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

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 шифрогамою, 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 посилених 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 посилених 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 зархітектурою процесора – x86, ОС – Microsoft Windows XP та вище

```
gepard.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

```
libgepard.a         9CA38523 1246AC1A BE4C714F 6B9F246C 8E80D4C3 A41E629A FE479C21 33AEA408
libasn1-module.a    7065F3FD B227A637 81A6EB0A 71A652AE 823561D2 B4B093B3 E2AFC68C BEA363DA
libpkix-module.a    FF4E66B4 D558BE47 A211F7C7 6D6AA673 506045F0 D52E0F13 92409A72 6D9173F1
```

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

```
libgepard.a         C2BBDBB5 43F7FFB0 8FA7D85E 625CCD26 74986CEC D4320238 CF61CB72 EE5AD0A6
libasn1-module.a    79B68442 96BC0D4B BEF94F73 3D2C7D32 FF6BA86D E58C54F7 6DB19E4B 84CCFDE8
libpkix-module.a    CFE248CD F9E58142 1CA7BB4B 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 75C365EB 538E89E9 9FF1F23D 98C36F16 EB0EFE94 805D1708 03BEB814
pkix-module.lib	AA7E0073 1418A150 D07F9267 7CD1DA42 1664ED84 E4CFFF23 3EF2A93F 9D54FDFD

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

libgepard.a	C6B3C983 826813B1 F5C10E15 DBCE5C89 99BD3DE0 89D17A2A D0564FF5 1CBEBB67
libasn1-module.a	A2734E48 48CB28BE B0020115 0121DA86 681E1B85 AB710098 180136CC 4784F571
libpkix-module.a	77223DFE 32BA116D 8DEDEF00 C5EFC04E BF8FC141 00CAAB0C 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 7DB981F9

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 BDA80ABF 90EF6DCB F2C014BB
libpkix-module.a	B3DFAF6A 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 CDDE61A3 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 15055B9E 463FD911
libpkix-module.a*	84049A1E A8905900 42E3F130 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 2EE30DB8
pkix-1.39.1.jar	E380D546 B9C27637 032CED22 87E77664 7801F839 B58092C3 06B585A5 BC9065B6
proguard4.8.jar	7E855A39 2F83EC88 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