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

26.04.2023 № 04/05/02-872/ВС1 На № _____ від _____

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 26.04.2023 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 22.04.2022 № 576.

Об'єкт експертизи: Програмний комплекс криптографічного захисту мережевих TLS-з'єднань «Шифр-WEB» ТЗ У 72.2-42125815-005:2022.

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

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

Висновки:

1. Об'єкт експертизи правильно використовує криптографічні перетворення, що реалізовані у засобі криптографічного захисту інформації Програмний комплекс криптографічних перетворень «Шифр+» версія 2.1 ТЗ У 72.2-23154898.003:2016, що має експертний висновок Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 21.08.2022 № 04-1022/ВС1.
2. Формат сертифікатів відкритих ключів, що використовуються та обробляються в об'єкті експертизи відповідає вимогам ДСТУ ISO/IEC 9594-8:2014, IETF RFC 5280.
3. В об'єкті експертизи протокол автентифікації серверного та клієнтських компонентів інформаційно-комунікаційних систем, протокол розподілу ключів та алгоритму обчислення спільного сеансового ключа та синхропосилки відповідають вимогам документу «Методика автентифікації серверного та клієнтських компонентів інформаційно-комунікаційних систем розподілу ключів та обчислення спільного сеансового ключа та синхропосилки UA.42125815.00005-01 94 01».
4. 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 в Міністерстві юстиції України 30.07.2007 за № 862/14129.

5. 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.
6. Об'єкт експертизи відповідає вимогам технічного завдання ТЗ У 72.2-42125815-005:2022 в частині реалізації функцій криптографічних перетворень.
7. 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:

```
cipher_engine.so       6CA4238C C37E0739 47661E1B 012E3B11 6F59617F A775DA1B 274F3002 F2E24A7D

Каталог Release-DLL-x64-skylake
libCCPPLib-linux.so    0E34F5C0 A74BEC46 447FDDFE 05DBE7D2 556DE774 75078AB4 510837E9 4CC82063

Каталог Release-DLL-x64-generic
libCCPPLib-linux.so    95C60B7E 277B0AF7 73EF299C 51B4B0A6 80BB1F47 43A3DD6B 2318DD2B 618049B9
```

Розрахунок геш-функцій здійснено відповідно до ДСТУ 7564:2014 (у режимі Купина-256 з використанням нульового вектора ініціалізації).

Термін дії експертного висновку – до 18.08.2027.

Голова Служби Юрій ЩИГОЛЬ