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

29.12.2023 № 04/05/02-1192/ВС1 На № _____ від _____

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 29.12.2023 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 29.12.2023 № 600.

Об'єкт експертизи: Комплекс криптографічного захисту мережевих з'єднань програмний «Шифр-VPN» версії 2.

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

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

Висновки:

1. В об'єкті експертизи правильно реалізовано криптографічні алгоритми, визначені ДСТУ 7624:2014 (у режимах «Калина-128/128-CBC», «Калина-128/256-CBC», «Калина-256/256-CBC», «Калина-256/512-CBC», «Калина-512/512-CBC»), ДСТУ 7564:2014 (у режимах «Купина-256», «Купина-384», «Купина-512»), ДСТУ 8845:2019 (у режимах «Струмок-256», «Струмок-512»), ДСТУ 4145-2002, ДСТУ ГОСТ 28147:2009 (у режимі гамування зі зворотним зв'язком), ГОСТ 34.311-95.
2. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування AES, визначений ДСТУ ISO/IEC 18033-3:2015 (у режимі CBC, визначеному ДСТУ ISO/IEC 10116:2019, з довжиною ключа 128, 192 та 256 біт).
3. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування TDEA, визначений ДСТУ ISO/IEC 18033-3:2015 (у режимі CBC, визначеному ДСТУ ISO/IEC 10116:2019, з довжиною ключа 112 та 168 біт).
4. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування DES, визначений ДСТУ ISO/IEC 18033-3:2015 (у режимі CBC, визначеному ДСТУ ISO/IEC 10116:2019, з довжиною ключа 56 біт).
5. В об'єкті експертизи правильно реалізовано алгоритм формування та перевіряння електронного підпису RSA, визначений ДСТУ ISO/IEC 14888-2:2015.
6. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного підпису ECDSA, визначений ДСТУ ISO/IEC 14888-3:2019.
7. В об'єкті експертизи правильно реалізовано криптографічний протокол розподілу ключів Діффі-Гелмана в групі точок еліптичної кривої (ECDH), визначений ДСТУ ISO/IEC 11770-3:2023.

8. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-1, SHA-256, SHA-384, SHA-512, визначені ДСТУ ISO/IEC 10118-3:2023.
9. В об'єкті експертизи алгоритм ініціалізації генератора випадкових двійкових послідовностей відповідає вимогам документу «Методика ініціалізації генератора випадкових двійкових послідовностей. UA.42125815.00001-01 94 01».
10. Формат сертифіката відкритого ключа, формат списку відкликаних сертифікатів, які реалізовані та використовуються в об'єкті експертизи, відповідають вимогам ДСТУ ETSI EN 319 412:2016.
11. Формати запитів на отримання інформації про статус сертифікату та інформації про статус сертифіката, які реалізовані та використовуються в об'єкті експертизи, відповідають вимогам IETF RFC 6960.
12. Формат тестових ключових файлових контейнерів, що створюються та обробляються в об'єкті експертизи, відповідає вимогам IETF RFC 7292.
13. Об'єкт експертизи відповідає вимогам технічного завдання ТЗ У 72.2-42125815-005:2021 в частині реалізації функцій криптографічних перетворень.
14. Методи захисту, реалізовані в об'єкті експертизи, відповідають вимогам до засобів криптографічного захисту інформації класу Б1 (захист від порушника другого рівня), 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 у Міністерстві юстиції України 30.07.2007 за № 862/14129 (зі змінами).
15. В об'єкті експертизи правильно реалізовано методи захисту, визначені пунктом 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 у Міністерстві юстиції України 26.05.2021 за № 696/36318.
16. 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 62.0-42125815-005:2023.

Термін дії експертного висновку – до 29.12.2028.

Голова Служби

Юрій МИРОНЕНКО