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

18.03.2019 № 04/03/02-750

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 18.03.2019 м. Київ

Виданий: Товариству з обмеженою відповідальністю «Авест-Україна» (код ЄДРПОУ 37963188)

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 15.03.2019 № 391.

Об'єкт експертизи: Програмний виріб взаємодії з програмно-апаратними засобами криптографічного захисту інформації «AvestPKCS#11».

Розроблений (виготовлений): Товариством з обмеженою відповідальністю «Авест-Україна» (код ЄДРПОУ 37963188).

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

Висновки:

1. В об'єкті експертизи правильно реалізовано криптографічні алгоритм гешування ГОСТ 34.311-95.
2. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-1, SHA-256, визначені ДСТУ ISO/IEC 10118-3:2005.
3. Формат посилених сертифікатів відкритих ключів, формат списків відкликаних сертифікатів, формат підписаних даних, структура об'єктних ідентифікаторів для криптоалгоритмів, що є державними стандартами, які створюються та/або 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 у Міністерстві юстиції України 20.08.2012 за № 1398/21710.
4. Прикладний програмний інтерфейс, який реалізовано в об'єкті експертизи, відповідає вимогам спільного наказу Міністерства юстиції України та Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 27.12.2013 № 2782/5/689 «Про затвердження вимог до алгоритмів, форматів та інтерфейсів, що реалізуються у засобах шифрування та надійних засобах електронного цифрового підпису», зареєстрованого в Міністерстві юстиції України 27.12.2013 за № 2228/24759.
5. Об'єкт експертизи відповідає вимогам технічного завдання «Розробка програмного виробу взаємодії з програмно-апаратними засобами криптографічного захисту інформації», шифр «AvestPKCS#11» в частині реалізації функцій криптографічних перетворень.

6. Об'єкт експертизи 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, видів «А» та «Б».

Особливі умови (рекомендації): дія експертного висновку поширюється на зразки об'єкта експертизи, у яких криптографічні перетворення здійснюються програмним модулем, що має наступні значення геш-функції:

avcryptokinxt.dll	72C54E6A CE13BFC9 329B7CA1 2FEE5811 267B2A6B AC920C98 DD98CFEA BA777DBA

Розрахунок геш-функції 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 15.03.2024.

Перший заступник Голови Служби О.М. Чаузов