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

18.03.2019 № 04/03/02-749

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 18.03.2019 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 15.03.2019 № 391.

Об'єкт експертизи: Програмний комплекс криптографічного захисту мережевих з'єднань «Шифр-VPN» ТЗ У 72.2 23154898-004:2018.

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

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 (в режимі гамування зі зворотнім зв'язком), ДСТУ 7624:2014 (в режимі CBC), ГОСТ 34.311-95, ДСТУ 7564:2014.
2. В об'єкті експертизи правильно реалізовано криптографічні алгоритми шифрування DES, TDEA, AES, визначені ДСТУ ISO/IEC 18033-3:2015 (в режимі CBC, визначений ДСТУ ISO/IEC 10116:2014).
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 15946-3:2015.
4. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-1, SHA-256, SHA-384, SHA-512, визначені ДСТУ ISO/IEC 10118-3:2005.
5. Формат посилених сертифікатів відкритих ключів, формат списків відкликаних сертифікатів, протокол визначення статусу сертифікату, структура об'єктних ідентифікаторів для криптоалгоритмів, що є державними стандартами, які створюються та/або 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.
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. Об'єкт експертизи відповідає вимогам технічного завдання ТЗ У 72.2 23154898-004:2018 в частині реалізації функцій криптографічних перетворень.

8. 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 CiPlus v2.5
Каталог android-armv7-32
Каталог DLL
libCCPPLib.so                  3E6781F7 A8E01208 B31CCF1D C612FED0 B9500751 CCDAFCF2 E07BD84E 564AFFE2
libCCPPLib.so.recipe           28EF2736 D96F2398 CAFCE4C1 28234163 BA28EDAF CAEEE5AA AA81586F 00166ABD
libCCPPLib.a                   85DD0DD9 16CDBECF 62D0ED83 FCA46D6C 4B4A5CFE EE525F1F ED3C0EA4 A8455854
libCCPPLib.a.recipe            841B714C F139E414 E8098F93 FDDFE95A 04A7269E DE15D0CF 42D6F3A3 2C3EFF93
Каталог android-armv8-64
Каталог DLL
libCCPPLib.so                  7E00B0A9 50A18218 459A98BF AFE7E5D0 8ACDB5DE 7D73002B 3420B937 6A324502
libCCPPLib.so.recipe           42D18C82 557F15DF 15EB4850 C6EBBF00 FE78EB0C 547AEE3B 8B420AD1 D3742ECD
libCCPPLib.a                   8DCDB8C9 866DEA59 089B2AB0 94047E4D 35823F75 36886921 D6C6788F 75668B39
libCCPPLib.a.recipe            059A5AD8 47B22AF7 BE48F00E F73268CC 36288348 8827A000 D785E2C0 8478C516
Каталог android-x86-64
Каталог DLL
libCCPPLib.so                  7F5B4F66 8C8BA205 F9D591E8 E08D1182 5C496A01 C5154612 61087EDF CCCB3043
libCCPPLib.so.recipe           15B8AA2C 0F1D1EAC 15E8DEDC E28223B8 F5CB3805 42557FEB B83FC177 E66D2663
libCCPPLib.a                   7B04F081 A189F991 C30D7A6C B15A6E48 DC271F8A 2933F77D A61CDBAE 7F1AD588
libCCPPLib.a.recipe            F846ED6A F4B69870 B8399A5B 8AE71A3F FD849A2C C2252C6E CC05630A 0D4D5D6E
Каталог android-x86
Каталог DLL
libCCPPLib.so                  2B431B48 4236CE7A 91386EF6 308EA3CF FF3474B1 FFE6198F AF70526E 6AAB1C25
libCCPPLib.so.recipe           79E1099A 5ED35932 A288FB5A 29D8DE78 32B56F45 C4F6793A 13577DBA 278046BA
libCCPPLib.a                   4E95F102 E79F09D0 1F60468C 62574C0C B008AF84 FEEA4C1D 14445BF9 83149612
libCCPPLib.a.recipe            4542158E A26034D4 C93D196B 877E73FC 566D3C30 DD07C6BF 6C4307A4 472100E8

