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

06.06.2018 № 04/03/02-1321

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 06.06.2018 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 01.06.2018 № 347.

Об'єкт експертизи: Модуль криптографічний «Гряда-61» ЄААД.469535.044.

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 внутрішній апаратний генератор випадкових послідовностей, алгоритм генерації випадкових двійкових послідовностей та порядок генерації ключових даних відповідають документу «Методика генерації ключових даних ЄААД.468244.020 Д1.05».
3. 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.
4. В об'єкті експертизи криптографічний протокол розподілу ключів ECDH реалізовано відповідно до вимог наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 18.12.2012 № 739 «Про затвердження Вимог до форматів криптографічних повідомлень», зареєстрованого у Міністерстві юстиції України 14.01.2013 за № 108/22640.
5. Інтерфейси засобів криптографічного захисту інформації, реалізовані 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.
6. Об'єкт експертизи відповідає вимогам технічного завдання ЄААД.469535.044 ТЗ із Доповненнями № 1, № 2, № 3 до нього, в частині реалізації функцій криптографічних перетворень.

7. 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 26.2-22723472-027:2016 із Зміною № 1.

Термін дії експертного висновку – до 01.06.2023.

Перший заступник Голови Служби О.М. Чаузов