Прим. № 1


# 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


28.12.2016 № 04/03/02-5282

## ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 28.12.2016 м. Київ

Виданий: Товариству з обмеженою відповідальністю "ІНТЕГРОВАНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ" (код ЄДРПОУ 38773869)

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 27.12.2016 № 270.

Об'єкт експертизи: Програмно-технічний комплекс центру сертифікації ключів електронного цифрового підпису за алгоритмами ДСТУ 4145-2002, RSA, ECDSA UA.IIT.38773869.00001-01.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю "ІНТЕГРОВАНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ" (код ЄДРПОУ 38773869).

Експертний заклад: Приватне акціонерне товариство "АЛЬТРОН" (код ЄДРПОУ 31633037).

Висновки:

1. В об'єкті експертизи правильно реалізовано криптографічні алгоритми ДСТУ ГОСТ 28147:2009, ГОСТ 34.311-95, ДСТУ 4145-2002 (у поліноміальному базисі).
2. В об'єкті експертизи алгоритм генерації випадкових послідовностей відповідає вимогам додатку А ДСТУ 4145-2002.
3. 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.
4. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування AES, визначений ДСТУ ISO/IEC 18033-3:2015 (в режимах ECB та CBC, визначені ДСТУ ISO/IEC 10116:2014).
5. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного цифрового підпису RSA, визначений PKCS#1 v2.2: RSA Cryptography Standard (за схемами RSASSA-PKCS1-v1_5 та RSASSA-PSS).
6. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного цифрового підпису ECDSA, визначений ANSI X9.62:2005.
7. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-1, SHA-256, SHA-384, SHA-512, визначені ДСТУ ISO/IEC 10118-3:2005.
8. В об'єкті експертизи правильно реалізовано криптографічний алгоритм гешування SHA-224, визначений IETF RFC 3874.
9. Алгоритм генерації ключових даних, що реалізовано в об'єкті експертизи, відповідає вимогам документу "Програмно-технічний комплекс центру сертифікації ключів електронного цифрового підпису за алгоритмами ДСТУ 4145-2002, RSA, ECDSA. Методика генерації ключових даних" (до вх. 6337 від 26.12.2016).

10. Об'єкт експертизи відповідає вимогам технічного завдання UA.ІІТ.38773869.00001-01 ТЗ 01 та Доповнення № 1 до нього, в частині реалізації функцій криптографічних перетворень.
11. Формат посиленого сертифіката відкритого ключа, структура об'єктних ідентифікаторів для криптоалгоритмів, що є державними стандартами, формат списку відкликаних сертифікатів, формат підписаних даних, протокол фіксування часу, протокол визначення статусу сертифіката, які реалізовані та використовуються в об'єкті експертизи, відповідають вимогам наказу Міністерства юстиції України та Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.08.2012 № 1236/5/453 "Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису", зареєстрованого у Міністерстві юстиції України 20.08.2012 за № 1398/21710.
12. Формати криптографічних повідомлень та протоколи узгодження ключів, які реалізовані та використовуються в об'єкті експертизи, відповідають 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.
13. Алгоритми формування ключів шифрування ключів та захисту особистих ключів електронного цифрового підпису та особистих ключів шифрування, формати транспортних контейнерів особистих ключів електронного цифрового підпису та особистих ключів шифрування, формати контейнерів зберігання особистих ключів електронного цифрового підпису, особистих ключів шифрування та сертифікатів відкритих ключів, прикладний програмний інтерфейс, які реалізовані, створюються та використовуються в об'єкті експертизи, відповідають вимогам спільного наказу Міністерства юстиції України та Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 27.12.2013 № 2782/5/689 "Про затвердження вимог до алгоритмів, форматів та інтерфейсів, що реалізуються у засобах шифрування та надійних засобах електронного цифрового підпису", зареєстрованого в Міністерстві юстиції України 27.12.2013 за № 2228/24759.
14. В об'єкті експертизи правильно реалізовано вимоги до форматів даних та протоколів (CAC, OID, CRL, TSP, OCSP, CMS) інфраструктури відкритих ключів для алгоритмів RSA та ECDSA відповідно до вимог ДСТУ ISO/IEC 9594-8:2014.
15. В об'єкті експертизи правильно реалізовано вимоги до форматів даних та протоколів (CAC, OID, CRL, TSP, OCSP, CMS) відповідно до вимог RFC 3297, RFC 4055, RFC 5758, RFC 5280, RFC 6960, RFC 3161, ETSI TS 101 861, RFC 5652, RFC 2898, RFC 5208, ETSI EN 319 412-1, ETSI EN 319 412-2, ETSI EN 319 412-3, ETSI EN 319 412-5, ETSI TS 119 312 в частині їх використання в національній інфраструктурі відкритих ключів.
16. В об'єкті експертизи правильно реалізовано вимоги PKCS #10 у частині їх використання в національній інфраструктурі відкритих ключів.
17. 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, які виготовлені відповідно до технічних умов ТУ У 72.2-38773869-001:2016.

Термін дії експертного висновку – до 27.12.2021.

Перший заступник Голови Служби О.М. Чаузов