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

16.05.2017 № 04/03/02-1674

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 16.05.2017 м. Київ

Виданий: Товариству з обмеженою відповідальністю "САЙФЕР БІС" (код ЄДРПОУ 33349855)

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 16.05.2017 № 291.

Об'єкт експертизи: Програмний комплекс криптографічних перетворень "Шифр+", версія 2.1 (ТЗ У 72.223154898003:2016).

Розроблений (виготовлений): Товариством з обмеженою відповідальністю "САЙФЕР БІС" (код ЄДРПОУ 33349855).

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 криптографічні алгоритми, визначені ДСТУ 7564:2014, ДСТУ 7624:2014 (у режимах ECB, OFB, CFB, CBC, CTR, XTS, KW, CMAC, GMAC, GCM, CCM).
2. В об'єкті експертизи правильно реалізовано криптографічні алгоритми, визначені ДСТУ ГОСТ 28147:2009, ГОСТ 34.311-95, ДСТУ 4145-2002 (в поліноміальному базисі).
3. В об'єкті експертизи алгоритм генерації випадкових двійкових послідовностей відповідає додатку А ДСТУ 4145-2002 та розділу 7 ГОСТ 34.310-95.
4. В об'єкті експертизи правильно реалізовано криптографічні алгоритми шифрування DES, TDEA, AES відповідно до ДСТУ ISO/IEC 18033-3:2015 (в режимах ECB, OFB, CFB, CBC, CTR, CMAC, визначені ДСТУ ISO/IEC 10116:2014).
5. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування RSA, визначений IEEE P1363-2000 та PKCS#1 v2.2 RSA Cryptography Standard (за схемою RSA-OAEP).
6. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного цифрового підпису ECDSA (в поліноміальному базисі), визначений ДСТУ ISO/IEC 14888-3:2015, BSI-TR-03111:2012, ISO/IEC 15946-2:2002.
7. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного цифрового підпису ECGDSA (в поліноміальному базисі), визначений ДСТУ ISO/IEC 14888-3:2015, IEEE P1363-2000, ISO/IEC 15946-2:2002, NIST FIPS 186-4:2013.
8. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного цифрового підпису RSA (RSA1S, RSA2S, RSA-PSS) відповідно до IEEE P1363-2000, ДСТУ ISO/IEC 14888-2:2015, NIST FIPS 186-4:2013.

9. В об'єкті експертизи правильно реалізовано криптографічний алгоритм гешування SHA-1, визначений ДСТУ ISO/IEC 10118-3:2005.
10. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256, визначені FIPS PUB 180-4:2012.
11. В об'єкті експертизи правильно реалізовано алгоритми вироблення ключа шифрування на основі спільного секрету KDF1, KDF2, KDF3 відповідно до ДСТУ ISO/IEC 18033-2:2015 та відповідно до вимог 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.
12. В об'єкті експертизи правильно реалізовано алгоритми вироблення ключа шифрування на основі паролю PBKDF1, PBKDF2 відповідно до PKCS#5 v2.1 та IETF RFC 2898 та відповідно до вимог 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.
13. В об'єкті експертизи правильно реалізовано алгоритм вироблення ключа шифрування на основі паролю PBKDFUAPfx відповідно до вимог 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 алгоритм шифрування на основі паролю PBES2 відповідно до PKCS#5 v2.1, IETF RFC 2898 та відповідно до вимог 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.
15. В об'єкті експертизи правильно реалізовано алгоритм обчислення коду автентифікації на основі паролю PBMAC1 відповідно до PKCS#5 v2.1, IETF RFC 2898 та відповідно до вимог 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.
16. В об'єкті експертизи правильно реалізовано криптографічні протоколи розподілу ключів: ECKAS-DH1 (KANIDH, ECDH) відповідно до IEEE P1363-2000 і ДСТУ ISO/IEC 15946-3:2006; ECKAS-DH2 (KADH2KP, KADH2SKC) відповідно до IEEE P1363-2000 і ДСТУ ISO/IEC 15946-3:2006; ECKAS-MQV1 (KAMQV1P, KAMQV2P) відповідно до IEEE P1363-2000 і ДСТУ ISO/IEC 15946-3:2006; ECKAS-MQV2 відповідно до ДСТУ ISO/IEC 15946-3:2006; ECKAS-EG (KAEG) відповідно до ДСТУ ISO/IEC 15946-3:2006.
17. В об'єкті експертизи правильно реалізовано алгоритми обчислення коду автентифікації повідомлення з використанням: блокових симетричних шифрів ДСТУ ГОСТ 28147:2009, ДСТУ 7624:2014, AES, DES, TDEA і геш-функцій, визначених ГОСТ 34.311-95, ДСТУ 7564:2014, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256 відповідно до IETF RFC 2104.

18. В об'єкті експертизи правильно реалізовано алгоритми кодування даних: EMSA1 відповідно до IEEE P1363-2000; EMSA2 відповідно до IEEE P1363-2000 та X9.31; EMSA3 відповідно до IEEE P1363-2000 та PKCS#1 v2.2; EMSA4 відповідно до IEEE P1363-2000 та PKCS#1 v2.2; EMSR1 відповідно до IEEE P1363-2000 та ISO/IEC 9796:1991; EMSR3 відповідно до IEEE P1363a-2004.
19. В об'єкті експертизи правильно реалізовано алгоритми доповнення відповідно до вимог PKCS#7, PKCS#5, NIST FIPS 800-38a, ДСТУ 7624:2014, ANSI X.923.
20. В об'єкті експертизи алгоритм ініціалізації генератора випадкових послідовностей відповідає вимогам документу "Методика ініціалізації генератора випадкових двійкових послідовностей" UA.33349855.00001 – 01 94 01.
21. В об'єкті експертизи правильно реалізовано алгоритм шифрування ключів KeyWrap відповідно до вимог 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.
22. Об'єкт експертизи відповідає вимогам технічного завдання ТЗ У 72.223154898003:2016 в частині реалізації функцій криптографічних перетворень.
23. 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 android

