



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@dsszzl.gov.ua

04.08.2019 № 04/03/02-1537

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 04.08.2019

м. Київ

Виданий: Товариству з обмеженою відповідальністю «ДБО Софт» (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 30.05.2019 № 404.

Об'єкт експертизи: Програмний виріб криптографічного захисту інформації «Гепард 2.0» UA.37619243.00004-01 90 01-1.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю «ДБО Софт» (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 реалізовано криптографічні алгоритми, 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 реалізовано криптографічні алгоритми шифрування TDEA, AES, визначені ISO/IEC 18033-3:2010 та ISO/IEC 10116-3:2006.
3. В об'єкті експертизи правильно реалізовано криптографічний алгоритм RSA, визначений PKCS#1 v2.1 «RSA Cryptography Standard» (за схемами RSAES-OAEP, RSAES-PKCS1-v1_5 та RSASSA-PKCS-v1_5).
4. В об'єкті експертизи правильно реалізовано криптографічні алгоритми ґешування SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, визначені ДСТУ ISO/IEC 10118-3:2005.
5. В об'єкті експертизи правильно реалізовано криптографічний алгоритм HMAC, визначений IETF RFC-2104.
6. В об'єкті експертизи правильно реалізовано алгоритм вироблення загального секретного значення за схемою Діффі-Гелмана для асиметричних ключів, згідно ДСТУ ISO/IEC 15946-3:2006, ГОСТ Р 34.10-2001.
7. В об'єкті експертизи правильно реалізовано криптографічний алгоритми формування та перевіряння електронного цифрового підпису DSA, ECDSA, визначені ДСТУ ISO/IEC 14888-3:2015.
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 UA.37619243.00004-01 90 01-1 з Доповненнями № 1, 2 до нього 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:

Комплекти бібліотек ANSI C-реалізації Виробу

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – x86, ОС – Microsoft Windows XP та вище

gopard.lib	2642993A 802E8B69 CDB10088 EC9KE6FF 5B5B5124 BDCD28F0 59119709 736DB284
asn1.lib	803BEBC8 55A99077 8D9FF681 C4CFC156 1CA9B9DB 7A981C9F B9294BB8 BA89050B
pkix.lib	4979081E 33AA4D27 41A86F2A 2BD1D0D0 F702793E 636901D6 4897E83 762F72BA

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – x86, ОС – Linux 2.6 та вище

libgopard.a	1E50A606 K043C5C9 8KE9D258 290EC95B 953876DB E3B0296C 9079AE5C 79992E47
libasn1.a	4F2D5875 59CC5AFE 9F296D32 40EF1C43 E417 F01 E8B8FAF1 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

libgopard.a	75FKDX04 F 45078C A7134A77 D45596B2 9B6FDA13 AEE2B1E0 2E15BB6B AEC7CBFC
libasn1.a	6F7F0AB7 F435553E CERD35AF 5635CFE9 12ADDA47 B9F48BAE CC249749 115BF687
libpkix.a	0509B127 455803B7 5DF6984D A0AA22F7 75795A53 F3685E08 BEK397BC F1257E5B

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – x86, ОС – Oracle Solaris 11 та вище

libgopard.a	AD45BACE C3DF290E DA0FAC82 656CD87C C38431ED C7300782 F13D4D5E B8K6C950
libasn1.a	329D89A0 F2882A7F KBF62A49 2D900E43 459816B1 1B8E57B5 97145E7D B79AA05
libpkix.a	F5011BFB K3AD7A65 271157D6 CAE16FE7 C26E3EF1 7CE008A6 66943667 02B17304

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – x86, ОС – Google Android 3.1 та вище

libgopard.a	D3DEK0B5 D4C0E61F 2EC3ECF0 55557E61 7FA53 E4 2024E453 1E770A78 0B8BA054
libasn1.a	808C7969 ECD08654 57D5C623 546FE25C 074FTD13 E2910E44 KEA81A00 883D16BB
libpkix.a	0B428AB3 48DK9381 22030708 CB72BA56 2EAB5AEE 1B99DFBC 0CB076A6 58D13669

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – x86-64, ОС – Microsoft Windows XP та вище

gopard.lib	98E0C360 K1C31813 A908223D 1BD7E8BA 8583443B C4D31005 43962EBB 6E8971F1
asn1.lib	0F19DB27 A94C000D 32F211B2 5258A79B 3FB4B334 1DB44EEC 55B65A92 703129E2
pkix.lib	550D6838 0BA8677 302B59A9 1679E242 50C8255B EC5529A6 F7E9873E B7910766

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – x86-64, ОС – Linux 2.6 та вище

libgopard.a	228FC188 78EE90FE 74AFA98A 69DEC9BB 92110E66 82D6989D 1BEC9603 46C71602
libasn1.a	6161340A A0456AF0 4873A515 C20EBC45 EA4CFD8E B7574D0F 1D46DBF2 DBEB05AF
libpkix.a	FA3E07BF E5767764 31DF8501 C6ABEFCE F27D3D20 56F2CB10 E733C723 ED20CEDE

