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


07.09.2021 № 04/05/02-2523 На № _____ від _____

# ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 07.09.2021 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 07.09.2021 № 513.

Об'єкт експертизи: Програмне забезпечення програмного-технічного комплексу центру сертифікації ключів електронного цифрового підпису за алгоритмами ДСТУ 4145-2002, RSA, ECDSA UA.38773869.00001-01.

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 ДСТУ ГОСТ 28147:2009 (у режимах простої заміни, гамування, гамування із зворотнім зв'язком та обчислення імітовставки), ДСТУ 7564:2014 (у режимах Купина-256, Купина-384, Купина-512), 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 правильно реалізовано криптографічний алгоритми шифрування AES визначений ДСТУ ISO/IEC 18033-3:2015 (у режимах ECB, CBC, визначені ДСТУ ISO/IEC 10116:2019).
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 гешування SHA-224, визначений FIPS PUB 180-4.
6. 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.
7. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного підпису RSA, визначений PKSC#1 v.2.2 «RSA Cryptography Standard» (за схемами RSASSA-PKCSl-vl_5, RSASSA-PSS).

8. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного підпису ECDSA, визначений ДСТУ ISO/IEC 14888-3:2019, ANSI X9.62:2005.
9. Алгоритм генерації ключових даних, що реалізовано в об'єкті експертизи, відповідає вимогам документу «Програмно-технічний комплекс центру сертифікації ключів електронного цифрового підпису за алгоритмами ДСТУ 4145-2002, RSA, ECDSA. Методика генерації ключових даних» (до вх. 6337 від 26.12.2016).
10. Формат та вміст статусів сертифікатів та запитів на їх отримання відповідає вимогам IETF RFC 6960 «Internet Public Key Infrastructure Online Certificate Status Protocol».
11. Формат та вміст сертифікатів і списків відкликаних сертифікатів відповідають вимогам ДСТУ ETSI EN 319 412:2016 (ETSI EN 319 412:2016, IDT) «Електронні підписи й інфраструктури (ESI). Профілі сертифікатів».
12. Формат та вміст підписаних даних (криптографічних повідомлень типу «signed-data») відповідають вимогам ДСТУ ETSI EN 319 122:2016 (ETSI EN 319 122:2016, IDT). Електронні підписи й інфраструктури (ESI). Цифрові підписи CAdES».
13. Формат та вміст позначок часу TSP та запитів на їх отримання відповідають вимогам ДСТУ ETSI EN 319 422:2016 (ETSI EN 319 422:2016, IDT). Електронні підписи й інфраструктури. Протокол мітки часу та профілі токенів мітки часу».
14. В об'єкті експертизи формати запитів на сертифікацію реалізовано відповідно PKCS#10 «Certification Request Syntax Standard».
15. Методи захисту, реалізовані в об'єкті експертизи, відповідають вимогам до засобів криптографічного захисту інформації класу Б2 (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 (зі змінами).
16. Об'єкт експертизи відповідає вимогам технічного завдання UA.38773869.00001-01 ТЗ 01 із Доповненнями № 1, № 2 № 3 до нього, 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.
18. Об'єкт експертизи може бути використаний для надання кваліфікованих електронних довірчих послуг.

Особливі умови (рекомендації): дія експертного висновку поширюється на зразки об'єкта експертизи, виготовлені відповідно до технічних умов ТУ 72.2-38773869-001:2016 зі Змінами № 1, № 2, № 3 до них.

Термін дії експертного висновку – до 07.09.2026.

Голова Служби Юрій ЩИГОЛЬ