Каталог ccpplib-andrd-arm
libCCPPLib_android.a 88FC59D9 2684AAAF 183DE5DA F1778D29 B2CB88C0 6783EE07 09B543F8 D228DD8B
libCCPPLib_android.so F23F32CB 8863F86B B2B98D53 F6355476 BB240847 94CF551B E28C1F32 61632B31

Каталог ccpplib-andrd-arm64
libCCPPLib_android.a 759E1ABC 41D13F75 159A676A EB08E41D 22705DD1 E4F1684C 01AAE384 18364C56
libCCPPLib_android.so B49374CB 76EF7636 93E8E787 A85B2CF4 850A79C9 AAC808BB E9B9041F 33FEAFA4

Каталог ccpplib-andrd-x86
libCCPPLib_android.a B3EE8824 5131E19D CE0798A9 900A1DCA A985761C 0CB35053 8E708A39 375AC6A9
libCCPPLib_android.so 541A32CF B283C6B0 7AB4C3E9 B16B9DA2 2E146B01 9A2B9D76 C1864366 B8F68B79

Каталог ccpplib-andrd-x86-64
libCCPPLib_android.a B2240EFD DBFD3476 B3F9D48F 7D7D8213 F09AE2D2 91DC7B6D C0C9787C 98EC6302
libCCPPLib_android.so 7287805A B6052437 1D9E1519 51C9B76C 2D9988A5 812921DF 77DB094A B8F6CC70

Каталог freebsd

Каталог ccpplib-freebsd-x86
libccpplib-freebsd.a 8CEB9728 9ED446BE 3BF0A64A 3D0DFB99 8B07EE1C ED1A9646 6188695F D8DD81BE

Каталог ccpplib-freebsd-x86-64
libccpplib-freebsd.a 99E7DC8C 065ACEC4 AB42EDD6 86FCCA83 B768CDEA CFC195DE 1D2065D3 4AEA3C23
libccpplib-freebsd.so C00DA9A0 AF435A20 DC11B8F0 629E99C4 2F96BB3B FC4F6844 3153BAB2 E2FA253A

Каталог ios

Каталог ccpplib-ios-comb
CCPPLib-ios-combined.a E75B9A0B 00288CB6 9EB7AD35 B750B42E 44BAB8A6 E14D716B A6F5E731 6DE7C4DB

Каталог ccpplib-ios-iphone
libCCPPLib-iOS.a 8A7BB334 9870B96A 8E3666D1 A70089D0 347DD115 E505928E 73123JD8 5F79C5F2

Каталог ccpplib-ios-simul
libCCPPLib-iOS.a 69765175 F4E428B5 474F551A 6FEF7E27 4B55E7A7 7276A037 01B043F1 4CE41D3E

Каталог linux

Каталог ccpplib-linux-x64
libccpplib-linux.a CE126E48 E55F4377 8EBCBA3A 9190EEDC 7E717F5A DC644154 A1EA4D29 A4247329
libccpplib-linux.so D61E612F F47456CF 57E5EE5C 7D5CDFA3 2BC9F1E7 3BCCBD43 7E4D7479 EF76021E

Katanor ccpplib-linux-x86

libccpplib-linux.a	66197A1B 77D61AE4 9BA5439A 015F4700 C3EB89E8 397FCF4C A9FCA262 1E5297C9
libccpplib-linux.so	239B7734 69D922C2 1FF7985F AACCF71E CB059C19 68D43D2B 3867F7C5 40552150

Katanor macos

Katanor ccpplib-macos-x86-64

libCCPPLib.a	819131C4 11F7D461 0A582C58 2B6782EC 4B910986 EE7EAFF3 DFE09FDE B46CE980
libCCPPLib-dynamic.dylib	2034AB48 E2200D37 190B5517 EB3C28D0 B763F89F 0B4AF759 FDDBAF19 5EB03854

Katanor windows

Katanor ccpplib-win-x86

CCPPLib.lib	D03A07F5 9F6A1DE4 E12C243E 75B06FD7 FCE56308 141560C9 A463D6CB B1AEF7CF
CCPPLib.dll	81BECEED 4AAFF6A6 8FD4EEB8 950AC1C6 0B7D02B9 EC542708 EBEF2150 F537261C

Katanor ccpplib-win-x86-64

CCPPLib.lib	53161CB6 712A3976 024794E8 D2A0CBA2 2CCB0BC6 EC189F5F 4BE7EBB2 DEF16871
CCPPLib.dll	[illegible]

