



**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

14.04.2021 № 001/05702 - 995 На № _____ від _____

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 14.04.2021

м. Київ

Виданий: Приватному акціонерному товариству «Інститут інформаційних технологій»
(код ЄДРПОУ 22723472)

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 14.04.2021 № 498.

Об'єкт експертизи: Ключ електронний «Алмаз-1К» ЄААД.469535.153.

Розроблений (виготовлений): Приватним акціонерним товариством «Інститут інформаційних технологій» (код ЄДРПОУ 22723472).

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

Висновки:

1. В об'єкті експертизи правильно реалізовано криптографічні алгоритми, визначені ДСТУ ГОСТ 28147:2009 (у режимах простої заміни, гамування із зворотним зв'язком та вироблення імітовставки), ГОСТ 34.311-95, ДСТУ 4145-2002.
2. В об'єкті експертизи алгоритм генерації випадкових двійкових послідовностей та порядок генерації ключових даних реалізовано згідно документу «Методика генерації ключових даних ЄААД.468244.020 Д1.05».
3. В об'єкті експертизи внутрішній апаратний генератор випадкових послідовностей реалізовано згідно документу «Методика генерації ключових даних ЄААД.468244.020 Д1.05».
4. Протокол взаємної автентифікації об'єкта експертизи з програмним забезпеченням користувачів відповідає документу «Методика (протокол) автентифікації програмних засобів користувачів та електронного ключа ЄААД.469535.153 Д3».
5. В об'єкті експертизи правильно реалізовано протокол автономного узгодження ключів в групі точок еліптичної кривої типу Діффі-Геллмана (KANIDH), визначений п. 8.2 ДСТУ ISO/IEC 15946-3:2006.
6. Об'єкт експертизи відповідає вимогам технічного завдання ЄААД.469535.153.01 ТЗ із Доповненням № 1 до нього, в частині реалізації функцій криптографічних перетворень.
7. Об'єкт експертизи може бути використаний як складова частина при побудові засобів криптографічного захисту інформації видів «А» та «Б», призначених 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 26.2-22723472-020:2014 із Зміною № 1:2019 до них.

Термін дії експертного висновку – до 10.05.2024.

Голова Служби



Юрій ЩИГОЛЬ



Прим № 1

АДМІНІСТРАЦІЯ ДЕРЖСПЕЦЗВ'ЯЗКУ

Департамент захисту інформації
(ДЗІ Адміністрації Держспецзв'язку)

вул. Солом'янська, 13, м. Київ, Україна, 03110,

тел.: (044) 281-96-92 е-

mail: dzi@cip.gov.ua

№ _____

На № _____ від _____

Приватному акціонерному товариству
«Інститут інформаційних технологій»
e-mail: jsciitua@gmail.com

Щодо терміну дії експертних висновків

Адміністрацією Держспецзв'язку опрацьовано лист (вх. № 9115/ВС від 11.04.2024) щодо продовження терміну дії експертних висновків на засіб криптографічного захисту інформації ключ електронний «Алмаз-1К» ЄААД.469535.153 та зазначаємо про таке.

Термін дії експертних висновків на засіб криптографічного захисту інформації ключ електронний «Алмаз-1К» ЄААД.469535.153 закінчується 10.05.2024.

У зв'язку із введенням Указом Президента України від 24.02.2022 № 64/2022 воєнного стану в Україні з 24.02.2022, Експертною комісією з питань проведення державної експертизи у сфері криптографічного захисту інформації Держспецзв'язку (протокол засідання від 27.03.2022 № 536) прийнято рішення протягом періоду дії правового режиму воєнного стану в Україні та трьох місяців після його припинення чи скасування продовжувати на шість місяців терміни дії експертних висновків засобів криптографічного захисту інформації, які закінчуються.

Слід зазначити, що інформація про продовження термінів дії експертних висновків на засоби криптографічного захисту інформації, що закінчується протягом періоду дії правового режиму воєнного стану в Україні розміщується на офіційному веб-сайті Держспецзв'язку за посиланням <https://cip.gov.ua/ua/news/perelik-zasobiv-kriptografichnogo-zakhistu-informaciyiyaki-mayut-ekspertnii-visnovok-za-rezultatami-derzhavnoyi-ekspertizi-ugaluzi-kzi>.

Т.в.о. директора Департаменту

Олександр ГРИЩЕНКО



УВ Юлія ТЕРЕЩЕНКО (044)281-97-77

Адміністрація Держспецзв'язку

№04/05/02-3799/СЕД від 16.04.2024

КЕП: Грищенко О. О. 16.04.2024 19:55

10E3F0

Сертифікат дійсний з 05.03.2024 12:37 до 05.03.2026 12:37