Каталог freebsd-x86-64
Каталог DLL
libccpplibib.so                66568BD2 9C0963C5 86DE5B70 A3D60BAA B7A182F3 1A5B5CCB 6911A956 059983F8
libccpplib.a                   83295316 4773D296 04D386C4 7C327979 19857C91 82E92D75 A3304C86 8DAEAC00
Каталог freebsd-x86
libccpplib.a                   46DE0AE2 E0784B06 28CBEE63 3C9ECB43 C7CE79E4 4060582C 8BD38F37 E8299031
Каталог ios
CCPPLib-ios-combined.a         54A770D8 4ED64E81 A56786BD FA3E4F57 96FBAA9E 96ABC7AB EC0079B1 D53A443F
libCCPPLib-iOS-simulator.a     0BC36A9F 09DBEA21 87BC39F4 A2195B53 BC1B5524 316F6292 BDD4DDD6 9E92561D
libCCPPLib-iOS.a               7CE2B087 A337C069 6C69B8D9 35BFAA8F 8C5F69D9 2E3F6E2E AC822C34 EE6903F5
Каталог linux-x86-64
Каталог DLL
libccpplib-linux.so            4ACD46E0 A1AC0DD5 0E540F16 2C83E5D3 9153E0B9 FFFAF904 94F0B5C6 61DC4449
libccpplib-linux.a             289F892B FBDB4812 E7760FBF 93C0D4B4 51A32C0C 8ECE3DCC 6BFBCD1A 1E784E4D
Каталог linux-x86
Каталог DLL
libccpplib-linux.so            B5E97894 F02918AB 3817FF6A B5DF258E 79E9D6CE 7F10875B 052E2E1E A75BD928
libccpplib-linux.a             9EE459B7 DA187B93 B7B062AD 5B5C4782 6E27E9C9 5FB1A59A A740FBFD 34F17FA9
Каталог macos
libCCPPLib.a                   C175EDF9 0EBDCB14 EBC3E99C 9AC29B5F 1EE172F2 3C1D87B4 3E3907BC 004A83E1
Каталог windows-x86-64
Каталог DLL
CCPPLib.lib                    D6434CC6 95006B3D DB3E89B1 C4466749 FAB68012 77828BBA FBE7B31D D979FDC2
CCPPLib.dll                    C1022C5D 51BCE4C7 FBCF810B 3C58D9FB CF780B04 1B36ACA6 AEDFB354 27C41413
CCPPLib.lib                    B3CBF8A9 EFB48CD5 2ECB711F C996D7F8 EE64B505 20AF47CF A39323A1 5919DDE7
Каталог windows-x86
Каталог DLL
CCPPLib.dll                    A5505C57 CE3CFF7C 30272992 7E2F448F B31A9D46 E0195E5F 54B2BD89 745BB860
CCPPLib.lib                    A71D9A66 C0D178EB BE0D16A4 E1DF478D EA72C5B3 C9468B1D 0838017E A319CF90
```

CCPPLib.lib	713847F2 2939C22E 99345AA8 AD243BE4 C45F1ACB 6F9ED27F BB54C9F9 A5FAB926
Каталог CiVPN	
Каталог android (x86, x86-64, ARMv7, ARMv8)	
civpn-0.7.7.apk	5BB8E178 0B9126E2 CBF3AED8 B277766E 70A1E043 6F964D28 B7595C71 4816A23C
Каталог freebsd-x86-64	
CiVPNServer	5797456F B6244CC1 AAB2A0C2 F028E622 7D7E3F48 8DB73026 ABBC2779 B033C133
CiVPN_serv	769FC3DF 62F9CFAC 2F22D6D2 3C2F734C 9B101EE9 C56173FF 0C076E53 D5F634FE
libcipher_openssl_engine.so	E7572F79 69929B4B 8D8EEDA9 D1B05134 6E2E6AE4 9127CF0A D4980E82 5EB97B5E
libcrypto.so.1.1	8A35E16F 6D65B676 46DE3408 C7C055F7 0105C453 EF32F2A4 0E333025 DB91FC86
libssl.so.1.1	35EB6565 F60219C4 C873DD3F E7E5F1E1 658D8BAD 1B4C2A55 3134A47B 77A07739
Каталог freebsd-x86	
CiVPNServer	6A7CC21F 6288D5AC 0CD2C9C4 591EA511 3DD30757 2A8978E0 7CAAA09E 7245CD43
CiVPN_serv	041B6385 A1BBE2ED 26A71BFE 439FD239 D1134B80 11FCE66C A26D3DF6 7CCCCF89
libcipher_engine.so	A13A873C 46D9BBCA 5361C80D 4432B2B5 3ABB29E8 C4E2ADD9 769E19DE 1CC75FC0
