Прим. № 1

АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ
(АДМІНІСТРАЦІЯ ДЕРЖСПЕЦЗВ'ЯЗКУ)

вул. Солом'янська, 13, м. Київ, 03110, тел. (044) 281-93-08, факс: (044) 281-94-83,
e-mail: info@cip.gov.ua, сайт: www.cip.gov.ua, код згідно з ЄДРПОУ 34620942

12.09.2024 № 04/04/02-15077/ВН На № _____ від _____

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 12.09.2024 м. Київ

Виданий: Товариству з обмеженою відповідальністю «САЙФЕР ПРО» (код ЄДРПОУ 42125815)

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 03.09.2024 № 622.

Об'єкт експертизи: Програмний комплекс криптографічних перетворень «Шифр-JCSP Extender» версії 1.0 ТЗ У 72.2-42125815-006:2024.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю «САЙФЕР ПРО» (код ЄДРПОУ 42125815).

Експертний заклад: Товариство із обмеженою відповідальністю «ЗАХИСТ.ЮЕЙ» (код ЄДРПОУ 42292899).

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), ДСТУ 8845:2019, ДСТУ 9041:2020, ДСТУ ГОСТ 28147:2009 (у режимах простої заміни, гамування, гамування зі зворотним зв'язком та обчислення імітовставки), ГОСТ 34.311-95, ДСТУ 4145-2002 (у поліноміальному базисі).
2. В об'єкті експертизи алгоритми генерації випадкових двійкових послідовностей відповідають додатку А ДСТУ 4145-2002, NIST SP 800-90A rev.1, Intel Digital Random Number Generator (DRNG): Software Implementation Guide, Revision 1.1.
3. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування TDEA, визначений ДСТУ ISO/IEC 18033-3:2015 (у режимах ECB, OFB, CFB, CBC, CTR, CMAC, визначених ДСТУ ISO/IEC 10116:2019).
4. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування AES, визначений ДСТУ ISO/IEC 18033-3:2015 (у режимах ECB, OFB, CFB, CBC, CTR, CMAC, визначених ДСТУ ISO/IEC 10116:2019, у режимі CCM, визначеному NIST FIPS 800-38C, у режимі GCM, визначеному NIST FIPS 800-38D).
5. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування RC2, визначений IETF RFC 2268 (у режимах ECB, OFB, CFB, CBC, CTR, CMAC, визначених ДСТУ ISO/IEC 10116:2019).

6. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування RC4, визначений IETF RFC 7292.
7. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування RC5, визначений IETF RFC 2040 (у режимах ECB, OFB, CFB, CBC, CTR, CMAC, визначених ДСТУ ISO/IEC 10116:2019).
8. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування ChaCha20, визначений IETF RFC 8435 (у режимі AEAD_ChaCha20_Poly1305).
9. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування RSA, визначений ДСТУ ISO/IEC 18033-2:2015.
10. В об'єкті експертизи правильно реалізовано криптографічні алгоритми формування та перевіряння електронного підпису ECDSA, EC-GDSA, визначені ДСТУ ISO/IEC 14888-3:2019.
11. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного підпису RSA, визначений ДСТУ ISO/IEC 14888-2:2015 (у режимах роботи RSA1S, RSA2S).
12. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного підпису EdDSA, визначений IETF RFC 8032, NIST FIPS 186-5:2023.
13. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-1, SHA-256, SHA-384, SHA-512, SHA-3, визначені ДСТУ ISO/IEC 10118-3:2023.
14. В об'єкті експертизи правильно реалізовано алгоритми вироблення ключа шифрування на основі спільного секрету KDF1, KDF2, KDF3, визначені ДСТУ ISO/IEC 18033-2:2015.
15. В об'єкті експертизи правильно реалізовано алгоритми вироблення ключа шифрування на основі паролю PBKDF1, PBKDF2, PBKDF2-PFX, визначені IETF RFC 2898.
16. В об'єкті експертизи правильно реалізовано алгоритм шифрування на основі паролю PBES2, визначений IETF RFC 2898.
17. В об'єкті експертизи правильно реалізовано алгоритм обчислення коду автентифікації на основі паролю PBMAC1, визначений IETF RFC 2898.
18. В об'єкті експертизи правильно реалізовано криптографічні протоколи розподілу ключів ECKAS-DH1 (KANIDH, ECDH), ECKAS-DH2 (KADH2KP, KADH2SKC), ECKAS-MQV1 (KAMQV1P), ECKAS-MQV2 (KAMQV2P), ECKAS-EG (KAEG), визначені ДСТУ ISO/IEC 11770-3:2015, EdCKAS-DH, визначений IETF RFC 7748.
19. В об'єкті експертизи правильно реалізовано алгоритми обчислення коду автентифікації повідомлення з використанням криптографічних алгоритмів: шифрування ДСТУ ГОСТ 28147:2009, ДСТУ 7624:2014, AES, TDEA, RC2, RC5; гешування ДСТУ 7564:2014, ГОСТ 34.311-95, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256, визначених IETF RFC 2104; SHA-3/224, SHA-3/256, SHA-3/384, SHA-3/512, SHAKE128, SHAKE256, визначених NIST PUB 202; Poly1305, визначеного IETF RFC 8435.
20. В об'єкті експертизи правильно реалізовано алгоритми кодування даних: EMSA1, EMSA2, визначені IEEE P1363-2000; EMSA3, EMSA4, визначені IEEE P1363-2000; EMSR1, визначений IEEE P1363-2000, ISO/IEC 9796:1991; EMSR3, визначений IEEE P1363a-2004; EME1, EME2, визначений IEEE P1363-2000; EME-ДСТУ 9041:2020, визначений ДСТУ 9041:2020.
21. В об'єкті експертизи правильно реалізовано формат підписаних даних (у форматі XAdES), визначений ДСТУ ETSI EN 319 132-1:2016 та ДСТУ ETSI EN 319 132-2:2016.
22. В об'єкті експертизи правильно реалізовано формат підписаних даних (у форматі CAdES), визначений ДСТУ ETSI EN 319 162-1:2016, ДСТУ ETSI EN 319 162-2:2016.
23. В об'єкті експертизи правильно реалізовано формат підписаних даних (у контейнері ASiC-E), визначений ДСТУ ETSI EN 319 122-1:2016 та ДСТУ ETSI EN 319 122-2:2016.
24. В об'єкті експертизи правильно реалізовано формати позначки часу та запиту на її формування, визначені ДСТУ ETSI EN 319 422:2016.