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – x86-64, ОС – Apple MacOS X 10.6 та вище

libgopard.a	948F0386 2D65A35E 9F104591 17A6DE86 A3C86DC0 B0E31CA0 4DB74C7E 5D331FA9
libasn1.a	86DB3357 7FA614AE 99A4AC82 5F5C222E 406296C8 165E5FF5 20FEAD6E 73CE7582
libpkix.a	67250A17 DF3F5D3F 3C454981 C77F21C0 54D1488A 35CA 723 B75BA3C1 FA2E60B6

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – x86-64, ОС – FreeBSD 9 та вище

libgopard.a	117C7F52 83986BAA FCF4B5E8 636E0568 C2A30AA5 7C2E71A9 D817D798 549CAE15
libasn1.a	D8DA13C6 69K0BA96 6A3F9E 3DF4601E 1B9D9B79 55D4EFC1 98458392 D4D7987B
libpkix.a	5009C5DC C5F0A958 22AFFB27 7A28BA5A 011AD2F1 4752647F A17838D3 B885C937

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – PowerPC, ОС – IBM AIX 5.2 та вище

libgopard.a	4168C1E0 AD152032 11695074 CC1DF643 50E8B9E6 10A5D170 K1994DF5 9E5C0CAB
libasn1.a	C32F0352 319E8C14 F53DAC9 0BC2CF69 E8CF5A1C D7FB60EE 6835CF52 441ED586
libpkix.a	A987CF27 2F24074E E61AF134 494385E0 B3BF64DD DF3DB795 6942337C 6B99884F

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – PowerPC, OC – Linux 2.6

та вище

libgopard.a	1C527E24	684FCFA5	446B83E7	80F510A3	FDAN75DA	145FF4CF	C47BD639	52207763
libasn1.a	1C53B4A3	1F053450	2AD9941C	74E18D2C	B7BB4E68	15107854	09FBA722	0950BA53
libpkix.a	A8E522A3	54B74E4C	7E051C54	42AE517E	01968DA2	A3604EA8	E71543EB	5C3AB4D5

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – PowerPC-64, OC – IBM

AIX 5.2 та вище

libgopard.a	06EE11CB	99AE9E0B	3AA76062	20975518	60869D36	5CD32A01	E1931978	D904D063
libasn1.a	39B8BC61	FAPC76CC	293B55A1	D8348558	3105449F	02492547	43F51D66	04D5E272
libpkix.a	4C642BF5	15C74850	BC21161	AD221EF0	9CE65737	93BACF63	96F83EA8	FF383629

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – PowerPC-64, OC – Linux

2.6 та вище

libgopard.a	34B6696E	CD24E30B	B1BD3DA	B4B51857	2D146E3D	F0050C8D	B1B05352	0C63048E
libasn1.a	8377A6BC	FE5FA484	A3C74E61	E25A3261	D84F5887	784786CD	66C57C12	69827E34
libpkix.a	F7095B2F	56C386E5	6DF91B34	6354E415	F6914C52	56C9493E	A0D59681	621C8B22

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – Sparc, OC – Oracle Solaris

11 та вище

libgopard.a	1D5D45F9	3B9B528E	EE227E8B	482AADCA	4B543B7D	768D61A0	D6015D05	BEDCDF6C
libasn1.a	EA07FB6A	52641646	61B74A30	533137BE	F3EE71E5	D03509BA	0B46C6E3	0AF7E890
libpkix.a	F175E6E4	A1CDD0D2	F3106CB8	98CB47AA	853EC246	D5B431CB	0C374372	D52CA2B8

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – Sparc-64, OC – Oracle

Solaris 11 та вище

libgopard.a	5188D25D	FED631EE	19CD160E	ED0379A9	900A65A1	69973FAR	R18F9F38	84D1B3C6
libasn1.a	2D6E78B0	DB46294B	F03066DB	2453E9D0	A08D1C7D	772DD5E8	05A28A24	B41B2CFB
libpkix.a	362C9575	851B02B9	BA4F6FBD	6D59FDD0	68327758	FAB58C19	9ED6E4A4	A9CB6541

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – IA64, OC – Hewlett-

Packard HP-UX 11 та вище

libgopard.a	D500A4B7	64529650	2A7AB47E	7BCB7CD3	AC928ABF	F9523429	8DC5CAAE	FC0E4F7B
libasn1.a	7744DE23	6FAB17BC	E0A31FE6	05D3B8B9	588F2DF0	71D70CE3	0BDEE76A	FA25078F
libpkix.a	F379F7A2	28975D27	5B00CAA4	FD2C6537	CC8F44FF	80D8BC86	0FC1EB03	91479C04

