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

23.05.14 № 05/02/02 – 1812

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 23.05.2014 м. Київ

Виданий: Товариству з обмеженою відповідальністю "БІФІТ Сервіс" (код ЄДРПОУ 37619243)

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 23.05.2014 № 149.

Об'єкт експертизи: Програмний виріб криптографічного захисту інформації "Гепард 2.0" (UA.37619243.00004-01 90 01-1).

Розроблений (виготовлений): Товариством з обмеженою відповідальністю "БІФІТ Сервіс" (код ЄДРПОУ 37619243).

Експертний заклад: Адміністрація Державної служби спеціального зв'язку та захисту інформації України (код ЄДРПОУ 34620942).

Висновки:

1. В об'єкті експертизи правильно реалізовані криптографічні алгоритми, які визначені ДСТУ 4145-2002, ГОСТ 34.311-95, ГОСТ 34.310-95, ГОСТ Р 34.10-2001, ДСТУ ГОСТ 28147:2009.
2. В об'єкті експертизи правильно реалізовані криптографічні алгоритми шифрування TDEA, AES, які визначені в ISO/IEC 18033-3:2010 і ISO/IEC 10116-3:2006.
3. В об'єкті експертизи правильно реалізовані криптографічні алгоритми SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 які визначені ДСТУ ISO/IEC 10118-3:2005.
4. В об'єкті експертизи правильно реалізований криптографічний алгоритм HMAC, який визначено IETF RFC-2104.
5. В об'єкті експертизи правильно реалізовані криптографічні алгоритми RSAES-OAEP, RSAES-PKCSl-vl_5, RSASSA-PKCS-vl 5, які визначені PKCS#1 v2.1 "RSA Cryptography Standard".
6. В об'єкті експертизи правильно реалізований алгоритм вироблення загального секретного значення за схемою Діффі-Гелмана для асиметричних ключів, які визначені ДСТУ ISO/IEC 15946-3:2006, ГОСТ Р 34.10-2001.
7. В об'єкті експертизи правильно реалізовані криптографічні алгоритми DSA, ECDSA, які визначені ДСТУ ISO/IEC 14888-3-2002.
8. Формат посиленого сертифіката відкритого ключа, структура об'єктних ідентифікаторів для криптоалгоритмів, що є державними стандартами, 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 20.08.2012 за № 1398/21710.
9. Формати криптографічних повідомлень, які реалізовані та використовуються в об'єкті експертизи, відповідають вимогам наказу Адміністрації Держспецзв'язку від 18.12.2012 № 739 "Про затвердження Вимог до форматів, криптографічних повідомлень", зареєстрованого в Міністерстві юстиції України 14.01.2013 за № 108/22640.
10. Об'єкт експертизи відповідає вимогам технічного завдання з доповненнями UA.37619243.00004-01 90 01-1 в частині реалізації функцій криптографічних перетворень.
11. 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:

Назва файлу	Значення геш-вектора
Комплекти бібліотек ANSI C-реалізації Виробу	
Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора - x86, ОС - Microsoft Windows XP та вище	
gepard.lib	2642993A 802EBB69 CDB10088 EC9EE6FF 5B5B5124 BDCD28F0 59119709 736DB284
asnl.lib	803BEBC8 55A99077 8D9FF681 C4CFC156 1CA989DB 7A981C9F B9294BB8 BA89050B
pkix.lib	49790E1E 33AA4D27 41A86F2A 2BD1DDD0 F702793E 636901D6 4897E83E 762F72BA
Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора - x86, ОС - Linux 2.6 та вище	
libgepard.a	1E50A606 E843C5C9 8EE9D258 290EC95B 953876DB E3B8296C 9079AE5C 79992E47
libasnl.a	4F2D5875 59CC5AFE 9F296D32 40EF1C43 E4171F81 EBBBFAF1 B2567909 BA5A8B1E
libpkix.a	334B6103 730E0B6B D0B12E2A 261BF88B 07ECCB8E 859BC41A 6EF10660 40A5052C
Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора - x86, ОС - Apple MacOS X 10.6 та вище	
libgepard.a	75FEDE84 FA45078C A7134A77 D45596B2 9B6FDA13 AEE2BIE0 2E15BB6B AEC7CBFC
libasnl.a	6F7F8AB7 F435553E CEED35AF 5635CFE9 12ADDA47 E9F4BBAE CC249749 115BF687
libpkix.a	0509B127 455803B7 5DF6984D A0AA22F7 75796A63 F3685E08 BEE397BC F1257E5B
Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – x86, ОС - Oracle Solaris 11 та вище	
libgepard.a	AD45BACE C3DF290E DA0FAC82 656CD87C C38431ED C7300782 F13D4D5E B8E6C950
libasnl.a	329D89A0 F2882A7F EBF62A49 2D900E43 459816B1 1BBE57B5 97145E7D B79AA05D
libpkix.a	F5011BFB E3AD7A65 271157D6 CAE16FE7 C26E3EF1 7CE008A6 66943667 02B17304
Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – x86, ОС – Google Android 3.1 та вище	
libgepard.a	D3DE00B5 D4C0E61F 2EC3ECF0 55557E61 7FA531E4 2024E453 1E770A78 0B88A054
libasnl.a	808C7969 ECBD8654 57D5C623 546FE25C 074F7D13 E2910E44 EEA81A00 883D16BB
libpkix.a	0B428AB3 48DE9381 22030708 CB72BA56 2EAB5AEE 1B99DFBC 0CB076A6 58D13669
Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – x86-64, ОС – Microsoft Windows XP та вище	
gepard.lib	98E0C360 E1C31813 A908223D 1BD7E8BA 8583443B C4D31005 43962EBB 6E8971F1
asnl.lib	0F19DB27 A94C000D 32F211B2 5258A79B 3FB48334 1DB44EEC 55B65A92 703125E2
pkix.lib	550D6838 0BA86779 302B59A9 1679E242 50C8255B EC5529A6 FE9873E8 B7910766
Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – x86-64, ОС – Linux 2.6 та вище	
libgepard.a	228FC188 78EE90FE 74AFA98A 69DEC9BB 92110E66 82D6989D 1BEC9603 46C71602
libasnl.a	6161340A A0456AF0 4873A515 C20EBC45 EA4CFD8E B7574D0F 1D46DBF2 DBEB05AF
libpkix.a	FA3E07BF E5767764 31DF8501 C6ABEFC5 F27D3D20 56F2CB10 E733C723 ED20CEDE
Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – x86-64, ОС – Apple MacOS X 10.6 та вище	