libcrypto.so.1.1	3AFD1B39 D287716E B57E2561 66AE6ECF 9D24920C 560A48D6 A8AB6DE1 562F6CD6
libssl.so.1.1	6EEB9BCB 60524E21 FD7B15C9 2FDC68D2 0563BDD1 74DE627E 5370C04A 85468695
Каталог linux-x86-64	
CiVPNServer	ABF4D604 2BAB07AC B2241B3E 2E676355 9C6979A1 6B1F380F E40239C7 96028745
CiVPN_serv	B5F54A0D 56057DE3 A66FF54B 0E3880F0 22F90C88 05A2738F 02E9B90F EBF66A8A
libcipher_openssl_engine.so	D31488F8 CDEBEF73 B00C4407 EF0DE656 63ABC4D1 4FBE0DE9 53E49870 AA0C2AF7
libcrypto.so.1.1	FB6E07D3 D9378933 98E42CEA 88C2BBC7 86C4A3CF 1DF5913E 2CDD3136 DC0D248D
libssl.so.1.1	A1CC4466 368C02E9 4D846203 239AB8D3 7FBC6DB8 182C3BC7 B377CEEC 6259A133
Каталог linux-x86	
CiVPNServer	2CEED640 CD98EB35 2D5F71AF FE4E8418 9A13BBCE CA588898 F682F6F7 FFB927D3
CiVPN_serv	E6D06C98 78544EDA EE15C270 44DE95F5 4E113EF6 BA191287 4F68C594 24719D26
libcipher_openssl_engine.so	E32FE5B8 10F8A566 A869709C EE758E52 5C45115D BB486325 8AC998F7 DE47946D
libcrypto.so.1.1	9F4C0BAA 4AC21509 7DF5B4AC 8DEDC6CC CD431B4D BD35791A A5767670 4CA768EF
libssl.so.1.1	8F347CA5 034E7879 80C20670 60580D8F D5FFB123 B8C7A857 838B4123 3CE45DE6
Каталог macosx-x86-64	
CiVPNServer	1C096811 65248A8D 16F13B18 93128ED1 16C5BD11 5F4E542D 7F2AA5BE 11400745
CiVPN_serv	4741A839 8E79EDF9 6002BB2D 856B6968 6F0F4FF4 0D69C843 304AFB51 5E66514C
libcipher_openssl_engine.dylib	6CF2D52E BED3A153 4E2A0009 8DBA9F38 D1C755EB 852A2D40 D7A2A9F2 28254812
libcrypto.dylib	4B0E2039 ED518B93 02F5D126 99AAF370 BC099F8F 43FD1891 644FFC1E 7F40B283
libssl.dylib	35EB6565 F60219C4 C873DD3F E7E5F1E1 658D8BAD 1B4C2A55 3134A47B 77A07739
Каталог windows-x86-64	
cipher_engine.dll	76A08622 F5255A1E 78C1FDE7 B5802DA6 DC2D67C6 99CDFCAA 5563C862 A56DDFAE
CiVPNServer.exe	89C159FB 46272E13 7D5C59B1 E3E153CB C0CEB6BD C2DD63A0 64EE0BE7 28B51B3B
CiVPN_serv.exe	AF0B06ED 3410D779 C2A26383 003DCCAC 2A4B3609 BD6BAC03 F2CE150A 9527A8FD
libcrypto-1_1-x64.dll	3C960A3A 932B5A14 02FFE080 5AC0815A E9AB6F79 EADE54EB 06733BD9 34551FA3
libssl-1_1-x64.dll	B08F6425 6844E5F1 D06D4DDC E85A5247 84EF269B 9E3AD689 7412A994 CCA0B89A
lzo2.dll	530059CC 565A8A63 28A8D79D 333E5FC9 B3D5B677 65003988 368C99AF 9C94EBBD
Каталог windows-x86	
cipher_engine.dll	58F2600C DFBEF3EE AF3523FB F421061F 7D3D9590 3C76103E 0235A94F 18AADB8A
CiVPNServer.exe	9C9ACB23 9C92ED6B 00427089 0B5A142C EF1A8A6A FAE5039B AADFE0E7 E05B91A2
CiVPN_serv.exe	4A8C8E06 CB182CCB FAEEA2AB E0B80F67 1FE17FE7 C798B18E FC51910B 96210DE4
libcrypto-1_1.dll	1F49D1A4 CB187F27 6E210C25 176833B6 9B9328B8 202749EA 9A8C0520 F713C5B7
libssl-1_1.dll	F3479708 87BBF2AA 73EF5C69 0AC8C9DD 47B203A0 A0075198 24C997B5 0E7A7EB9
lzo2.dll	4F382C3A E8F1D3FE 5314A971 F37E7D0B 46DB4766 2B83E7FC CEE9DF37 34BD2C0F

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 15.03.2024.

Перший заступник Голови Служби О.М. Чаузов