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – IA64, OC – Linux 2.6 та

вище

libgopard.a	67E8641D	623E8DF5	EBF665DC	6470780E	CC839211	E5E88F60	DE7A5AB1	2DF6CCB9
libasn1.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, OC – Microsoft

Windows XP та вище

gopard.lib	6621F6A0	30F23BA2	EPD85128	40E790AA	CB394868	6A7A9531	1C8E9E7F	0679B55E
asn1.lib	13D497EF	C3262640	D5511D93	07FC1334	06A97037	918290D8	13DAD0F0	18DA592C
pkix.lib	5876BB79	E593DE0E	880CFC69	FF66E1BA	D85EC1E7	D61B9972	22228FAE	EF5B10F8

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – ARMv7, OC – Google

Android 3.1 та вище

libgopard.a	185B06BB	B58E2FA6	1A55008C	1E1910A4	E275096B	8B3E8688	1A9A3B42	8A0165D1
libasn1.a	4AD4AADA	C8304BAE	54FE8437	4A26A712	703C5776	26A14E8D	09FEB787	6E5D611A
libpkix.a	94350B32	18961797	26F05542	FKD84CF0	98925D92	EC8C3FA7	CB2B96CF	D8AF0FC3

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – ARMv7a, OC – Google

Android 3.1 та вище

libgopard.a	424C917D	396C2F3E	34CD41B7	AKB938B8	46C98D86	6744A33F	9B7B04AD	A0E87F32
libasn1.a	6F26659B	18B9AB6F	4552B820	EC8F1E15	4922BF46	F39C0F06	BC06C0F9	12BAEBE8
libpkix.a	F7F6AB77	1A5D81A0	748B3826	3D9A40DD	980E1856	FF21C054	1DE5BC31	1474AA49

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – ARMv7, ARMv7a, ARM8;

OC – Apple iOS 4 та вище

libgopard.a	AB5062E3	E3E586BA	5A5CC5B6	7478B2A9	EPD65E50	E56870CD	F4A3FA31	7C62C3A8
libasn1.a	EAF4E92E	6EF79D25	9C902D70	2FDD6FED	7E0C78D9	03AAA4FC	5172118F	E51C4D1F
libpkix.a	A17A17E8	ED04FBAE	8B7239BC	37E67F9A	1241.6923	3D04EF03	FF705A74	2216D2F6

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – MIPS, OC – Google

Android 3.1 та вище

libgopard.a	CA4D9362	E310A0F1	6AD40788	93E1F0AC	89CB145F	D3053405	B0B08339	C7D2862D
libasn1.a	B8983FAF	EAF296A5	0019FE87	255307B0	CD4CB5A3	19FBEA57	83745542	97987650
libpkix.a	46F885D7	C43A5576	B8993C18	100356A5	C77902CE	F328A10A	29378B65	B5FEB1E5

Комплект бібліотек Java-реалізації Виробу

gopard-2.9.0.jar	18346423	963B2F36	3C05426C	F960CA91	659A6A90	B8ADA85C	61C66AD7	A2EB4B33
gopard-android-2.9.0.jar	5A06C8AF	0E0XF9F7	BF7544A7	CEDD6D71	86CE9B0A	B1D6620C	1001202A	5FE30661
pkix-1.25.1.jar	F44ED980	57234051	688956C5	D10CE0C7	E885-9886	886ADA93	FFA1DDC9	93EB7453
asn1-1.8.0.jar	ABCB18EC	8DD3A12C	7F0E686C	ABBE8053	2065439A	03263D42	B2798F48	9F3AD863
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
alf4j-android-1.6.1-RC1.jar	6781D455	37DB541F	BFAF550E	4D9CEC98	C01B7602	C16229A0	75A97660	5B6884CD

elf4j-api-1.7.5.jar
elf4j-log4j2-1.7.5.jar

C3FB3F74 41D2CF91 0320CBDA 697B9C70 016A129C DD0E6CAA 86B6A846 E1CE9413
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 30.11.2019.