25. В об'єкті експертизи правильно реалізовано формати запиту та відповіді про статус сертифікату, визначені IETF RFC 6960.
26. В об'єкті експертизи правильно реалізовано формати сертифікатів відкритих ключів, визначені ДСТУ ETSI EN 319 412-1:2016, ДСТУ ETSI EN 319 412-2:2016, ДСТУ ETSI EN 319 412-3:2016, ДСТУ ETSI EN 319 412-4:2016.
27. В об'єкті експертизи правильно реалізовано формат ключових файлових контейнерів, визначений IETF RFC 7292.
28. В об'єкті експертизи алгоритм ініціалізації генераторів випадкових послідовностей відповідає вимогам документу «Методика ініціалізації генератора випадкових двійкових послідовностей UA.42125815.00006 – 01 93 01».
29. Об'єкт експертизи спільно із засобами криптографічного захисту інформації: ключ електронний «Secure Token-338» ТУ У 26.2-32248356-029:2020, карта мікропроцесорна «CryptoCard-338» ТУ У 26.2-32248356-030:2020, ключ електронний «Алмаз-1К» ЄААД.469535.153, криптомодуль мережний «ГРЯДА-301» ЄААД.469535.049, ЄААД.469535.240, ЄААД.469535.241, ЄААД.469535.243, криптомодуль мережний «Шифр-HSM» ТУ У 26.2-42125815-001:2020, що мають чинні експертні висновки за результатами державної експертизи в сфері криптографічного захисту інформації, може бути використаний в якості засобу кваліфікованого електронного підпису чи печатки для надання електронних довірчих послуг.
30. Методи захисту, реалізовані в об'єкті експертизи, відповідають вимогам до засобів криптографічного захисту інформації класу Б2 (захист від порушника першого та нульового рівнів), визначеним в Положенні про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженому наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141, зареєстрованим в Міністерстві юстиції України 30.07.2007 за № 862/14129.
31. Об'єкт експертизи відповідає вимогам п. 3 Вимог до засобів криптографічного захисту інформації, призначених для захисту таємної інформації, яка не становить державної таємниці, та конфіденційної інформації в державних органах, органах місцевого самоврядування, на підприємствах, в установах та організаціях, які належать до сфери їх управління, військових формуваннях, які створені відповідно до закону, затверджених наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 07.05.2021 № 278, зареєстрованим в Міністерстві юстиції України 26.05.2021 за № 696/36318.
32. Об'єкт експертизи відповідає вимогам технічного завдання ТЗ У 72.2-42125815-006:2024 в частині реалізації функцій криптографічних перетворень.
33. 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, виготовлені відповідно до технічних умов ТУ У 62.0-42125815-006:2024 із Сповіщенням 42125815.016-001:2024 про зміну № 1 до ТУ У 62.0-42125815-006:2024.

Термін дії експертного висновку – до 03.09.2029.

Голова Служби Юрій МИРОНЕНКО