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

19.01.18 № 04/02/03-171

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: __.01.2018 м. Київ

Виданий: Приватному акціонерному товариству «Інститут інформаційних технологій» (код ЄДРПОУ 22723472).

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 18.01.2018 № 330.

Об'єкт експертизи: КЛЮЧ ЕЛЕКТРОННИЙ «КРИСТАЛ-1» СААД.469535.040.

Розроблений (виготовлений): Приватним акціонерним товариством «Інститут інформаційних технологій» (код ЄДРПОУ 22723472).

Експертний заклад: Адміністрація Державної служби спеціального зв'язку та захисту інформації України (код ЄДРПОУ 34620942).

Висновки:

1. В об'єкті експертизи правильно реалізовано криптографічні алгоритми ДСТУ ГОСТ 28147:2009, ГОСТ 34.311-95, ДСТУ 4145-2002.
2. В об'єкті експертизи алгоритм генерації випадкових двійкових послідовностей відповідає додатку А ДСТУ 4145-2002.
3. В об'єкті експертизи внутрішній апаратний генератор випадкових послідовностей та алгоритм генерації ключових даних відповідає документу «Методика генерації ключових даних СААД.468244.020 Д1.05».
4. В об'єкті експертизи правильно реалізовано протокол автономного узгодження ключів в групі точок еліптичної кривої типу Діффі-Геллмана (KANIDH), визначений п. 8.2 ДСТУ ISO/IEC 15946-3:2006.
5. Протокол узгодження ключа Діффі-Геллмана ECDH, що реалізований в об'єкті експертизи, відповідно 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.
6. Алгоритми формування ключів шифрування ключів та захисту особистих ключів електронного цифрового підпису та особистих ключів шифрування, формати транспортних контейнерів особистих ключів електронного цифрового підпису та особистих ключів шифрування, контейнерів зберігання особистих ключів електронного цифрового підпису, особистих ключів шифрування та сертифікатів відкритих ключів, які реалізовані 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 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.

7. В об'єкті експертизи забезпечується захист записаних даних від несанкціонованого доступу від безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання.
8. Об'єкт експертизи може бути використаний для автентифікації особи під час надання та/або отримання електронних послуг.
9. Об'єкт експертизи відповідає вимогам технічного завдання ЄААД.469535.040 ТЗ з доповненнями № 1, 2, 3 до нього, в частині реалізації функцій криптографічних перетворень.
10. 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.

Особливі умови (рекомендації): дія експертного висновку поширюється на зразки об'єкта експертизи, виготовлені відповідно до технічних умов ТУ У 30.0-22723472-001:2007 із змінами № 1, 2, 3.

Термін дії експертного висновку – до 18.01.2023.

Перший заступник Голови Служби О.М. Чаузов