Перший заступник Голови Служби

О.М. Чаузов





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@dsszri.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-PKCS1-v1_5, RSASSA-PKCS1-v1_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-Гельмана 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	
Комплекти бібліотек для апаратно-програмних платформ з архітектурою процесора - x86, ОС - Microsoft Windows XP та вище	
gwpard.lib	2642993A 802E8D69 CDB10088 BC9EE6FF 5B5B5124 BDCD28F0 59119709 736DB284
asnl.lib	803BEEC0 55A99077 8D9FF681 C4CFC156 1CA989CD 7A981C9F D9294DD8 BA89050D
pkix.lib	49790E1E 33AA4D27 41AB6F2A 2BD1DDDD F702793E 636901D6 4897E83E 762F72BA
Комплекти бібліотек для апаратно-програмних платформ з архітектурою процесора - x86, ОС - Linux 2.6 та вище	
libgwpard.a	1E50A606 B843C5C9 BE89D258 290EC95B 953876DB E3B8296C 9079AE5C 79992E47
libasnl.a	4F2D5875 59CC5A7E 9F296D32 40EF1C43 E4171F01 E3B8FAP1 D2567909 BAA8B81E
libpkix.a	334B6103 730E0B6D D0B12E2A 261BF08B 07ECCB8E 859DC41A 6EF10660 40A0552C
Комплекти бібліотек для апаратно-програмних платформ з архітектурою процесора - x86, ОС - Apple MacOS X 10.6 та вище	
libgwpard.a	75FEDE84 FA45078C A7134A77 D45596B2 9B6FDA13 AEE2B1E0 2E15BDB6 ARC7CBFC
libasnl.a	6F7F0AD7 F435553E C8ED35AF 5635CFE9 12ADDA47 E9F4BBAE CC249749 115BF687
libpkix.a	0509B127 455B03B7 5DF6984D A0AA22F7 75796A63 F3685E08 EE397BDC F1257E5B
Комплекти бібліотек для апаратно-програмних платформ з архітектурою процесора - x86, ОС - Oracle Solaris 11 та вище	
libgwpard.a	AD45BACE C3D7290E DA0FACB2 656CD87C C38431ED C7300782 F13D4D5E B0E6C950
libasnl.a	329D09A0 F2862A7F EBF62A49 2D900E43 459816B1 1B8E57B5 97145E7D B79AA05D
libpkix.a	F5011BFB E3AD7A65 271157D6 CAE16FE7 C26E3EF1 7CE00BA6 66943667 02B17304
Комплекти бібліотек для апаратно-програмних платформ з архітектурою процесора - x86, ОС - Google Android 3.1 та вище	
libgwpard.a	D3DE00B5 D4C0E61F 2BC3ECF0 55557E61 7FA531E4 2024E453 1E770A78 0B8BA054
libasnl.a	808C7949 ECD8E654 57D5C623 546FE25C 074F7D13 E2910E44 EBA81A50 883D16BD
libpkix.a	0B428A8D 48CE9381 22030708 CB72BA56 2EAB5AE8 1B99DFDC 0CB076A6 58D13669
Комплекти бібліотек для апаратно-програмних платформ з архітектурою процесора - x86-64, ОС - Microsoft Windows XP та вище	
gwpard.lib	98E0C360 E1C31813 A908223D 1ED7E0DA B583443B C4D31005 43962E8D 6E8971F1
asnl.lib	0F19DB27 A94C000D 32F211B2 5258A79B 3FB48334 1DB46EBC 55B6A592 703125E2
pkix.lib	550D6838 0BA8E779 302B59A9 1679E242 50C8255D EC5529A6 FE9873E8 B7910766
Комплекти бібліотек для апаратно-програмних платформ з архітектурою процесора - x86-64, ОС - Linux 2.6 та вище	
libgwpard.a	228FC188 78EE907E 74AFA98A 69CEC9BD 92110E46 82D6989D 1BEC9603 46C71602
libasnl.a	6161340A A0456AF0 4873A515 C20EBC45 EA4CFD8E B7574D0F 1D46DBF2 DBED05AF
libpkix.a	FA3E07BF E5767764 31DF0501 C6A8EFC5 F27D3D20 56F2CB10 E733C723 ED20CEDE
Комплекти бібліотек для апаратно-програмних платформ з архітектурою процесора - x86-64, ОС - Apple MacOS X 10.6 та вище	
libgwpard.a	94BFC386 2D65A35E 9F104591 17A6DE86 A3CB6DC0 B0E31CA0 4DB74C7E 5D331FA9
libasnl.a	66DB3357 7FA614AE 99A4AC02 5F5C222E 406296C8 165E5FF5 20FEAD6E 73CE7502
libpkix.a	67250A17 D93F5D3F 3C4549B1 C77F21C0 54D1488A 35CAE723 B75BA0C1 FA2E60D6
Комплекти бібліотек для апаратно-програмних платформ з архітектурою процесора - x86-64, ОС - FreeBSD 9 та вище	
libgwpard.a	117C7F52 8398B8AA FCF4B5EE 636E0568 C2A30AA5 7C2E71A9 D817D798 549CAE15
libasnl.a	DEDA13C6 69E0BA96 6DA3F980 30F4601E 1B9D9879 55D4EFC1 98458392 D4D7987B
libpkix.a	5009CBDC C5F0A958 22A7F827 7A2E8A5A 011AD2F1 4752647F A17838D3 B885C937
Комплекти бібліотек для апаратно-програмних платформ з архітектурою процесора - PowerPC, ОС - IBM AIX 5.2 та вище	
libgwpard.a	4168C180 AD152032 11695074 CC1DF643 50EFD8E6 10A5D170 E1994DF5 9E5C0CAB
libasnl.a	C32F0352 319E8C14 F53DACC9 08C2CF69 E0CF5A1C D7FB608E 6835CF52 441ED586
libpkix.a	A987CF27 2F24074E E61AF134 494385B0 B3BF64DD DF3DB795 6942337C 6D99BE4F
Комплекти бібліотек для апаратно-програмних платформ з архітектурою процесора - PowerPC, ОС - Linux 2.6 та вище	
libgwpard.a	1C527E24 684FCFA5 446B03E7 80F510A3 F0A7F5DA 145FF4CF C47ED639 52207763
libasnl.a	1C53B4A3 17053450 2AD9941C 74E18D2C B7ED4E48 15107854 09FEA722 0950BA53
libpkix.a	A8E522A9 54B74E4C 7E051C54 42AE517E 01960DA2 A3604EAB E71543ED 5C3AD4D5
Комплекти бібліотек для апаратно-програмних платформ з архітектурою процесора - PowerPC-64, ОС - IBM AIX 5.2 та вище	
libgwpard.a	08EE11CB 99A8E80B 3AA76062 20975518 60869D36 5CD32A01 E1931978 D904D063
libasnl.a	39B8BC61 FAFCT60C 293B55A1 D8348558 3105449F 02492547 43F51D66 04D5E272
libpkix.a	4C642BFB 15C74850 B0C21161 AD221EFO 9CE65737 93BACF63 96FE3EAB FF383629
Комплекти бібліотек для апаратно-програмних платформ з архітектурою процесора - PowerPC-64, ОС - Linux 2.6 та вище	
libgwpard.a	3486694E CD24E30B B01BD3DA B4B51857 2D146E3D F0050C8D B1B05352 0C6304BE
libasnl.a	B377A6DC FE5FA484 A3C74E61 E25A3261 D64F5B87 784786CD 66C57C12 69827E34
libpkix.a	F7095B2F 56C386E5 6DF91B34 6354E415 F6914C52 56C9493E A0D59681 621C8B22
Комплекти бібліотек для апаратно-програмних платформ з архітектурою процесора - Sparc, ОС - Oracle Solaris 11 та вище	
libgwpard.a	1D5D45F9 2B9B528E EE227E8D 482AADCA 4B543B7D 768D61AD D6015D05 BBDCEFC6
libasnl.a	EAD7FB6A 52641646 61B74A30 533137BE F3EE71E5 D03509BA 0B46C6B3 0AF7E890
libpkix.a	F175E6E4 A1CD08D2 FC106CB8 9DCB47AA B53EC246 D5B431CB 0C374372 D52CA2BF
Комплекти бібліотек для апаратно-програмних платформ з архітектурою процесора - Sparc-64, ОС - Oracle Solaris 11 та вище	
libgwpard.a	5188D25D F80631EE 19CD160E ED0379A9 200865A1 59973FAB B18DF32B D4D1B3C6
libasnl.a	2D6E78B0 DB46294B FD3066DB 2453EFD0 A0BD1C7D 772DD5B8 05A28A24 B41B2CFB
libpkix.a	362C9575 851B02B9 BA4F6FED 6D59FD08 68327758 FAD58C19 9ED6E4A4 A9CB6541

