



# ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

вул. Солом'янська, 13, м. Київ, 03110,  
тел. (044) 281-92-10, факс: (044) 281-94-83, e-mail: info@dsszzi.gov.ua

23.07.2018 № 04/03/02 - 2958

## ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 23.07.2018

м. Київ

Виданий: Товариству з обмеженою відповідальністю «Техноконсалтинг»  
(код ЄДРПОУ 25284317)

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 19.07.2018 № 354.

Об'єкт експертизи: Засіб електронного цифрового підпису апаратно-програмний «Tellipse4»  
25284317.467649.004.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю  
«Техноконсалтинг» (код ЄДРПОУ 25284317).

Експертний заклад: Інститут спеціального зв'язку та захисту інформації НТУУ  
«КПІ імені Ігоря Сікорського» (код ЄДРПОУ 34979237).

### Висновки:

1. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування електронного цифрового підпису, визначений ДСТУ 4145-2002 (у поліноміальному базисі).
2. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування RSA, визначений IETF RFC 3447 (за схемою RSAES-PKCS1-v1\_5).
3. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного цифрового підпису ECDSA, визначений ДСТУ ISO/IEC 14888-3:2015.
4. В об'єкті експертизи забезпечується захист записаних даних від несанкціонованого доступу від безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання.
5. Об'єкт експертизи відповідає вимогам технічного завдання на дослідно-конструкторську роботу Розробка надійного засобу електронного цифрового підпису, шифр «Tellipse4», в частині реалізації функцій криптографічних перетворень.
6. 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 26.2-25284317-004:2018.

Термін дії експертного висновку – до 19.07.2023.

Голова Служби



Л.О. Євдоченко