКІ PKCS#11» Версія 1.02 UA.21541987.00016-01 90 03, яка має чинний експертний висновок Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 12.03.2019 № 04/03/02-690.
2. Об'єкт експертизи правильно використовує функції криптографічних перетворень, що реалізовані у Бібліотеці процедур криптографічного захисту інформації «Тайфун-РКІ PKCS#11» Версія 1.02 UA.21541987.00016-01 90 03.
3. Об'єкт експертизи відповідає вимогам технічного завдання UA.21541987.00016-01 90 04 в частині реалізації функцій криптографічних перетворень (п.4.1.3, 4.2.1 – 4.2.4, 4.4.1, 4.4.3, 4.4.4, 4.4.6 – 4.4.8, 4.4.11 – 1.4.14 ТЗ).
4. 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, що реалізовані та використовуються в об'єкті експертизи, відповідають вимогам наказу Міністерства юстиції України та Адміністрації Державної служби спеціального зв'язку та захисту інформації України 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.
5. Формати криптографічних повідомлень та протоколи узгодження ключів, які реалізовані та використовуються в об'єкті експертизи, відповідають 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.