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора - IA64, ОС - Hewlett-Packard HP-UX 11 та вище	
libgwpard.a	D500A4B7 64529650 2A7A847E 7BCB7CD3 AC928ABF F9523429 8DC5CAAE F0BE4F7B
libaaml.a	7744DE23 6FAD17BC E0A31FE6 05D3BBD9 588F2DF0 71D70CE3 0BDEE76A FA25078F
libpkix.a	F379F7A2 28975D27 5B00CAAA F02C6537 C8BF44FF 800DC06 0FC1E0D3 91479C04
Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора - IA64, ОС - Linux 2.6 та вище	
libgwpard.a	67E8641D 623EEDF5 EBF665DC 6470780E CC839211 E5E88F00 DE7A5AB1 2DF6CCB9
libaaml.a	2CD215F4 E2CF10FD 9937C038 7176F08 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	
gwpard.lib	6621F6A0 30F23BA2 EFD05128 40E790AA CB394868 6A7A9531 1C8E9E7F 0679D55E
aaml.lib	13D497EF C3262640 D5511D93 07FC1334 06A97037 918290DB 13DAD0F0 1DDA592C
pkix.lib	5876B079 E593CE0 880CFC69 FF66E1DA D85E1E7 D61B9972 22228FAE EF5B10F0
Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора - ARMv7, ОС - Google Android 3.1 та вище	
libgwpard.a	105D06ED B58E2FA6 1A55008C 1E1910A6 E275096B 8B3E8688 1A9A3B42 8A0165D1
libaaml.a	4A04AADA C8304DAE 54FE8437 4A26A712 703C5776 26A148BD 09FED787 6E5D611A
libpkix.a	94350B32 1B961797 26FD5542 FEE84CF0 98925D92 EC0C3FA7 CB2D96CF D6AF0FC3
Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора - ARMv7a, ОС - Google Android 3.1 та вище	
libgwpard.a	424C917D 396CF3E8 34CD41B7 AED93EED 46C9ED86 8744A33F 9B7BD4AD A5EE7F32
libaaml.a	6F26659D 1B99A86F 4552B820 E0BF1E15 4922BF46 F39C0F06 B0C4C0F9 12DAE8E8
libpkix.a	F7F6AD77 1A5081A0 74BD3826 3D9A40CD 9B0E1856 FF21C054 1DE5DC31 1474AA49
Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора - ARMv7, ARM8, ОС - Apple iOS 4 та вище	
libgwpard.a	AB5062E3 E3E586BA 5A5CC5D6 7478D2A9 EFD65E50 E56870CD F4A37A31 7C6D23A8
libaaml.a	BAF4E92E 6EF79025 9C8D2D70 2FDD6FED 780C75D9 03AAA4FC 5172118F E51C4D1F
libpkix.a	A17A17E8 ED04F8AE 807239DC 37E67F9A 12416923 3D04EFD3 FF705A74 2216D2F6
Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора - MIPS, ОС - Google Android 3.1 та вище	
libgwpard.a	CA4D9362 E310A071 6AD40788 93E1F0AC 89CB145F D3053405 BDB08339 C7D2862D
libaaml.a	B8903FAF EAF296A5 0019FE87 255307B0 CD4C85A3 19FEEA57 83745542 97987650
libpkix.a	46F085D7 C43A2576 D8993C18 100356A5 C77902CE F328A10A 29378B65 B5FED1E5
Комплект бібліотек Java-реалізації Виробу	
gwpard-2.9.0.jar	18346423 943B2F36 3C05426C F960CA91 659A6A90 B8ADAB5C 61C66AD7 A2ED4B33
gwpard-android-2.9.0.jar	5A06C8AF 0E0EF9F7 BFF544A7 C8E06D71 86CE9B0A B1D6620C 1001202A 5FE30661
pkix-1.25.1.jar	F44ED980 57234051 68B956C5 D10C80C7 B8B59886 886ADA93 FFA1DC09 93EB7453
aaml-1.8.0.jar	ADCB1B8C 8DD3A12C 7F0E686C ADBE8053 2065439A 03263D42 B2798F48 9F3AD063
log4j-1.2.17.jar	D6A4F46A B79E90E8 1E01F990 B8E40052 93B87B2A F20AFB0A 7F63F30F 89AF09C8
pkix-crypto-1.2.0.jar	9FC96647 0B3FA2ED 11DE56A9 FDDA0F62 9463A03A E4CF1FA3 A112AA32 1DF33DC6
slf4j-android-1.6.1-RC1.jar	6781D455 37DB541F BFAF550E 40BC8C98 C01B7602 C16229AD 75A97660 5B6804CD
slf4j-api-1.7.5.jar	C3FB3F74 41D2CF91 0320C8DA 697B8C70 016A129C D00E6CAA 88D6A246 E1CE9413
slf4j-log4j12-1.7.5.jar	0206B809 F53113D5 B09247D7 6874E425 20E81BC8 2E18E8A7 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