Katanor headers

AESDataTest.h	91B3241A A53D332C 38EA2F71 6484B0E2 8FC624A2 099FCAC3 6A41DF51 9597146C
Alg1d.h	1373049F B00A80DF 4234FC7A 6DF53006 0C614585 FCACB252 F58701E4 0FD181C9
Api1Dec1.h	3D84B83C C4960F8A BF8CD40B B547F4F8 6CFF5237 8842950A 4BB91732 E005B1D7
CCPPLib.h	A4F3A1F0 2938BEA4 1FEBAE16 2060C154 D026B497 9E8FF8B3 F334CDC9 7C7C5B50
CryptoErrors.h	82D8811A B39F4BCF C4B5AF95 4DC322E8 D6A7DF6E 36391D50 A64AB211 99E4C27A
DESDataTest.h	43EB352F 6D2F464E BF76A189 4E30C83B EB17427F 071DE8EB 3F567A39 51E17368
DSTU41452002DataTest.h	20775200 87CD6CFA 2218A5E0 713F7DA0 420A3C47 5508E5CE 5635653C 1D7FB796
DSTU75642014DataTest.h	CA0C6D40 58A3F3D2 9A6EC899 AA4C38B7 47B91AAC A94A5705 18CF30DE 83334D87
DSTU76242014DataTest.h	D0787A8E 44311D6E 3083CFDA 485BC049 E6A06932 0CFD2AF1 43CA0FBB BD28F9EB
ECDSADataTest.h	FABC8785 81577589 7148DC49 37022644 613C2FA5 C801772D 1FD1CC86 70783286
ECGDSADataTest.h	77181C36 41696CAA 07778E71 951B9335 5344F8E7 9EE02616 B82CF6F8 F272EBF8
ECKASDH1DataTest.h	C2168F5E 8C903831 9EA1EA76 6F9946AE B95571F8 DF706AB2 9208EB71 C530921E
EME1DataTest.h	1087EED5 7CF1A33F D467CE9B 87D06BF9 FBC098A4 F96E8BB4 70960EA3 5C157582
EME2DataTest.h	97FD5DE0 53BEAD24 B9CFD720 4901162E 04B05989 805D9DC5 247609CF 785ED6A7
EMSA1DataTest.h	6497C143 E6E8A86B 9414A4BB F2689298 DE2D0145 C5843632 CA9D88D9 9900D9F1
EMSA2DataTest.h	FC5283AB 01EF074D 8C44CC3A 48219323 EAA0ADFE C4E61C5F AB7FB707 72BFFD64
EMSA3DataTest.h	EB3DA91D E265C4D3 2E608F46 758008D0 CB808B86 57CD4675 39F584A7 2E01FA28
[illegible]	[illegible]
EMSR3DataTest.h	95C0F9F5 7E091A0D 1C5AADC5 1A0E084C C4D9FD69 8E44D4CF 2D5F7D1A 533B9B17
F2mECRandomTests.h	77545152 AA49780F 351F0359 A673EF38 B86BE308 5CC433E1 2B3E4DFD 34D87C41
F2mFieldRandomTests.h	F21DB16A 8679002F EC77382D D0E0E6D4 22836334 7DB8EA72 7C4144C2 B9F0E100
FIPS1863Params.h	5FB414B2 47D39C67 03274765 A7FCAC1A 5E07ACD6 FF196801 76829C39 0A535A85
FpECRandomTests.h	71E22CF4 B26873C1 62CC96CF 2CA19B68 07E19768 09B4AF07 81BF1DA7 4046994C
FpFieldRandomTests.h	9F8693C4 3AC33DAA 25B5EFC8 AF0A98F1 4C28B1A8 97D2CDA6 E5346075 E44A0794
GOST28147Data[illegible]	[illegible]
GOST28147WrapDataTest.h	F8D2DD23 A60C5C95 DAB79E66 982D5FBE 2AFF631A B276A368 763DA940 A342F75A
IBigNum.h	DB8FC9A4 E575C764 1FDBAC82 5214E6FD FF68D617 11C56C78 BC613DF7 6C04C921
ICommonSystemParams.h	9908EA13 A145A250 FDA34920 826AC246 67FD4B1C 5E6D5423 B6902472 0011DA71C
IECPoint.h	05C6C59E A1B9751E EB4F9204 9566754E 675BCC8E 35E4988A 9477EC45 0881587A
IExRandomTests.h	83A08CAF D53040F9 832FCBF3 FC5C7B9B 52629EF5 6B3A6F68 8CF98C21 6024ED96
IHash.h	ED107BDB EBF3C1AC 25CD0CBA F4F4CBD5 F295B4B4 EF528640 A905C79C 345FBF65
IKDF.h	15513DD7 CBA9A765 5D78F81A B3D55F7E E17996A5 0F512107 F1DF122F 1F900ACF
IKeyedDigest.h	D950DC08 05ADE949 EECF74E5 4D35C98F 08623AED 502A6B33 DFA8CE5C B95B4BB9
IMEM.h	947F5CF5 A47518D5 E5EC6E5D 1BC3683E 6CC2CF91 9C2BD38C 35DA79C5 45B2CC39
IMsgDigest.h	5127018D DE166512 E5F4F1D6 CA819F69 9136B9C5 0D47A818 8F5C961E 38D8E845
InnerMacros.h	0689D14C 0BE49772 0D8EAF03 4522B0B3 3A099046 3A977EB4 20D68DA6 93912FBC
IPBES.h	008F0DE7 5BC52C35 741EA0F9 3109F111 A34B444A DA85DF3D 6B929231 5DE48B72
IPBKeyedDigest.h	1BE8DADD A43DA065 61E890EE 0D16C8AE F148527C FCCC8A8C 52C90A28 B56A5B96
IPrivateKey.h	B62A9D69 D3952492 791438B6 9A5BB9AC FA19220A 7D98F4CB A3C19E79 CBFDE99D
IPublicKey.h	8E56A867 A3C07893 0CF76DCA FB2CB536 5EDA6AD6 19C9EEEC 47E7CE7B 1559FE02
ISMG.h	5E75C25C 73C84072 C83E82E4 1DA439FE ED44AD3F AC565EDB B87EC92A 2DB08FAB
ISignature.h	5B9A051E 1253E0AB 789B9E79 540A30B9 E8E6BE12 8C40996A 0A7F6DB3 A9B0C5C0
ISymCipher.h	8BF87572 573FBF43 C23A0CCC BC3E2238 2C004DAB D1036F87 B682D441 2C8B0634
IVerifyData.h	183AC643 753EC67D ACDCA265 F220D3EA AA233AB9 3F6EB40D 83B58EED 7FAC98D6
[illegible]	[illegible]
KDF2DataTest.h	21C8CF5E 90C1CAB4 8EEC720D D0DD15D3 F83DB9E0 34539ED1 7DE54D8A 8E8BE663
KDF3DataTest.h	2564E13A 7E3490FF 231311F6 76A10756 4F64ECCE 252F3BC8 2A592097 17F9671E
LargeNumRandomTests.h	21E63A8B DFA476B0 EBECFC06 9A57E12F 0F0A6D03 08FCBA9A CDEEF246 D7A7A620
LargeNumRingRandomTests.h	6B8B0BB8 D762718D 268E8009 4F17E7F5 7B2786CB A7496BFF FE934889 E5980532
PBES2DataTest.h	8685A343 F108CF55 65C433A1 FD59F8E4 0A01BC08 49FF2134 21CDE9F0 49006DE4
PBKDF1DataTest.h	35ED7F3F DAD3E5BF E2C2A42D 9F7DBA46 AEB03864 77E9E21E 760C4188 5EEA5923
[illegible]	[illegible]
PBKDFUAPfxDataTest.h	EF081B5C F9FA97EA C0340E9D DEC9285D 2E0355F4 275022FE 9CDADF27 FA6A95C3
PBMAC1DataTest.h	4371BF46 C2198B85 4222BD17 434D6962 DC55F7D7 82F32A10 D270AB34 75958E1E
RFC5649Params.h	C6F496FA DD972FB8 810A5CB0 C93BE155 41DA549C B45C1EED ABE69224 05CA2263
RSA1SDataTest.h	58B6F810 2A85B0A0 6F402457 C7B7A8ED 18F7ED3F 56C9ED9E 7E7ECE88 2178F1F1
RSA2SDataTest.h	BD0A39CC 52EFD06C DA185C33 59C7EE22 69FD7D06 82B0B1D9 1E544EE4 1D81F275
RSAEDataTest.h	EF50E706 59F7EAFA 52C24B29 2BD88C94 86858775 61B4E1A6 B9782076 AEC88ADC
RSAEPKCS1v15DataTest.h	48BB01F4 D5583E74 F7DC8195 26BA4E16 9711A949 598D0987 1B1BFDD2 A6E21935
RSAPSSDataTest.h	09EAC8EE 9D424B48 0E186D88 CED00583 EFFE488C 82C09915 A5ABD405 02009DDB
SHA1DataTest.h	B5BF6E60 4B1A7E50 9FD363AC B696C110 C88BCC17 94FF1775 41E98E4C 5FAB1CBB
SHA2DataTest.h	5BC7B96F E722ACC8 ECF10C5C BA86BC8D A1E5E6AD 9CFBFD60 FAE26665 3ED8FBBF
SystemParams.h	7663A8A6 C7987853 A711089F 62F2F7B0 062F7D76 06AAFC5A 1CC5DB3F C5082C8E
TestUtils.h	873BAD20 1B857D8A 43608576 6FC8EC97 7D396F52 A75C6039 5653F9C4 3268EA6D
UAGovParams.h	A2DB9820 A682DEE8 A494BF8A 7B553CD8 770E8A0E 0F622ECA D40EFC07 58030921

