



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

вул. Солом'яньська, 13, м. Київ, 03110, тел. (044) 281-93-08, факс: (044) 281-94-83,  
e-mail: info@cip.gov.ua, сайт: www.cip.gov.ua, код згідно з ЄДРПОУ 34620942

29.08.2023 № 04/05/02 - 1066/ДС-1 На № \_\_\_\_\_ від \_\_\_\_\_

**ЕКСПЕРТНИЙ ВИСНОВОК**

Дата видачі: 29.08.2023

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 29.08.2023 № 589.

Об'єкт експертизи: Програмне забезпечення Комплексу програмного центру сертифікації ключів «ІТ ЦСК-1» (версія 1.3) ЄААД.468244.021.

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:**

- В об'єкті експертизи правильно реалізовано криптографічні алгоритми, визначені ДСТУ 7624-2014 (у режимах «Калина-256/256-CFB», «Калина-256/256-CBC», «Калина-256/256-SMAC»), ДСТУ 4145-2002 (у поліноміальному базисі), ДСТУ 7564-2014 (у режимі «Купина-256»), ГОСТ 28147-89 (у режимах гамування зі зворотним зв'язком та обчислення імітовставки), ГОСТ 34.311-95.
- В об'єкті експертизи правильно реалізовано криптографічні алгоритми шифрування AES, TDEA, визначені ДСТУ ISO/IEC 18033-3:2015 (у режимі CBC, визначеному ДСТУ ISO/IEC 10116:2019).
- В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного підпису ECDSA, визначений ДСТУ ISO/IEC 14888-3:2019.
- В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-1, SHA-256, SHA-384, SHA-512, визначені ДСТУ ISO/IEC 10118-3:2023.
- В об'єкті експертизи правильно реалізовано криптографічний алгоритм гешування SHA-224, визначений FIPS PUB 180-4.
- В об'єкті експертизи правильно реалізовано протоколи узгодження ключів типу Діффі-Геллмана (DH, ECDH), визначені ДСТУ ISO/IEC 11770-3:2023.
- В об'єкті експертизи механізм генерації ключових даних відповідає документу «Методика генерації ключових даних ЄААД.468244.020 Д1.05».
- Формат та вміст статусів сертифікатів та запитів на їх отримання відповідає вимогам IETF RFC 6960 «Internet Public Key Infrastructure Online Certificate Status Protocol».

9. 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».

10. 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».

11. 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».

12. 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.

13. Об'єкт експертизи відповідає вимогам технічного завдання ЄААД.468244.021 ТЗ із доповненнями № 1, № 2, № 3, № 4 до нього, в частині реалізації функцій криптографічних перетворень.

14. 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.

15. Об'єкт експертизи може бути використаний у складі програмно-технічного комплексу, що забезпечує виконання функцій, пов'язаних з наданням кваліфікованих електронних довірчих послуг.

Особливі умови (рекомендації): дія експертного висновку поширюється на зразки об'єкта експертизи, виготовлені відповідно до технічних умов ТУ У 62.0-22723472-028:2016 зі Зміною № 1:2023.

Термін дії експертного висновку – до 29.08.2028.

Голова Служби

Юрій ЩИГОЛЬ