Прим. № __

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

вул. Солом'янська, 13, м. Київ, 03680,
тел. (044) 281-92-10, факс: (044) 281-94-83, e-mail: info@dsszzi.gov.ua

22.02.2013р № 05/02/02 – 616

ЕКСПЕРТНИЙ ВИСНОВОК

Виданий: Товариству з обмеженою відповідальністю "Інтер-Метл" (код ЄДРПОУ 25279440)

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 22.02.2013 № 106.

Об'єкт експертизи: Виріб програмний "Криптографічний сервіс-провайдер "ЦЕЗАРІС-CSP" (ТУ У 72.2-25279440-002:2011).

Розроблений (виготовлений): Товариством з обмеженою відповідальністю "Інтер-Метл" (код ЄДРПОУ 25279440).

Експертний заклад: Державний науково-дослідний інститут спеціального зв'язку та захисту інформації Державної служби спеціального зв'язку та захисту інформації України (код ЄДРПОУ 34732331).

Висновки:

1. В об'єкті експертизи правильно реалізовані та використовуються криптографічні алгоритми, які визначені ДСТУ ГОСТ 28147:2009, ДСТУ 4145-2002, ГОСТ 34.311-95.
2. В об'єкті експертизи реалізовані криптографічні алгоритми SHA-1, SHA-256, SHA-384, SHA-512 відповідають вимогам ДСТУ ISO/IEC 10118-1:2005, ДСТУ ISO/IEC 10118-3 та ДСТУ ETSI TS 102 176-1 в частині використання геш-функцій.
3. В об'єкті експертизи реалізований криптографічний алгоритм симетричного шифрування DES відповідає вимогам ISO/IEC 18033-3 у режимах ECB та CBC, що визначені ISO/IEC 10116.
4. В об'єкті експертизи реалізований криптографічний алгоритм симетричного шифрування TDEA/3DES відповідає вимогам ISO/IEC 18033-3 у режимі CBC, що визначений ISO/IEC 10116.
5. В об'єкті експертизи реалізований криптографічний алгоритм симетричного шифрування AES відповідає вимогам ISO/IEC 18033-3 у режимі ECB, що визначений ISO/IEC 10116, для довжини ключа 128 біт.
6. В об'єкті експертизи реалізований криптографічний алгоритм RSA, з довжиною ключа, кратною 512 біт, відповідає вимогам RFC 2313:1998 PKCS#1 v1.5 та ДСТУ ETSI TS 102 176-1.
7. В об'єкті експертизи реалізовані криптографічні алгоритми RSASSA-PSS з довжиною ключа, кратною 512 біт, і RSAES-OAEP, які відповідають вимогам PKCS#1 v2.1.
8. В об'єкті експертизи реалізований криптографічний протокол автономного узгодження ключів типу Діффі-Геллмана, який відповідає вимогам ДСТУ ISO/IEC 15946-3.
9. Генерація ключових даних в об'єкті експертизи відповідає вимогам документа "Методика генерації та розподілу ключових даних "Цезаріс-М" (UA.32206929.3КЦ.П1.002).
10. 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 Держспецзв'язку від 20.08.2012 № 1236/5/453 "Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису", зареєстрованого в Міністерстві юстиції України від 20.08.2012 за № 1398/21710.

11. В об'єкті експертизи формування та обробка запитів на отримання сертифікатів здійснюється відповідно до вимог PKCS #10.

12. В об'єкті експертизи алгоритм обчислення симетричних ключів з використанням паролю відповідає вимогам Додатку В PKCS #12.

13. В об'єкті експертизи алгоритми зберігання та резервування ключових даних в файловому токені відповідають вимогам PKCS #11.

14. Об'єкт експертизи відповідає вимогам технічного завдання (32206929.1КЦ.003.ТЗ.01.1) та технічних умов (ТУ У 72.2-25279440-002:2011) в частині реалізації функцій криптографічних перетворень.

15. 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 72.2-25279440-002:2011) і мають значення геш-функції установочного файлу

CesarisCryptoPack316c.exe	C503C3A6	448CF380	D231DD62	D461031A	2A1CD6EF	29A60D79	BB890A4F	355614AC

Термін дії експертного висновку: до 22.02.2018.

Перший заступник Голови Служби О.Г. Цуркан