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

02.08.2019 № 04/03/02-2099

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 02.08.2019

м. Київ

Виданий: Товариству з обмеженою відповідальністю «ДБО Софт» (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 31.07.2019 № 416.

Об'єкт експертизи: Програмний виріб криптографічного захисту інформації «Гепард 2.0» UA.37619243.00004-01 90 01-1.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю «ДБО Софт» (код ЄДРПОУ 37619243).

Експертний заклад: Товариство з обмеженою відповідальністю «Безпека та інновації інформаційних систем» (код ЄДРПОУ 41449076).

Висновки:

1. В об'єкті експертизи правильно реалізовано криптографічний алгоритм, визначений ДСТУ ГОСТ 28147:2009 (у режимі простої заміни, гамування, гамування зі зворотним зв'язком, вироблення імітовставки).
2. В об'єкті експертизи правильно реалізовано криптографічний алгоритм, визначений ДСТУ 7624:2014 (у режимах простої заміни, гамування, гамування зі зворотним зв'язком за шифротекстом, вироблення імітовставки, зчеплення шифроблоків, гамування зі зворотним зв'язком за шифрограмою, вибіркове гамування із прискореним виробленням імітовставки, вироблення імітовставки і гамування, індексованої заміни, захисту ключових даних).
3. В об'єкті експертизи правильно реалізовано криптографічний алгоритм TDEA, визначений ДСТУ ISO/IEC 18033-3:2015 (у режимах згідно ДСТУ ISO/IEC 10116:2014).
4. В об'єкті експертизи правильно реалізовано криптографічний алгоритм AES, визначений ДСТУ ISO/IEC 18033-3:2015 (у режимах згідно ДСТУ ISO/IEC 10116:2014).
5. В об'єкті експертизи правильно реалізовано алгоритм гешування, визначений ГОСТ 34.311-95.
6. В об'єкті експертизи правильно реалізовано алгоритм гешування, визначений ДСТУ 7564:2014 (у режимах Купина-256, Купина-384, Купина-512).
7. В об'єкті експертизи правильно реалізовано алгоритм гешування SHA-1, визначений ДСТУ ISO/IEC 10118-3:2005.
8. В об'єкті експертизи правильно реалізовано алгоритми гешування SHA-256, SHA-384, SHA-512, визначені ДСТУ ISO/IEC 10118-3:2005, та SHA-224, визначений FIPS PUB 180-4.
9. В об'єкті експертизи правильно реалізовано алгоритми гешування SHA3-224, SHA3-256, SHA3-384, SHA3-512, визначені ISO/IEC 10118-3:2018.
10. В об'єкті експертизи правильно реалізовано обчислення коду автентифікації повідомлень HMAC, визначеного IETF RFC-2104.

