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

12.06.2022 № 04-197/ВС1 На № _____ від _____

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 12.06.2022 м. Київ

Виданий: Товариству з обмеженою відповідальністю «С.І.Т» (код ЄДРПОУ 38773869)

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 10.06.2022 № 547.

Об'єкт експертизи: Криптомодуль «OLYMP» 38773869.00005-01.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю «С.І.Т» (код ЄДРПОУ 38773869).

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, визначені ГОСТ 28147-89 (у режимі простої заміни, гамування, гамування зі зворотним зв'язком та обчислення імітовставки), ДСТУ 7624:2014 (в режимах ECB, OFB, CFB, CBC, CTR, GCM, KW), ДСТУ 7564:2014 (у режимах Купина-256, Купина-384, Купина-512), ДСТУ 4145-2002 (у поліноміальному базисі), ГОСТ 34.311-95.
2. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування AES, визначений ДСТУ ISO/IEC 18033-3:2015 (у режимах ECB, CTR, CFB, CBC, OFB, визначених ДСТУ ISO/IEC 10116:2019, та у режимі GCM, визначеному NIST SP 800-38D, з довжиною ключа 128, 192, 256 біт).
3. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування RSA, визначений IETF RFC 3447 (за схемою RSAES-OAEP).
4. В об'єкті експертизи правильно реалізовано криптографічний алгоритм електронного підпису RSA, визначений ДСТУ ISO/IEC 14888-2:2015, IETF RFC 3447 (за схемами RSASSA-PKCS1-v1_5, RSASSA-PSS).
5. В об'єкті експертизи правильно реалізовано криптографічний алгоритм обчислення та перевіряння електронного підпису ECDSA, визначений ДСТУ ISO/IEC 14888-3:2019.
6. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-1, SHA-256, SHA-384, SHA-512, визначені ДСТУ ISO/IEC 10118-3:2005.
7 В об'єкті експертизи правильно реалізовано криптографічний алгоритм гешування SHA-3, визначений ISO/IEC 10118-3:2018.

8. В об'єкті експертизи правильно реалізовано протокол автономного узгодження ключів в групі точок еліптичної кривої типу Діффі-Геллмана, визначений п. Е.7 додатку Е ДСТУ ISO/IEC 11770-3:2015.
9. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування коду автентифікації CMAC, визначений ДСТУ 7624:2014 (у режимі CMAC).
10. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування коду автентифікації повідомлень CBC-MAC за алгоритмом AES, визначений ДСТУ ISO/IEC 9797-1:2015.
11. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування коду автентифікації повідомлень HMAC, визначений ДСТУ 9797-2:2015.
12. В об'єкті експертизи формування параметрів детермінованого генератора псевдовипадкових біт реалізовано відповідно до вимог документу «Методика ініціалізації генератора псевдовипадкових послідовностей 38773869.00005-01 90 01».
13. В об'єкті експертизи захист особистих ключів здійснюється відповідно до вимог документу «Методика захисту особистих ключів користувачів 38773869.00005-01 90 02».
14. Методи захисту, реалізовані в об'єкті експертизи, відповідають вимогам до засобів криптографічного захисту інформації класу Б1 (захист від порушника другого рівня), визначеним в Положенні про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженому наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141, зареєстрованим в Міністерстві юстиції України 30.07.2007 за № 862/14129.
15. В об'єкті експертизи правильно реалізовано методи захисту, визначені пунктом 3 «Вимог до засобів криптографічного захисту інформації, призначених для захисту таємної інформації, яка не становить державної таємниці, та конфіденційної інформації в державних органах, органах місцевого самоврядування, на підприємствах, в установах та організаціях, які належать до сфери їх управління, військових формуваннях, які створені відповідно до закону», затверджених наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 07.05.2021 № 278, зареєстрованим у Міністерстві юстиції України 26.05.2021 за № 696/36318.
16. Об'єкт експертизи відповідає вимогам технічного завдання UA.38773869.00005-01 ТЗ 02 в частині реалізації функцій криптографічних перетворень.
17. 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 26.2-38773869-005:2022.

Термін дії експертного висновку – до 12.06.2027.

Заступник Голови Служби Олександр ПОТІЙ