Прим. № __

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

15.05.2020 № 04/03/02-1191 На № _____ від _____

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 15.05.2020 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 15.05.2019 № 453.

Об'єкт експертизи: Шлюз захисту «Бар'єр-301» ЄААД.469535.095.

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, ДСТУ 4145-2002, ГОСТ 34.311-95.
2. В об'єкті експертизи генерація ключових даних відповідає документу «Методика генерації ключових даних» ЄААД.468244.020 Д1.05.
3. В об'єкті експертизи криптографічний протокол Діффі-Геллмана (DH), що реалізований та використовується в об'єкті експертизи, відповідає вимогам наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 18.12.2012 № 739 «Про затвердження Вимог до форматів криптографічних повідомлень», зареєстрованого у Міністерстві юстиції України 14.01.2013 за № 108/22640, та ДСТУ ISO/IEC 15946-3:2006.
4. В об'єкті експертизи формати захищених і підписаних даних реалізовано згідно вимог IETF RFC 5652 «Cryptographic Message Syntax (CMS)», PKCS#7 Cryptographic Message Syntax Standard, IETF RFC 5126 «CMS Advanced Electronic Signatures (CAdES)», ДСТУ ETSI EN 319 122-1:2016, ДСТУ ETSI EN 319 122-2:2016.
5. В об'єкті експертизи формати запитів на отримання інформації про статус сертифіката та формати відповідей про статус сертифіката реалізовано згідно вимог RFC 2560 «Internet X.509 Public Key Infrastructure Online Certificate Status Protocol (OCSP)».
6. В об'єкті експертизи формати запитів на формування позначок часу реалізовано згідно вимог IETF RFC 3161 «Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)», ДСТУ ETSI EN 319 422:2016.

7. В об'єкті експертизи формати контейнерів особистих ключів реалізовано згідно вимог PKCS#8 Private-Key Information Syntax Standard, PKCS#12 Personal Information Exchange Syntax Standard, IETF RFC 5958 «Asymmetric Key Packages».
8. В об'єкті експертизи інтерфейси бібліотек підтримки криптомодулів взаємодії реалізовано згідно вимог PKCS#11 Cryptographic Token Interface Base Specification.
9. В об'єкті експертизи формати сертифікатів та списків відкликаних сертифікатів реалізовано згідно вимог ДСТУ ISO/IEC 9594-8:2006, IETF RFC 5280 «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile».
10. Об'єкт експертизи відповідає вимогам часткового технічного завдання ЄААД.469535.095 із Доповненням № 1 до нього 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 26.2-22723472-010:2020.

Термін дії експертного висновку – до 15.05.2025.

Голова Служби Валентин ПЕТРОВ