libgepard.a	948F0386 2D65A35E 9F104591 17A6DE86 A3C86DC0 B0E31CA0 4DB74C7E 5D331FA9
libasnl.a	86DB3357 7FA614AE 99A4AC82 5F5C222E 406296C8 165E5FF5 20FEAD6E 73CE7582
libpkix.a	67250A17 DF3F5D3F 3C4549B1 C77F21C0 54D1488A 35CAE723 B75BA3C1 FA2E60B6
Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – x86-64, ОС – FreeBSD 9 та вище	
libgepard.a	117C7F52 83986BAA FCF4B5EE 636E0568 C2A30AA5 7C2E71A9 D817D798 549CAE15
libasnl.a	DBDA13C6 69E0BA96 6DA3F9E0 3DF4601E 1B9D9879 55D4EFC1 98458392 D4D7987B
libpkix.a	5009C5DC C5F0A958 22AFFB27 7A2BBA5A 011AD2F1 4752647F A17838D3 B885C937
Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – PowerPC, ОС – IBM AIX 5.2 та вище	
libgepard.a	4168C1E0 AD152032 11695074 CC1DF643 50EFB9E6 10A5D170 E1994DF5 9E5C0CAB
libasnl.a	C32F8352 319E8C14 F53DACC9 0EC2CF69 E8CF5A1C D7FB60EE 6835CF52 441ED586
libpkix.a	A987CF27 2F24074E E61AF134 494385E0 B3BF64DD DF3DB795 6942337C 6B99BE4F
Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – PowerPC, ОС – Linux 2.6 та вище	
libgepard.a	1C527E24 684FCFA5 446B83E7 80F510A3 FDAF75DA 145FF4CF C47BD639 52207763
libasnl.a	1C53B4A3 1F853450 2AD9941C 74E18D2C B7BB4E68 15107854 09FBA722 09508A53
libpkix.a	A8E522A3 54B74E4C 7E051C54 42AE517E 01968DA2 A3604EA8 E71543EB 5C3AB4D5
Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – PowerPC-64, ОС – IBM AIX 5.2 та вище	
libgepard.a	08EE11CB 99AE9E0B 3AA76062 20975518 60869D36 5CD32A01 E1931978 D904D063
libasnl.a	39B8BC61 FAFC76CC 293B55A1 D8348558 3105449F 02492547 43F51D66 04D5E272
libpkix.a	4C642BF5 15C74850 BCC21161 AD221EF0 9CE65737 93BACF63 96FE3EA8 FF383629
Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – PowerPC-64, ОС – Linux 2.6 та вище	
libgepard.a	3486696E CD24E30B BB1BD3DA B4B51857 2D146E3D F0050C8D BIB05352 0C6304BE
libasnl.a	8377A6BC FE5FA484 A3C74E61 E25A3261 D84F5B87 784786CD 66C57C12 69827E34
libpkix.a	F7095B2F 56C386E5 6DF91B34 6354E415 F6914C52 56C9493E A0D59681 621C8B22
Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – Sparc, ОС – Oracle Solaris 11 та вище	
libgepard.a	1D5D45F9 3B9B528E EE227E8B 482AADCA 4B543B7D 768D61A0 D6015DD5 BEDCDF6C
libasnl.a	EA07FB6A 52641646 61B74A30 533137BE F3EE71E5 DD3509BA 0B46C6E3 0AF7E890
libpkix.a	F175E6E4 A1CD08D2 FC106CB8 9BCB47AA 853EC246 D5B431CB 0C374372 D52CA2BF
Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – Sparc-64, ОС – Oracle Solaris 11 та вище	
libgepard.a	5188D25D FE0631EE 19CD160E ED0379A9 200865A1 59973FA8 B1BDF32B D4D1B3C6
libasnl.a	2D6E78B0 DB46294B FD3066DB 2453EF0D A08D1C7D 772DD5E8 05A28A24 B41B2CFB
libpkix.a	362C9575 851B02B9 BA4F6FBD 6D59FD08 68327758 FAB58C19 9ED6E4A4 A9CB6541