11. В об'єкті експертизи правильно реалізовано обчислення коду автентифікації повідомлень відповідно до ДСТУ 7564:2014 (у режимах Купина-256, Купина-384, Купина-512).
12. В об'єкті експертизи правильно реалізовано алгоритми RSAES-OAEP, RSAES-PKCS1-v1_5, визначені PKCS#1.
13. В об'єкті експертизи правильно реалізовано алгоритм обчислення та перевіряння електронного підпису, генерацію випадкових двійкових послідовностей, обчислення ключів електронного підпису, визначені ДСТУ 4145-2002 (у поліноміальному та оптимальному нормальному базисах з довжиною ключа 163 – 509 біт).
14. В об'єкті експертизи правильно реалізовано алгоритми обчислення та перевіряння електронного підпису DSA, ECDSA, визначені ДСТУ ISO/IEC 14888-3:2015.
15. В об'єкті експертизи правильно реалізовано алгоритм обчислення та перевіряння електронного підпису, визначений PKCS#1 v2.1 «RSA Cryptography Standart» (за схемою RSASSA-PKCS1-v1_5).
16. В об'єкті експертизи обчислення спільного секрету за схемою Діффі-Геллмана реалізовано відповідно до ДСТУ ISO/IEC 15946-3:2006 та наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 18.12.2012 № 739 «Про затвердження вимог до форматів криптографічних повідомлень», зареєстрованого в Міністерстві юстиції України 14.01.2013 за № 108/22640.
17. Формат посиленних сертифікатів, структури об'єктних ідентифікаторів криптографічних алгоритмів, що є державними стандартами, формат списків відкликаних сертифікатів, формат підписаних даних, протокол фіксування часу, протокол визначення статусу сертифікату 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 в Міністерстві юстиції України 20.08.2012 за № 1398/21710.
18. Формат посиленних сертифікатів шифрування та формат криптографічних повідомлень 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 в Міністерстві юстиції України 14.01.2013 за № 108/22640.

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:

Комплекти бібліотек ANSI C-реалізації Виробу

Комплект бібліотек для апаратно-програмних платформ архітектурою процесора – x86, ОС – Microsoft Windows XP та вище

gopard.lib	6DB24F44 B5352FD1 F2108547 A32DE058 3E6C730C 6528F17D 42A63FB5 36506600
asn1-module.lib	4FE7CC16 A6B7C6B0 3BFFC0BC B9BF912E D1FBFCBF 31DAA17B 02E3414A 7FE1E6C7
pkix-module.lib	1C9E074A 28C0509A CA351897 DCD38021 3943CA7F 2431BB13 F9ECDFE4 EED68A37

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – x86, ОС – Linux 3.0 та вище

libgopard.a	9CA38523 1246AC1A BB4C714F 6B9F246C 8E80D4C3 A41E629A FE479C21 33AEA408
libasn1-module.a	7065F3FD B227A637 81A6E80A 71A652AE 823561D2 B4B093B3 E2AFC68C BEA363DA
libpkix-module.a	FF4E66B4 D558BE47 A211F7C7 6D6AA673 506045F0 D52E0F13 92409A72 6D9173F1

Комплект бібліотек для апаратно-програмних платформ архітектурою процесора – x86, ОС – Apple MacOS X 10.6 та вище

libgopard.a	7645A893 A2B58BD8 97623332 5E83535A EA1DD268 E554C0E8 187E101B 19AEADD4
libasn1-module.a	F5D3439D AA39638A 357CC065 E67B9160 0519E9C6 42C0BCD2 2479C98C 8BD2A3B3
libpkix-module.a	BA32AEA0 DD11C940 1C3A1161 D597BDA8 877395D9 4528CD95 F89174AB 63C02C13

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – x86, ОС – Google Android 4.4 та вище

libgopard.a	C2BBD8B5 43F7FFB0 8FA7D85E 625CCD26 74986C8C D4320238 CF61CB72 EE5AD0A6
libasn1-module.a	79B68442 96BC0D4B BEF94F73 3D2C7D32 FF6BA86D E58C54F7 6DB19E4B 64CCFDE8
libpkix-module.a	CFE248CD F9E58142 1CA78B4B 535D4AF2 E4E9D3FC ED6FC799 EC017B7C F32E9B61

