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

17.12.2021 № 04/05/02-3771 На № _____ від _____

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 17.12.2021 м. Київ

Виданий: Товариству з обмеженою відповідальністю «САЙБЕР ЛАБ» (код ЄДРПОУ 43927493)

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 17.12.2021 № 528.

Об'єкт експертизи: Комплекс програмний криптографічного захисту інформації «Криптосервер 2.0» UA.43927493.00001-01.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю САЙБЕР ЛАБ» (код ЄДРПОУ 43927493).

Експертний заклад: Адміністрація Державної служби спеціального зв'язку та захисту інформації України (код ЄДРПОУ 34620942).

Висновки:

1. В об'єкті експертизи криптографічні алгоритми реалізовано відповідно до вимог ДСТУ ГОСТ 28147:2009 (у режимі гамування, гамування зі зворотним зв'язком та обчислення імітовставки), ДСТУ 7624:2014 (у режимах ECB, CFB, CBC), ДСТУ 7564:2014 (у режимах Купина-256, Купина-512), ГОСТ 34.311-95, ДСТУ 4145-2002.
2. В об'єкті експертизи алгоритм генерації випадкових послідовностей відповідає додатку А ДСТУ 4145-2002.
3. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування AES (AES-128, AES-192, AES-256), визначений ДСТУ ISO/IEC 18033-3:2015 (у режимі CBC, визначеному ДСТУ ISO/IEC 10116:2019).
4. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-1, SHA-256, SHA-512, визначені ДСТУ ISO/IEC 10118-3:2005, FIPS PUB 180-4 Federal Information Processing Standards Publication.
5. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного підпису RSA, визначений ДСТУ ISO/IEC 14888-3:2019.
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 генерація ключових даних та управління ключами відповідає вимогам документу «Методика генерації ключових даних та управління ключами UA.OBCT.00001 01 90 01-1».

8. 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.
9. 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.
10. Об'єкт експертизи відповідає вимогам технічного завдання UA.43927493.00001-01ТЗ 01 в частині реалізації функцій криптографічних перетворень.
11. 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 62.0-43927493-001:2021.

Термін дії експертного висновку – до 17.12.2026.

Голова Служби Юрій ЩИГОЛЬ