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – IA64, ОС – Hewlett-Packard HP-UX 11 та вище	
libgepard.a	D500A4B7 64529650 2A7A847E 7BCB7CD3 AC928ABF F9523429 8DC5CAAE FC0E4F7B
libasnl.a	7744DE23 6FAB17BC E0A31FE6 05D3BBB9 588F2DF0 71D70CE3 0BDEE76A FA25078F
libpkix.a	F379F7A2 28975D27 5B00CAA4 FD2C6537 CC8F44FF 80DDEC86 0FC1EB03 91479C04
Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – IA64, ОС – Linux 2.6 та вище	
libgepard.a	67E8641D 623EBDF5 EBF665DC 6470780E CC839211 E5EB8F80 DE7A5AB1 2DF6CCB9
libasnl.a	2CD215F4 E2CF10FD 9937C838 7176EF08 2870C206 57C0989D A8B3B130 321D5769
libpkix.a	D3C6A36A 3CAF321E AA0215FE 574D9E39 AA17D752 6B436CD4 257A08F7 A7F047F7
Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – IA64, ОС – Microsoft Windows XP та вище	
gepard.lib	6621F6A0 30F23BA2 EFD85128 40E790AA CB394868 6A7A9531 1C8E9E7F 0679B55E
asnl.lib	13D497EF C3262640 D5511D93 07FC1334 06A97037 918290DB 13DADDF0 1BDA592C
pkix.lib	5876BB79 E593DEE0 880CFC69 FF66E1BA D85EC1E7 D61B9972 22228FAE EF5B10F8
Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – ARMv7, ОС – Google Android 3.1 та вище	
libgepard.a	185B06BB B58E2FA6 1A55008C 1E1910A4 E275096B 8B3E8688 1A9A3B42 8A0165D1
libasnl.a	4AD4AADA C8304BAE 54FE8437 4A26A712 703C5776 26A14E8D 09FEB787 6E5D611A
libpkix.a	94350B32 IB961797 26FD5542 FED84CF0 98925D92 EC8C3FA7 CB2B96CF D8AF0FC3
Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – ARMv7a, ОС – Google Android 3.1 та вище	
libgepard.a	424C917D 396C2F3E 34CD41B7 AEB93EBB 46C9BDB6 8744A33F 9B7BD4AD A5EE7F32
libasnl.a	6F26659B 1BB9AB6F 4552BB20 EC8F1E15 4922BF46 F39C0F06 BC06C0F9 12BAEBE8
libpkix.a	F7F6AB77 1A5D81A0 748B3826 3D9A40DD 9B0E1856 FF21C054 1DE5BC31 1474AA49
Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – ARMv7, ARMv7a, ARM8; ОС – Apple iOS 4 та вище	
libgepard.a	AB5062E3 E3E586BA 5A5CC5B6 7478B2A9 EFD65E50 E56870CD F4A3FA31 7C62C3A8
libasnl.a	EAF4E92E 6EF79D25 9C9D2D70 2FDD6FED 7E0C75D9 03AAA4FC 5172118F E51C4D1F
libpkix.a	A17A17E8 ED04F8AE 887239BC 37E67F9A 12416923 3D04EFD3 FF705A74 2216D2F6
Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – MIPS, ОС – Google Android 3.1 та вище	
libgepard.a	CA4D9362 E310A0F1 6AD40788 93E1F0AC 89CB145F D3053405 B0B08339 C7D2862D
libasnl.a	B8983FAF EAF296A5 0019FE87 255307B0 CD4CB5A3 19FBEA57 83745542 97987650
libpkix.a	46F885D7 C43A5576 B8993C18 100356A5 C77902CE F328A10A 29378B65 B5FEB1E5
Комплект бібліотек Java-реалізації Виробу	
gepard-2.9.0.jar	18346423 963B2F36 3C05426C F960CA91 659A6A90 B8ADA85C 61C66AD7 A2EB4B33
gepard-android-2.9.0.jar	5A06C8AF 0E0EF9F7 BFF544A7 CEDD6D71 86CE9B0A B1D6620C 1001202A 5FE30661
pkix-1.25.1.jar	F44ED980 57234051 688956C5 D10CE0C7 E8B59886 886ADA93 FFA1DDC9 93EB7453
asnl-1.8.0.jar	ABC81BEC 8DD3A12C 7F0E686C AB8E8053 2065439A 03263D42 B2798F48 9F3ADB63
log4j-1.2.17.jar	D6A4F46A B79E90E8 1E01F990 B8E40052 93B87B2A F20AFB0A 7F63F30F 89AF09C8
pki-crypto-1.2.0.jar	9FC96647 0B3FAE8B 11DE56A9 FDDA0F62 9463A03A E4CF1FA3 A112AA32 1DF33DC6
slf4j-android-1.6.1-RC1.jar	6781D455 37DB54IF BFAF550E 4D8CEC98 C01B7602 C16229A0 75A97660 5B6884CD
slf4j-api-1.7.5.jar	C3FB3F74 41D2CF91 0320CBDA 697B8C70 016A129C DD0E6CAA 88B6AE46 E1CE9413
slf4j-log4j12-1.7.5.jar	0206BB09 F53113D5 B09247D7 6874E425 20EE1BC8 2E18EEA7 097D5859 60207E25

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 Держспецзв'язку від 12.06.2007 № 114, зареєстрованої в Міністерстві юстиції України 25.06.2007 за № 729/13996.

Термін дії експертного висновку - до 23.05.2019.

Перший заступник Голови Служби О.В. Корнейко