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 16.05.2022.

Перший заступник Голови Служби О.М. Чаузов

Прим. № 1

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

19.06.2015 № 05/02/01-2597

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 19.06.2015 м. Київ

Виданий: Товариству з обмеженою відповідальністю "САЙФЕР ЛТД" (код ЄДРПОУ 23154898)

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 19.06.2015 № 196.

Об'єкт експертизи: Програмний виріб "Шифр" (Бібліотеки функцій криптографічних перетворень. Версія 1.0) UA.23154898.00001-01.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю "САЙФЕР ЛТД" (код ЄДРПОУ 23154898).

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 реалізовано криптографічні алгоритми, які визначені ДСТУ ГОСТ 28147:2009, ГОСТ 34.310-95, ГОСТ 34.311-95.
2. Об'єкт експертизи відповідає вимогам технічного завдання UA. 23154898.00001-01 90 01 та Доповнення № 1 до нього, в частині реалізації функцій криптографічних перетворень.
3. Об'єкт експертизи може бути використаний для побудови засобів криптографічного захисту інформації з обмеженим доступом (крім службової інформації та інформації, що становить державну таємницю) та відкритої інформації, вимога щодо захисту якої встановлена законом, видів А та Б.

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:

c32csp.dll*	EBF94554 64F926A2 62FD3CC3 0519E8C3 DF202D49 DD600B5B 4AA08D7F B561A4B6
c32csp.h*	47DD1029 4FB5D573 C361949F 80099EEC 0B9C3FCA 792E730B C3DCFFED 1EABBE59
c32csp.lib*	E4D33201 5078E49F 81806951 E1DC45CA 13576178 A2BABE86 F1481967 49EA69A0
c32cspimp.lib*	9864DBC1 C6D4E7EC DBC8C6BF D27C7B3F 0CC3CFC4 FE97AB19 EDB8FDFF E3B0ED93
c32csp.zip*	1A733D6A 7D84ADD5 9CA67683 8926CD85 B6553003 51416B00 17EE0F0F 93BCE928

Розрахунок геш-функцій здійснено відповідно до ГОСТ 34.311-95 з урахуванням значення нульового стартового вектора та ДКБ № 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 19.06.2020.

Перший заступник Голови Служби О.В. Корнейко

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

01.02.2017 № 04103/02-302

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 01.02.2017 м. Київ

Виданий: Товариству з обмеженою відповідальністю "САЙФЕР БІС" (код ЄДРПОУ 33349855)

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 24.01.2017 № 273.

