



**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 10.08.2026 р. № 04/03/02-21165/2026/ВМ На № _____ від _____ 20__ р.

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 10.08.2026

м. Київ

Виданий: Приватному підприємству «СМАРТ ЛАБ» (код ЄДРПОУ 45217327)

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 10.08.2026 № 682.

Об'єкт експертизи: Засіб криптографічного захисту інформації на базі платформи JCOP 4.5.

Розроблений (виготовлений): Приватним підприємством «СМАРТ ЛАБ» (код ЄДРПОУ 45217327).

Експертний заклад: Товариство з обмеженою відповідальністю «Альтаір-775» (код ЄДРПОУ 25197618).

Висновки:

1. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння цифрового підпису, визначений ДСТУ 4145-2002 (у поліноміальному базисі).
2. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння цифрового підпису ECDSA, визначений ДСТУ ISO/IEC 14888-3:2019 (у поліноміальному базисі).
3. В об'єкті експертизи правильно реалізовано протокол автономного узгодження ключів в групі точок еліптичної кривої типу Діффі-Геллмана, визначений ДСТУ ISO/IEC 11770-3:2023 (у поліноміальному базисі).
4. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування AES, визначений ДСТУ ISO/IEC 18033-3:2015 із довжиною ключа 128 та 256 (у режимах ECB, CBC, визначених ДСТУ ISO/IEC 10116:2019, та CMAC, визначеному ДСТУ ISO/IEC 9797-1:2015 (NIST SP 800-38B)).
5. В об'єкті експертизи механізми автентифікації відповідають вимогам документу «Методика взаємної автентифікації засобу криптографічного захисту інформації на базі платформи JCOP 4.5 та зовнішніх пристроїв. 45217327.467649.001 M1».

6. Об'єкт експертизи відповідає вимогам технічного завдання на дослідно-конструкторську роботу «Розробка засобу криптографічного захисту інформації на базі платформи JCOP 4.5», в частині реалізації функцій криптографічних перетворень (п. 5.1.1 – 5.1.5, 5.1.15, 5.2, розділ 8).
7. 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 від 20.07.2007, зареєстрованим в Міністерстві юстиції України 30.07.2007 за № 862/14129.
8. Об'єкт експертизи відповідає вимогам пункту 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 в Міністерстві юстиції України 26.05.2021 за № 696/36318.
9. 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 26.1-45217327-001:2026.

Термін дії експертного висновку – до 10.08.2031.

Голова Служби



Олександр ПОТІЙ