Прим. № 1

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

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

18.02.2025 № 04/04/02-4376/2025/ВН На № _____ від _____

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 18.02.2025 м. Київ

Виданий: Товариству з обмеженою відповідальністю «ДІСІЄНСІ» (код ЄДРПОУ 41564452)

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 14.02.2024 № 639.

Об'єкт експертизи: Засіб програмний «Бібліотека криптографічних перетворень «АРТ-ЛІБ» UA.41564452.00001-01.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю «ДІСІЄНСІ» (код ЄДРПОУ 41564452).

Експертний заклад: Товариство з обмеженою відповідальністю «Безпека та інновації інформаційних систем» (код ЄДРПОУ 41449076).

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, обчислення імітовставки), ДСТУ 7624:2014 (у режимах «Калина-128/128-ECB, OFB, CFB, CTR, CMAC», «Калина-128/256-ECB, OFB, CFB, CTR, CMAC», «Калина-256/256-ECB, OFB, CFB, CTR, CMAC», «Калина-256/512-ECB, OFB, CFB, CTR, CMAC», «Калина-512/512-ECB, OFB, CFB, CTR, CMAC»), ДСТУ 7564:2014 (у режимах «Купина-256», «Купина-384», «Купина-512»), ДСТУ 4145-2002 (у поліноміальному базисі для ступеня розширення основного поля 163, 167, 173, 179, 191, 233, 257, 307, 367, 431, 571), ГОСТ 34.311-95.
2. В об'єкті експертизи правильно реалізовано криптографічні алгоритми шифрування AES, TDEA, визначені ДСТУ ISO/IEC 18033-3:2015 (у режимах ECB, OFB, CFB, CBC, CTR, визначених ДСТУ ISO/IEC 10116:2019).
3. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного підпису ECDSA, визначений ДСТУ ISO/IEC 14888-3:2019 (для еліптичних кривих NIST P-192, NIST P-256, NIST P-384, NIST P-521).
4. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного підпису RSA, визначений ДСТУ ISO/IEC 14888-2:2015 (для довжин відкритого ключа 1024, 2048, 3072, 4096).

5. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, визначені ДСТУ ISO/IEC 10118-3:2023.
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 11770-3:2023 (в поліноміальному базисі для ступеня розширення основного поля 163, 167, 173, 179, 191, 233, 257, 307, 367, 431, 571).
7. В об'єкті експертизи правильно реалізовано формат підписаних даних, визначений ДСТУ ETSI EN 319 122-1:2016 та ДСТУ ETSI EN 319 122-2:2016.
8. В об'єкті експертизи правильно реалізовано формати позначки часу та тестової позначки часу, визначені ДСТУ ETSI EN 319 422:2016.
9. В об'єкті експертизи правильно реалізовано формати запиту та відповіді про статус сертифікату, визначені IETF RFC 6960.
10. В об'єкті експертизи правильно реалізовано формати сертифікатів відкритих ключів, визначені ДСТУ ETSI EN 319 412-1:2016, ДСТУ ETSI EN 319 412-2:2016, ДСТУ ETSI EN 319 412-3:2016, ДСТУ ETSI EN 319 412-4:2016.
11. В об'єкті експертизи формат тестової заяви на формування сертифікату відкритого ключа відповідає вимогам PKCS#10.
12. В об'єкті експертизи алгоритм ініціалізації генератора випадкових послідовностей відповідає вимогам документу «Методика ініціалізації генератора випадкових послідовностей UA.41564452.00001-01 90 01».
13. В об'єкті експертизи алгоритми захисту ключової інформації відповідають вимогам документу «Методика захисту ключової інформації на зовнішніх носіях UA.41564452.00001-01/ME».
14. 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 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. Об'єкт експертизи відповідає вимогам технічного завдання UA.41564452.00001-01 ТЗ 01 із Доповненням № 2 до нього, в частині реалізації функцій криптографічних перетворень (п. 5.6.1 – 5.6.6, 5.7.1, 5.9.1, 5.9.4 технічного завдання).
16. 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 62.0-41564452-001:2025.

Термін дії експертного висновку – до 14.02.2030.

Голова Служби Олександр ПОТІЙ