Об'єкт експертизи: Система криптографічного захисту інформації "Шифр-Х.509" ТЗ У 72.2 23154898 002:2007.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю "САЙФЕР БІС" (код ЄДРПОУ 33349855).

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 криптографічні алгоритми, визначені ДСТУ ГОСТ 28147:2009, ГОСТ 34.311-95, ДСТУ 4145-2002 (в поліноміальному базисі).
2. В об'єкті експертизи правильно реалізовано криптографічний протокол автономного узгодження ключів типу Діффі-Гелмана (KANIDH), який наведено в п. 8.2 ДСТУ ISO/IEC 15946-3:2006.
3. В об'єкті експертизи механізми зберігання особистих ключів електронного цифрового підпису відповідають вимогам документа "Система криптографічного захисту інформації "Шифр-Х.509". Методика захисту особистого ключа ЦСК" (до вх. № 4787 від 13.12.2012).
4. 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.
5. Формати криптографічних повідомлень та протоколи узгодження ключів, які реалізовано 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.

6. 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, 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.

7. Формат заявок на формування сертифікатів відкритих ключів, що створюються та обробляються об'єктом експертизи, відповідає вимогам PKCS#10 Certification Request Syntax Standard.

8. Об'єкт експертизи відповідає вимогам технічного завдання ТЗ У 72.2 23154898 002:2007 із Доповненням № 1 ТЗ У 72.2 23154898 002:2007-1, Доповненням № 2 ТЗ У 72.2 23154898 002:2007-2 та Доповненням № 3 ТЗ У 72.2 23154898 002:2007-3 до нього в частині реалізації функцій криптографічних перетворень.

9. 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.

10. Об'єкт експертизи може бути використаний для побудови акредитованого центру сертифікації ключів.

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 CiX509_CA	
CiX509API.dll*	01B79814 69321B05 C3C5804F D63F9C1D 0B66A532 66BB28C2 B7238A31 1FBE320A
CiX509Core.dll*	E4CA8761 EE850B48 82737158 E0106BFC F6D9C0E9 4C81C081 5EE1817F B35EE820
CiX509Server.dll*	93E107EE 2C3C25F0 6FCFB9F1 BA88C541 5B131157 6F079423 35678495 54C71446
cixCSP_API.dll*	3A1B6A38 9C8DB668 3A59E990 344B2F1D CDFBEF00 E414BD05 B792C563 D42C07E7
cphpki.dll*	28620C7A BC4A5193 5DBFD29D E1858CC2 1F1D3054 93B07B61 F8FE7BD8 300571A4
cx509pki.dll*	EA57FEA3 33C0D400 33C0290E 5047BBC9 E2AD6AA4 C4E79B06 72E696A1 BB7B3653
dstu4145.dll*	3AE2BCF5 06F7D107 1D88B3C8 EAA3F0C5 871FAF67 1F55C0D8 33636D69 B9B45D95
Каталог CiX509_CAdm	
CiX509API.dll*	01B79814 69321B05 C3C5804F D63F9C1D 0B66A532 66BB28C2 B7238A31 1FBE320A
CiX509Core.dll*	E4CA8761 EE850B48 82737158 E0106BFC F6D9C0E9 4C81C081 5EE1817F B35EE820
CiX509Server.dll*	93E107EE 2C3C25F0 6FCFB9F1 BA88C541 5B131157 6F079423 35678495 54C71446
cixCSP_API.dll*	3A1B6A38 9C8DB668 3A59E990 344B2F1D CDFBEF00 E414BD05 B792C563 D42C07E7
cx509pki.dll*	EA57FEA3 33C0D400 33C0290E 5047BBC9 E2AD6AA4 C4E79B06 72E696A1 BB7B3653
dstu4145.dll*	3AE2BCF5 06F7D107 1D88B3C8 EAA3F0C5 871FAF67 1F55C0D8 33636D69 B9B45D95
Каталог CiX509_CAServer	
CiX509API.dll*	01B79814 69321B05 C3C5804F D63F9C1D 0B66A532 66BB28C2 B7238A31 1FBE320A
CiX509Core.dll*	E4CA8761 EE850B48 82737158 E0106BFC F6D9C0E9 4C81C081 5EE1817F B35EE820
CiX509Server.dll*	93E107EE 2C3C25F0 6FCFB9F1 BA88C541 5B131157 6F079423 35678495 54C71446
cixCSP_API.dll*	3A1B6A38 9C8DB668 3A59E990 344B2F1D CDFBEF00 E414BD05 B792C563 D42C07E7
cx509pki.dll*	EA57FEA3 33C0D400 33C0290E 5047BBC9 E2AD6AA4 C4E79B06 72E696A1 BB7B3653
dstu4145.dll*	3AE2BCF5 06F7D107 1D88B3C8 EAA3F0C5 871FAF67 1F55C0D8 33636D69 B9B45D95
Каталог CiX509_chk	
CiX509API.dll*	01B79814 69321B05 C3C5804F D63F9C1D 0B66A532 66BB28C2 B7238A31 1FBE320A
CiX509Core.dll*	E4CA8761 EE850B48 82737158 E0106BFC F6D9C0E9 4C81C081 5EE1817F B35EE820
cixCSP_API.dll*	3A1B6A38 9C8DB668 3A59E990 344B2F1D CDFBEF00 E414BD05 B792C563 D42C07E7
cx509pki.dll*	EA57FEA3 33C0D400 33C0290E 5047BBC9 E2AD6AA4 C4E79B06 72E696A1 BB7B3653
dstu4145.dll*	3AE2BCF5 06F7D107 1D88B3C8 EAA3F0C5 871FAF67 1F55C0D8 33636D69 B9B45D95
Каталог CiX509_CtxViewer	
CiX509API.dll*	01B79814 69321B05 C3C5804F D63F9C1D 0B66A532 66BB28C2 B7238A31 1FBE320A
CiX509Core.dll*	E4CA8761 EE850B48 82737158 E0106BFC F6D9C0E9 4C81C081 5EE1817F B35EE820
cixCSP_API.dll*	3A1B6A38 9C8DB668 3A59E990 344B2F1D CDFBEF00 E414BD05 B792C563 D42C07E7
cx509pki.dll*	EA57FEA3 33C0D400 33C0290E 5047BBC9 E2AD6AA4 C4E79B06 72E696A1 BB7B3653
dstu4145.dll*	3AE2BCF5 06F7D107 1D88B3C8 EAA3F0C5 871FAF67 1F55C0D8 33636D69 B9B45D95

