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

26.12.17 № 04-3507

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: __.12.2017 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 22.12.2017 № 328.

Об'єкт експертизи: КРИПТОМОДУЛЬ МЕРЕЖНИЙ «ГРЯДА-301» ЄААД.469535.049, ЄААД.469535.240, ЄААД.469535.241, ЄААД.469535.243.

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 (в режимах простої заміни, гамування зі зворотнім зв'язком та вироблення імітовставки), ГОСТ 34.311-95, ДСТУ 4145-2002.
2. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування RSA, визначений PKCS#1 v2.2 RSA Cryptography Standard (за схемою RSAES-PKCS1_v1_5).
3. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного цифрового підпису ECDSA, визначений ДСТУ ISO/IEC 14888-3:2014.
4. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного цифрового підпису RSA, визначений PKCS#1 v2.2: RSA Cryptography Standard (за схемою RSASSA-PKCSl-vl_5).
5. 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.
6. В об'єкті експертизи забезпечується захист записаних даних від несанкціонованого доступу, від безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання.
7. Формати криптографічних повідомлень та протоколи розподілу ключів, що реалізовані та/або 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.

8. Об'єкт експертизи відповідає вимогам технічного завдання ЄААД.469535.049 ТЗ із Доповненнями № 1, № 2, № 3, № 4, № 5, № 6 в частині реалізації функцій криптографічних перетворень.
9. 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 26.2-22723472-003:2017.

Термін дії експертного висновку – до 22.12.2022.

Перший заступник Голови Служби О.М. Чаузов