Прим. № 1

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

17.11.2020 № 04/05/02-3028 На № _____ від _____

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 17.11.2020 м. Київ

Виданий: Товариству з обмеженою відповідальністю «АЙ-ДЖИ-ЕМ» (код ЄДРПОУ 38777968)

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 12.11.2020 № 476.

Об'єкт експертизи: Програмний комплекс «Варта» 804.36002112.466452.002.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю «АЙ-ДЖИ-ЕМ» (код ЄДРПОУ 38777968).

Експертний заклад: Товариство з обмеженою відповідальністю «ЗАХИСТ.ЮЕЙ» (код ЄДРПОУ 42292899).

Висновки:

1. В об'єкті експертизи правильно реалізовано криптографічні алгоритми, визначені ДСТУ ГОСТ 28147:2009, ДСТУ 7624:2014, ДСТУ 7564:2014, ГОСТ 34.311-95, ДСТУ 4145-2002.
2. В об'єкті експертизи алгоритм генерації випадкових двійкових послідовностей відповідає додатку А ДСТУ 4145-2002.
3. В об'єкті експертизи правильно реалізовано алгоритми шифрування, формування та перевіряння електронного цифрового підпису RSA, визначені IETF RFC 3447.
4. В об'єкті експертизи правильно реалізовано криптографічні алгоритми шифрування DES, TDES, AES відповідно ДСТУ ISO/IEC 18033-3:2015 (в режимах CBC, CFB, OFB, CTR, визначених ДСТУ ISO/IEC 10116:2014).
5. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного цифрового підпису ECDSA, визначений ДСТУ ISO/IEC 14888-3:2015.
6. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-1, SHA-256, SHA-384, SHA-512, визначені ДСТУ ISO/IEC 10118-3:2005.
7. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування MD2, визначений IETF RFC 1319 «The MD2 Message-Digest Algorithm», MD4, визначений IETF RFC 1320 «The MD4 Message-Digest Algorithm», MD5, визначений IETF RFC 1321 «The MD5 Message-Digest Algorithm».
8. В об'єкті експертизи правильно реалізовано криптографічний протокол автономного узгодження ключів типу Діффі-Гелмана (KANIDH) та криптографічний протокол

узгодження ключів типу Діффі-Гелмана з двома цифровими підписами та підтвердження ключів (KADH2SKC), визначені п. 8.2 та п. 8.6 ДСТУ ISO/IEC 15946-3:2006 відповідно.

9. В об'єкті експертизи алгоритм формування початкових значень для генератора випадкових двійкових послідовностей відповідає документу «Програмний комплекс «Варта» Методика ініціалізації генератора випадкових послідовностей 804.36002112.466452-01.90.01».

10. В об'єкті експертизи алгоритм формування електронного цифрового підпису без розкриття змісту повідомлення відповідає документу «Програмний комплекс «Варта» Методика формування електронного цифрового підпису без розкриття змісту повідомлення 804.36002112.466452-02.93.01» (крім платформи реалізації JavaScript).

12. В об'єкті експертизи формат криптографічних повідомлень та криптографічні протоколи Діффі-Геллмана (DH, ECDH), що 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 та ДСТУ ISO/IEC 15946-3:2006.

14. Об'єкт експертизи забезпечує захист записаних на нього даних від несанкціонованого доступу, від безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання.

15. Об'єкт експертизи відповідає вимогам технічного завдання 804.36002112.466452.002.ТЗ із Доповненнями № 1, № 2 до нього в частині реалізації функцій криптографічних перетворень.

16. 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, у яких криптографічні перетворення здійснюються програмними модулями, що мають наступні значення геш-функцій:

Каталог .Net
CSPLibNET6.dll 16F9BAEB A3883F82 ACD59EE2 B5A63184 4001D570 4167D456 C88A12CE 14291BAE

Каталог JavaScript
qlweb.js 46BF8D67 08B984AD BEC49BF9 2CB2053A 47ABB27B C8E6C953 535B683E 9CE03550

Каталог Win32
CryptoLib6.dll 229A147A 94034143 284FFC57 ED89C4E5 D5A0D623 A398D7A4 CC3071D8 E564B269
CryptoLib7.dll F73EB334 1CF13F77 6F5F79F5 CB97FD4F 5EB43F58 A31C2305 35AF64BE EC2934F9
CSPLib6.dll 7BB38ECC EC3DD228 7B1D093C 106260D0 27437F30 0DDFFBB3 604B3610 B8869FE1

Каталог Win64
CryptoLib6.dll B89F491D D10958BA 1E589AD2 187C8E91 8898A9AF 9AEA2B98 76C32353 F3CDE822
CryptoLib7.dll C7A2D5F7 BDAE5B16 38703BF8 97A97953 EC45AC91 743011CA FBA2933A 75F5FC99
CSPLib6.dll AC1F6449 23A10D92 244A4234 808C5516 A717D05B 462D8EEC D7355715 054B0C7D

Розрахунок геш-функцій здійснено відповідно до ГОСТ 34.311-95 з урахуванням значення нульового стартового вектора та ДКЕ № 1 з додатка № 1 до Інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації, затвердженої наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 12.06.2007 № 114, зареєстрованої в Міністерстві юстиції України 25.06.2007 за № 729/13996.

Термін дії експертного висновку – до 12.11.2025.

Голова Служби Юрій ЩИГОЛЬ