Каталог CiX509_CVR

CiX509API.dll*	01B79814 69321B05 C3C5804F D63F9C1D 0B66A532 66BB28C2 B7238A31 1FBE320A
CiX509Core.dll*	E4CA8761 EE850B48 82737158 E0106BFC F6D9C0E9 4C81C081 5EE1817F B35EE820
CiX509_CVR.exe*	931EA593 6110698E C39CEA6F BB5E1866 9A71724C B9F48AF5 663B63FF E1ED4118
cixCSP_API.dll*	3A1B6A38 9C8DB668 3A59E990 344B2F1D CDFBEF00 E414BD05 B792C563 D42C07E7
cphpki.dll*	28620C7A BC4A5193 5DBFD29D E1858CC2 1F1D3054 93B07B61 F8FE7BD8 300571A4
cx509pki.dll*	EA57FEA3 33C0D400 33C0290E 5047BBC9 E2AD6AA4 C4E79B06 72E696A1 BB7B3653
dstu4145.dll*	3AE2BCF5 06F7D107 1D88B3C8 EAA3F0C5 871FAF67 1F55C0D8 33636D69 B9B45D95

Каталог CiX509_Java_lib

ccx509auth.jar*	52EC8E9E E8E9F25E 0D7B3924 CCB9072F 2C99D404 F850F03D 86C9FECC E2F2C26D
ccx509v1.20.jar*	0FC563A9 DD22B2CD 1F430269 A1BF5C7D 5DC55C14 2A71B946 C1F980C3 79EDAFDB
ccx509v1.22.jar*	3C802A5D 50C9353C EE49B8F8 97A9FC8F 1A73ADF6 EF167402 096574B1 947EAC58
cipherplus.jar*	8FB24B43 27208537 E3B901E3 D15362BD F7A083EF 233553A2 CDDC2B53 05299D4C

Каталог CiX509_KCC

CiX509_KCC.exe*	D1208942 6684633E 4E094758 8CD7DD91 E3A1BBB0 41687F9A 762BBD71 580BE3D9

Каталог CiX509_LogViewer

CiX509API.dll*	01B79814 69321B05 C3C5804F D63F9C1D 0B66A532 66BB28C2 B7238A31 1FBE320A
CiX509Core.dll*	E4CA8761 EE850B48 82737158 E0106BFC F6D9C0E9 4C81C081 5EE1817F B35EE820
cixCSP_API.dll*	3A1B6A38 9C8DB668 3A59E990 344B2F1D CDFBEF00 E414BD05 B792C563 D42C07E7
cx509pki.dll*	EA57FEA3 33C0D400 33C0290E 5047BBC9 E2AD6AA4 C4E79B06 72E696A1 BB7B3653
dstu4145.dll*	2C044E31 3AA74559 1FF522D9 23085CD9 50EFAEEE D527D179 915E81C9 A171CACE

Каталог CiX509_OCC

CiX509API.dll*	01B79814 69321B05 C3C5804F D63F9C1D 0B66A532 66BB28C2 B7238A31 1FBE320A
CiX509Core.dll*	E4CA8761 EE850B48 82737158 E0106BFC F6D9C0E9 4C81C081 5EE1817F B35EE820
cixCSP_API.dll*	3A1B6A38 9C8DB668 3A59E990 344B2F1D CDFBEF00 E414BD05 B792C563 D42C07E7
cx509pki.dll*	EA57FEA3 33C0D400 33C0290E 5047BBC9 E2AD6AA4 C4E79B06 72E696A1 BB7B3653
dstu4145.dll*	3AE2BCF5 06F7D107 1D88B3C8 EAA3F0C5 871FAF67 1F55C0D8 33636D69 B9B45D95

Каталог CiX509_OCSPServer

CiX509API.dll*	01B79814 69321B05 C3C5804F D63F9C1D 0B66A532 66BB28C2 B7238A31 1FBE320A
CiX509Core.dll*	E4CA8761 EE850B48 82737158 E0106BFC F6D9C0E9 4C81C081 5EE1817F B35EE820
cixCSP_API.dll*	3A1B6A38 9C8DB668 3A59E990 344B2F1D CDFBEF00 E414BD05 B792C563 D42C07E7
cx509pki.dll*	EA57FEA3 33C0D400 33C0290E 5047BBC9 E2AD6AA4 C4E79B06 72E696A1 BB7B3653
dstu4145.dll*	3AE2BCF5 06F7D107 1D88B3C8 EAA3F0C5 871FAF67 1F55C0D8 33636D69 B9B45D95
ocspsrv.exe*	89210265 AE316DF7 60279CBC 53CAF2B4 AB1A2793 D79814D4 F0B924B9 92A92D17

