Прим. № 1

АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ
(АДМІНІСТРАЦІЯ ДЕРЖСПЕЦЗВ'ЯЗКУ)

вул. Солом'янська, 13, м. Київ, 03110, тел. (044) 281-92-10, факс: (044) 281-94-83,
e-mail: info@dsszzi.gov.ua, сайт: www.dsszzi.gov.ua, код згідно з ЄДРПОУ 34620942

23.06.2020 № 04/03/02-1556 На № _____ від _____

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 23.06.2020 м. Київ

Виданий: Товариству з обмеженою відповідальністю «С.І.Т» (код ЄДРПОУ 3873869)

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 19.06.2020 № 456.

Об'єкт експертизи: Блок захищений системний інтегрований «ЗаСІБ» UA.IIT.38773869.00004-01.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю «С.І.Т» (код ЄДРПОУ 3873869).

Експертний заклад: Товариство з обмеженою відповідальністю «АЛЬТАЇР-775» (код ЄДРПОУ 25197618).

Висновки:

1. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування AES, визначений ДСТУ ISO/IEC 18033-3:2015 (в режимі CBC, визначеному ДСТУ ISO/IEC 10116:2014, із довжиною ключа 256 біт).
2. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування AES, визначений ДСТУ ISO/IEC 18033-3:2015 (у режимі GCM, визначеному NIST SP 800-38D, із довжиною ключа 256 біт).
3. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного цифрового підпису ECDSA, визначений ДСТУ ISO/IEC 14888-3:2015.
4. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-1, SHA-256, SHA-384, SHA-512, визначені ДСТУ ISO/IEC 10118-3:2005.
5. В об'єкті експертизи правильно реалізовано криптографічний алгоритм автентифікації повідомлень HMAC-SHA-384, визначений ДСТУ ISO/IEC 9797-2:2015.
6. В об'єкті експертизи правильно реалізовано криптографічний протокол Діффі-Гелмана (ECDH), визначений ДСТУ ISO/IEC 15946-3:2006.
7. В об'єкті експертизи протокол встановлення захищених мережевих з'єднань реалізовано згідно вимог IETF RFC 7296 Internet Key Exchange Protocol Version 2 (IKEv2).
8. В об'єкті експертизи протокол шифрування мережевого трафіку ESP реалізовано згідно вимог IETF RFC 4303.

9. В об’єкті експертизи алгоритм генерації ключових даних та алгоритм ініціалізації генератора псевдовипадкових чисел відповідає документу «Блок захищений системний інтегрований «Засіб». Методика генерації та розподілу ключових даних UA.IIT.38773869.00004-01 93 01.

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 26.2-38773869-002:2020.

Термін дії експертного висновку – до 19.06.2025.

Голова Служби Валентин ПЕТРОВ