



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

вул. Солом'янська, 13, м. Київ, 03110, тел. (044) 281-93-08,
e-mail: info@cip.gov.ua, web: cip.gov.ua
Код ЄДРПОУ 34620942

від 12.08 2025 р. № 04/03/02- На № _____ від _____ 20__ р.
19066/2025/ВН

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 12.08.2025

м. Київ

Виданий: Товариству з обмеженою відповідальністю «САЙФЕР ПРО»
(код ЄДРПОУ 42125815)

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 06.08.2025 № 656.

Об'єкт експертизи: Користувацькі програмні засоби криптографічного захисту інформації зі складу «Системи криптографічного захисту інформації «Шифр-Х.509» версії 2».

Розроблений (виготовлений): Товариством з обмеженою відповідальністю «САЙФЕР ПРО»
(код ЄДРПОУ 42125815).

Експертний заклад: Товариство з обмеженою відповідальністю «ЗАХИСТ.ЮЕЙ»
(код ЄДРПОУ 42292899).

Висновки:

1. В об'єкті експертизи правильно реалізовано криптографічні алгоритми, визначені ДСТУ ГОСТ 28147:2009 (у режимах простої заміни, гамування, гамування зі зворотним зв'язком та обчислення імітовставки), ГОСТ 34.311-95, ДСТУ 4145-2002 (в поліноміальному базисі), ДСТУ 7624:2014 (у режимах ECB, OFB, CFB, CBC, CTR, CMAC), ДСТУ 7564:2014.
2. В об'єкті експертизи алгоритм генерації випадкових двійкових послідовностей відповідає додатку А ДСТУ 4145-2002.
3. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування TDEA, визначений ДСТУ ISO/IEC 18033-3:2015 (в режимах ECB, OFB, CFB, CBC, CMAC, визначених ДСТУ ISO/IEC 10116:2019).
4. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування AES, визначений ДСТУ ISO/IEC 18033-3:2015 (в режимах ECB, OFB, CFB, CBC, CTR, CMAC, визначених ДСТУ ISO/IEC 10116:2019).
5. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування RSA, визначений ДСТУ ISO/IEC 18033-2:2015.

6. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного підпису RSA, визначений ДСТУ ISO/IEC 14888-3:2019.
7. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного підпису ECDSA, визначений ДСТУ ISO/IEC 14888-3:2019.
8. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256, визначені ДСТУ ISO/IEC 10118-3:2023.
9. В об'єкті експертизи правильно реалізовано протокол автономного узгодження ключів в групі точок еліптичної кривої типу Діффі-Геллмана, визначений п. Е.7 додатка Е ДСТУ ISO/IEC 11770-3:2023.
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 319 412:2021. «Електронні підписи та інфраструктури (ESI). Профілі сертифікатів».
12. Формат та вміст підписаних даних відповідають вимогам ДСТУ ETSI EN 319 132-1:2022 (ETSI EN 319 132-1 V1.2.1 (2022-02), IDT) «Електронні підписи та інфраструктури (ESI). Цифрові підписи XAdES. Частина 1. Структурні блоки та базові підписи XAdES».
13. Формат та вміст підписаних даних відповідають вимогам ДСТУ ETSI EN 319 132-2:2021 (ETSI EN 319 132-2 V1.1.1 (2016-04), IDT) «Електронні підписи та інфраструктури (ESI). Цифрові підписи XAdES. Частина 2. Розширені підписи XAdES».
14. Формат та вміст підписаних даних відповідають вимогам ДСТУ ETSI EN 319 162-1:2021 (ETSI EN 319 162-1 V1.1.1 (2016-04), IDT) «Електронні підписи та інфраструктури (ESI). Контейнери пов'язаних підписів (ASiC). Частина 1. Структурні блоки та базові контейнери ASiC».
15. Формат та вміст підписаних даних відповідають вимогам ДСТУ ETSI EN 319 162-2:2021 (ETSI EN 319 162-2 V1.1.1.1 (2016-04), IDT) «Електронні підписи та інфраструктури (ESI). Контейнери пов'язаних підписів (ASiC). Частина 2. Додаткові контейнери ASiC».
16. Формат та вміст підписаних даних відповідають вимогам ДСТУ ETSI EN 319 122-1:2021 (ETSI EN 319 122-1 V1.2.1 (2021-10), IDT) «Електронні підписи та інфраструктури (ESI). Цифрові підписи CAdES. Частина 1. Структурні блоки та базові підписи CAdES».
17. Формат та вміст підписаних даних відповідають вимогам ДСТУ ETSI EN 319 122-2:2021 (ETSI EN 319 122-2 V1.2.1 (2021-10), IDT) «Електронні підписи та інфраструктури (ESI). Цифрові підписи CAdES. Частина 2. Розширені підписи CAdES».
18. Формат та вміст підписаних даних відповідають вимогам ДСТУ ETSI EN 319 142-1:2016 (ETSI EN 319 142-1:2016, IDT) «Електронні підписи та інфраструктури. Цифрові підписи PAdES. Частина 1. Структурні елементи та базові PAdES підписи».
19. Формат та вміст підписаних даних відповідають вимогам ДСТУ ETSI EN 319 142-2:2016 (ETSI EN 319 142-2:2016, IDT) «Електронні підписи та інфраструктури. Цифрові підписи PAdES. Частина 2. Додаткові профілі підписів PAdES».
20. 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 та інфраструктури. Протокол мітки часу та профілі токенів мітки часу».
21. В об'єкті експертизи алгоритм формування початкових значень генератора випадкових двійкових послідовностей відповідає вимогам документа «Методика ініціалізації генератора випадкових двійкових послідовностей. UA.33349855.00001 – 01 94 01».
22. Об'єкт експертизи відповідає вимогам технічного завдання ТЗ У 72.2-42125815-002:2020 в частині реалізації функцій криптографічних перетворень.
23. Методи захисту, реалізовані в об'єкті експертизи, відповідають вимогам до засобів криптографічного захисту інформації класу В2 (захист від порушника першого та нульового

рівнів), визначеним в Положенні про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженому наказом Адміністрації Держспецзв'язку № 141 від 20.07.2007, зареєстрованим в Міністерстві юстиції України 30.07.2007 за № 862/14129 (зі змінами).

24. 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.

25. Об'єкт експертизи при спільному застосуванні із криптомодулем мережним «Шифр-HSM» МКМ 42125815.ТД-01, що має діючий експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації, забезпечує створення та функціонування довіреного каналу для застосування генерації сертифікатів та створення підпису, який відповідає вимогам профілів захисту, визначених ДСТУ EN 419211-4:2016 (EN 419211-4:2016 IDT), ДСТУ EN 419211-5:2016 (EN 419211-5:2016 IDT) та може бути використаний у якості засобу кваліфікованого електронного підпису чи печатки для надання електронних довірчих послуг.

Особливі умови (рекомендації): дія експертного висновку поширюється на зразки об'єкта експертизи, виготовлені відповідно до технічних умов ТУ У 62.0-42125815-002:2025.

Термін дії експертного висновку – до 06.08.2030.

Голова Служби



Олександр ПОТІЙ