Каталог CiX509_Office_Addin

AddinCommon.dll*	78080D08 A2276F82 FB9C5AE0 36A1C405 52705BFF F521DA3B 8EF62554 74B4BDCD
CiX509API.dll*	01B79814 69321B05 C3C5804F D63F9C1D 0B66A532 66BB28C2 B7238A31 1FBE320A
CiX509Core.dll*	E4CA8761 EE850B48 82737158 E0106BFC F6D9C0E9 4C81C081 5EE1817F B35EE820
CiX509Server.dll*	93E107EE 2C3C25F0 6FCFB9F1 BA88C941 5B131157 6F079423 35678495 54C71446
CiXCSP_API.dll*	3A1B6A38 9C8DB668 3A59E990 344B2F1D CDFBEF00 E414BD05 B792C563 D42C07E7
cphpki.dll*	28620C7A BC4A5193 5DBFD29D E1858CC2 1F1D3054 93B07B61 F8FE7BD8 300571A4
cx509pki.dll*	EA57FEA3 33C0D400 33C0290E 5047BBC9 E2AD6AA4 C4E79B06 72E696A1 BB7B3653
dstu4145.dll*	3AE2BCF5 06F7D107 1D88B3C8 EAA3F0C5 871FAF67 1F55C0D8 33636D69 B9B45D95
Excel2010Crypto.dll*	3069D17B 18DFCE8B 78ED69B0 C975B53B 24273BB5 43D1C077 847AB0F9 14A34967
LibAdapter.dll*	4E2D2555 D01FDDB7 F7ED403E DE25E952 F00015D0 BF4920D8 322238DD F9D04DD1
Outlook2010Crypto.dll*	A99AF69B E1340D77 D5E68667 434592A2 9F70DE4B 897BAAF0 DF9211FF E128BDC4
PowerPoint2010Crypto.dll*	B2473905 972888E6 A77E5BA4 EEDCC886 8E55F999 3748C785 1670281F A11E37C4
Word2010Crypto.dll*	C5AC091C 61E034C5 D3DDB9C6 8CFACED3 C071D5B4 C65E50EA 2B5F5529 D3A4786E

Каталог CiX509_Opr

CiX509API.dll*	01B79814 69321B05 C3C5804F D63F9C1D 0B66A532 66BB28C2 B7238A31 1FBE320A
CiX509Core.dll*	E4CA8761 EE850B48 82737158 E0106BFC F6D9C0E9 4C81C081 5EE1817F B35EE820
CiXCSP_API.dll*	3A1B6A38 9C8DB668 3A59E990 344B2F1D CDFBEF00 E414BD05 B792C563 D42C07E7
cx509pki.dll*	EA57FEA3 33C0D400 33C0290E 5047BBC9 E2AD6AA4 C4E79B06 72E696A1 BB7B3653
dstu4145.dll*	3AE2BCF5 06F7D107 1D88B3C8 EAA3F0C5 871FAF67 1F55C0D8 33636D69 B9B45D95

Каталог CiX509_PW

careport1.dll*	E11506B7 5B6AFC2A FBCAD643 3603DEB3 B7CC816B 54168D93 239C5254 0D1F59DB
careport2.dll*	7FE99056 4D56A345 0CDC1820 6A6DF353 8D9E6DFD A5D40EF6 92E3F941 FC996700
CiX509-PW.exe*	28B227F8 E424C14B 744E45DA E997AD64 0573A2AC D91BB7AF 00FC9C63 7D9881DB
CiX509API.dll*	01B79814 69321B05 C3C5804F D63F9C1D 0B66A532 66BB28C2 B7238A31 1FBE320A
CiX509Core.dll*	E4CA8761 EE850B48 82737158 E0106BFC F6D9C0E9 4C81C081 5EE1817F B35EE820
CiXCSP_API.dll*	3A1B6A38 9C8DB668 3A59E990 344B2F1D CDFBEF00 E414BD05 B792C563 D42C07E7
cimtsa.dll*	F4C05D10 D2E3513F 4FF1DC33 44CA9B07 5948B62F CBF91A05 B9FB19EB 7C2E7786
cphpki.dll*	28620C7A BC4A5193 5DBFD29D E1858CC2 1F1D3054 93B07B61 F8FE7BD8 300571A4
cx509pki.dll*	EA57FEA3 33C0D400 33C0290E 5047BBC9 E2AD6AA4 C4E79B06 72E696A1 BB7B3653
dstu4145.dll*	3AE2BCF5 06F7D107 1D88B3C8 EAA3F0C5 871FAF67 1F55C0D8 33636D69 B9B45D95
tsareport1.dll*	2B71C753 A5529222 40FA5F50 9158D075 06F012E5 D9E0230A D196D7AD 9D8621A1
tsareport2.dll*	70F4C3FB 1D865F70 B884C4A9 BF90BAFF D0815BC3 847CBE3B FD3D54B7 F2011514

Каталог CiX509_RA

CiX509API.dll*	01B79814 69321B05 C3C5804F D63F9C1D 0B66A532 66BB28C2 B7238A31 1FBE320A
CiX509Core.dll*	E4CA8761 EE850B48 82737158 E0106BFC F6D9C0E9 4C81C081 5EE1817F B35EE820
cixCSP_API.dll*	3A1B6A38 9C8DB668 3A59E990 344B2F1D CDFBEF00 E414BD05 B792C563 D42C07E7
cx509pki.dll*	EA57FEA3 33C0D400 33C0290E 5047BBC9 E2AD6AA4 C4E79B06 72E696A1 BB7B3653
dstu4145.dll*	3AE2BCF5 06F7D107 1D88B3C8 EAA3F0C5 871FAF67 1F55C0D8 33636D69 B9B45D95

