



**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 02.07 2026р. № 04/03/02-17732/2026/ВН На № _____ від _____ 20__ р.

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 02.07.2026

м. Київ

Виданий: Товариству з обмеженою відповідальністю «Ілайф» (код ЄДРПОУ 36049014)

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 01.07.2026 № 679.

Об'єкт експертизи: Програмний засіб криптографічного захисту інформації «Криптос Гейт Плас» UA.36049014.00002-01.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю «Ілайф» (код ЄДРПОУ 36049014)

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

Висновки:

1. В об'єкті експертизи правильно реалізовано криптографічні алгоритми, визначені ДСТУ 9311:2024 (у режимах простої заміни, гамування із зворотним зв'язком та обчислення імітовставки), ДСТУ 7564:2014 (у режимі «Купина-256», «Купина-384», «Купина-512»), ДСТУ 4145-2002 (у поліноміальному базисі).
2. 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.
3. В об'єкті експертизи алгоритм ініціалізації генератора випадкових послідовностей реалізовано відповідно до документу «Методика ініціалізації генератора випадкових послідовностей. UA.36049014.00002-01 91 01».
4. В об'єкті експертизи правильно реалізовано формат заявок на формування сертифікатів відкритих ключів, визначений PKCS#10.
5. В об'єкті експертизи правильно реалізовано формати запиту та відповіді про статус сертифікату, визначені IETF RFC 6960.

6. В об'єкті експертизи правильно реалізовано формати позначки часу та запиту на її формування, визначені ДСТУ ETSI EN 319 422:2016.

7. 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.

8. Об'єкт експертизи відповідає вимогам технічного завдання (UA.36049014.00002-01) із Доповненням № 4 до нього, в частині реалізації функцій криптографічних перетворень.

9. 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, затверджене 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 (зі змінами).

10. 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, у яких криптографічні перетворення здійснюються програмними модулями, що мають наступні значення геш-функцій:

ElifeCrypto.dll B9EE1F43 B7A45894 51083BE6 390BF169 3D985DCA 78619FE7 DDA03574 DD5D516B
ElifeCrypto.Plus.dll BA8C826F 50F9A96B 5D18788A CEDD17EF 4BFBF27E 3514B91C 9EE51851 E2177C34

Розрахунок геш-функцій здійснено відповідно до ДСТУ 7564:2014 (у режимі роботи «Купина-256» з використанням нульового вектора ініціалізації).

Термін дії експертного висновку до 01.07.2031.

Голова Служби



Олександр ПОТІЙ