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – x86-64, ОС – Microsoft Windows XP та вище

gepard.lib	6DB4B0BA 9967FAF5 A40A7B37 BDA48DCF 9E5C7125 9548673E 32A11194 C83B76F2
asn1-module.lib	3FCE0E44 75C365E8 538E89E9 9FF1F23D 98C36F16 E80EFE94 805D1708 03BEB814
pkix-module.lib	AA7E0073 1418A150 D07F9267 7CD1DA42 1664ED84 E4CFF723 3EF2A93F 9D54FDFD

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – x86-64, ОС – Linux 3.0 та вище

libgepard.a	C6B3C983 82681381 F5C10E15 DBCE5C89 99BD3DE0 89D17A2A D0564FF5 1CBEBB67
libasn1-module.a	A2734E48 48CB28BE B0020115 0121DA86 681E1B85 AB710098 180136CC 4784F571
libpkix-module.a	77223DFE 32BA116D 8080F00 C5EFC04E BF8FC141 D0CAAB0C 93C5C609 6E9E87CC

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – x86-64, ОС – Apple MacOS X 10.6 та вище

libgepard.a	7645A893 A2B58BD8 97623332 5E83535A EA1DD268 E554C0E8 187E101B 19AEADD4
libasn1-module.a	F5D3439D AA39638A 357CC065 E67B9160 0519E9C6 42C0BCD2 2479C98C 8BD2A3B3
libpkix-module.a	BA32AEA0 DD11C940 1C3A1161 D597BDA8 877395D9 4528CD95 F89174AB 63C02C13

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – x86-64, ОС – Google Android 4.4 та вище

libgepard.a	43933759 4B8A69D5 FB52CB5C 8F57D0DC 559E1A26 B38F698B 98B265C6 2F192850
libasn1-module.a	8A53A519 8C68B5AD F408EF20 DD2B4C9A 7F6D4C16 3FFC2F1D 05647485 0B380805
libpkix-module.a	0C37B757 EBA9BF2E 34FA241A 1F5B165E DBE9BB9A 3B7A7A0F E58327EB 70B981F9

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – ARM v7a, ОС – Google Android 4.4 та вище

libgepard.a	71A025CB 4822A9E9 140B0A70 A9FEB2E6 A5BDAF7C 6EBF204F 02BBB00B 5BD9394B
libasn1-module.a	72915AA2 B0F642C8 D9171093 180DF74D AD7414C3 BDA8CABF 90EF6DCB F2C014BB
libpkix-module.a	B3DF8AF6A 8EDB4834 C0710C1E 74E167C8 3FAF61FE 248797DD 6DBEDF76 BCBC4F2E

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – ARM v8a, ОС – Google Android 4.4 та вище

libgepard.a	A4A739DE CDD61A3 C61BB8A8 41B6E3BE 04B6C3E9 B6765D21 180077DA 68EE591A
libasn1-module.a	8200EF6E 9DD02F93 3D9315E0 AFC6C04A 33A90302 38213D43 4BFC7C0A 21692670
libpkix-module.a	B4D66C87 7F5B82B2 4FCA50D6 9A6BB849 939EF462 72125344 B1C005FA 49352533

Комплект бібліотек для апаратно-програмних платформ з архітектурою процесора – ARM; ОС – Apple iOS 4 та вище

libgepard.a	8B792E1E 9955D102 77194F2F 7A0CD8A3 0EF5DE96 68B33567 17DA58C7 92438ED4
libasn1-module.a	18202072 B286E5C0 70C74F71 49737024 457710FB 93F848FD 15055B98 463FD911
libpkix-module.a*	84049A1E A8905900 42B3F130 0025BE81 9D3BA403 DB193A2B 7620F91B 16B1B52E

Комплект бібліотек Java-реалізації Виробу

gepard-2.14.2.jar	D4100849 31FB3442 787936DF E095661D CC9FF47D 1D9A682A D9DCBADE D31A86CB
gepard-android-2.14.2.jar	436DF528 1AD8FE1B 98C30AE9 CA91E568 1C743DDA 21FA6739 27427497 67554CE6
asn1-1.9.5.jar	D1502B4F 5606C44C 75D1E271 A478DC0D 06F5F38E BD2C5728 F437FB98 2EB30D88
pkix-1.39.1.jar	E380D546 B9C27637 032CED22 67E77664 78D1F839 B58092C3 06B585A5 BC9065B6
proguard4.8.jar	7E855A39 2F83CE88 00211C62 6BC8F5DC 01D4BA6B D7BAE035 E4D58634 746BD3C1

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 31.07.2024.

Голова Служби



Л. О. Євдоченко