Каталог CiX509_RA_CM								
CiX509API.dll*	01B79814	69321B05	C3C5804F	D63F9C1D	0B66A532	66BB28C2	B7238A31	1FBE320A
CiX509Core.dll*	E4CA8761	EE850B48	82737158	E0106BFC	F6D9C0E9	4C81C081	5EE1817F	B35EE820
cixCSP_API.dll*	3A1B6A38	9C8DB668	3A59E990	344B2F1D	CDFBEF00	E414BD05	B792C563	D42C07E7
cx509pki.dll*	EA57FEA3	33C0D400	33C0290E	5047BBC9	E2AD6AA4	C4E79B06	72E696A1	BB7B3653
dstu4145.dll*	3AE2BCF5	06F7D107	1D88B3C8	EAA3F0C5	871FAF67	1F55C0D8	33636D69	B9B45D95
Каталог CiX509_RRA								
CiX509API.dll*	01B79814	69321B05	C3C5804F	D63F9C1D	0B66A532	66BB28C2	B7238A31	1FBE320A
CiX509Core.dll*	E4CA8761	EE850B48	82737158	E0106BFC	F6D9C0E9	4C81C081	5EE1817F	B35EE820
cixCSP_API.dll*	3A1B6A38	9C8DB668	3A59E990	344B2F1D	CDFBEF00	E414BD05	B792C563	D42C07E7
cx509pki.dll*	EA57FEA3	33C0D400	33C0290E	5047BBC9	E2AD6AA4	C4E79B06	72E696A1	BB7B3653
dstu4145.dll*	3AE2BCF5	06F7D107	1D88B3C8	EAA3F0C5	871FAF67	1F55C0D8	33636D69	B9B45D95
Каталог CiX509_SA								
CiX509-SA.exe*	9D0C1659	68183E69	C5C9165A	E6389F63	8559AB60	11D22F1D	B3760398	2B5D985A
CiX509API.dll*	01B79814	69321B05	C3C5804F	D63F9C1D	0B66A532	66BB28C2	B7238A31	1FBE320A
CiX509Core.dll*	E4CA8761	EE850B48	82737158	E0106BFC	F6D9C0E9	4C81C081	5EE1817F	B35EE820
CiX509Server.dll*	93E107EE	2C3C25F0	6FCFB9F1	BA88C541	5B131157	6F079423	35678495	54C71446
cixCSP_API.dll*	3A1B6A38	9C8DB668	3A59E990	344B2F1D	CDFBEF00	E414BD05	B792C563	D42C07E7
cphpki.dll*	28620C7A	BC4A5193	5DBFD29D	E1858CC2	1F1D3054	93B07B61	F8FE7BD8	300571A4
cx509pki.dll*	EA57FEA3	33C0D400	33C0290E	5047BBC9	E2AD6AA4	C4E79B06	72E696A1	BB7B3653
dstu4145.dll*	2C044E31	3AA74559	1FF522D9	23085CD9	50EFABEE	D527D179	915E81C9	A171CACE
Каталог CiX509_TSPServer								
CiX509API.dll*	01B79814	69321B05	C3C5804F	D63F9C1D	0B66A532	66BB28C2	B7238A31	1FBE320A
CiX509Core.dll*	E4CA8761	EE850B48	82737158	E0106BFC	F6D9C0E9	4C81C081	5EE1817F	B35EE820
CiXCSP_API.dll*	3A1B6A38	9C8DB668	3A59E990	344B2F1D	CDFBEF00	E414BD05	B792C563	D42C07E7
cx509pki.dll*	EA57FEA3	33C0D400	33C0290E	5047BBC9	E2AD6AA4	C4E79B06	72E696A1	BB7B3653
dstu4145.dll*	3AE2BCF5	06F7D107	1D88B3C8	EAA3F0C5	871FAF67	1F55C0D8	33636D69	B9B45D95
tsavc.exe*	1CABEA3F	FF2BB733	5E7ACAAE	93EEE83C	4812C472	A4B28C39	9FB7E82D	12D77189
Каталог CiX509_Win32_lib								
CiX509API.dll*	01B79814	69321B05	C3C5804F	D63F9C1D	0B66A532	66BB28C2	B7238A31	1FBE320A
CiX509Core.dll*	E4CA8761	EE850B48	82737158	E0106BFC	F6D9C0E9	4C81C081	5EE1817F	B35EE820
CiXCSP_API.dll*	3A1B6A38	9C8DB668	3A59E990	344B2F1D	CDFBEF00	E414BD05	B792C563	D42C07E7
cphpki.dll*	28620C7A	BC4A5193	5DBFD29D	E1858CC2	1F1D3054	93B07B61	F8FE7BD8	300571A4
cx509pki.dll*	EA57FEA3	33C0D400	33C0290E	5047BBC9	E2AD6AA4	C4E79B06	72E696A1	BB7B3653
dstu4145.dll*	3AE2BCF5	06F7D107	1D88B3C8	EAA3F0C5	871FAF67	1F55C0D8	33636D69	B9B45D95
Каталог CiX509_Win32_lib_RA								
CiX509API.dll*	01B79814	69321B05	C3C5804F	D63F9C1D	0B66A532	66BB28C2	B7238A31	1FBE320A
CiX509Core.dll*	E4CA8761	EE850B48	82737158	E0106BFC	F6D9C0E9	4C81C081	5EE1817F	B35EE820
CiX509Server.dll*	93E107EE	2C3C25F0	6FCFB9F1	BA88C541	5B131157	6F079423	35678495	54C71446
CiXCSP_API.dll*	3A1B6A38	9C8DB668	3A59E990	344B2F1D	CDFBEF00	E414BD05	B792C563	D42C07E7
cx509pki.dll*	EA57FEA3	33C0D400	33C0290E	5047BBC9	E2AD6AA4	C4E79B06	72E696A1	BB7B3653
dstu4145.dll*	3AE2BCF5	06F7D107	1D88B3C8	EAA3F0C5	871FAF67	1F55C0D8	33636D69	B9B45D95

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 24.01.2022.

Перший заступник Голови Служби О.М. Чаузов