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

13.12.17 № 04/03/02-5063

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 13.12.2017 м. Київ

Виданий: Товариству з обмеженою відповідальністю «Ілайф» (код ЄДРПОУ 36049014).

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 07.12.2017 № 324.

Об'єкт експертизи: Програмний засіб криптографічного захисту інформації «Криптос Гейт Плас» UA.36049014.00002-01.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю «Ілайф» (код ЄДРПОУ 36049014).

Експертний заклад: Товариство з обмеженою відповідальністю «АЛТЕРСАЙН» (код ЄДРПОУ 38061489).

Висновки:

1. В об'єкті експертизи правильно реалізовано криптографічні алгоритми, визначені ДСТУ ГОСТ 28147:2009, ГОСТ 34.311-95, ДСТУ 4145-2002 (при реалізації в поліноміальному базисі).
2. В об'єкті експертизи правильно реалізовано алгоритм генерації випадкових двійкових послідовностей, визначений додатком А ДСТУ 4145-2002.
3. В об'єкті експертизи правильно реалізовано криптографічний протокол розподілу ключів Діффі-Гелмана (KANIDH), визначений п.8.2 ДСТУ ISO/IEC 15946-3:2006.
4. Алгоритм ініціалізації генератору випадкових послідовностей, реалізований в об'єкті експертизи, відповідає вимогам документу «Методика ініціалізації генератора випадкових послідовностей та зберігання особистих ключів асиметричних криптографічних алгоритмів UA.36049014.00002-01 91 01».
5. Формат посиленого сертифіката відкритого ключа, структура об'єктних ідентифікаторів для криптоалгоритмів, що є державними стандартами, формат списку відкликаних сертифікатів, 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 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 від 20.08.2012 за № 1398/21710.
6. Формати криптографічних повідомлень, які реалізовані та використовуються 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.

7. Алгоритми формування ключів шифрування ключів та захисту особистих ключів електронного цифрового підпису та особистих ключів шифрування, форматів транспортних контейнерів особистих ключів електронного цифрового підпису та особистих ключів шифрування, інтерфейсів бібліотек криптографічного захисту інформації, форматів контейнерів зберігання особистих ключів електронного цифрового підпису, особистих ключів шифрування, які реалізовані та використовуються в об'єкті експертизи, відповідають вимогам спільного наказу Міністерства юстиції України та Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 27.12.2013 № 2782/5/689 «Про затвердження вимог до алгоритмів, форматів та інтерфейсів, що реалізуються у засобах шифрування та надійних засобах електронного цифрового підпису», зареєстрованого в Міністерстві юстиції України 27.12.2013 за № 2228/24759.
8. Об'єкт експертизи відповідає вимогам технічного завдання UA.36049014.00002-01 90 01 із Доповненням № 1 UA.36049014.00002-01 90 02, Доповненням № 2 UA.36049014.00002-01 90 03 до нього, в частині реалізації функцій криптографічних перетворень.
9. 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:

```
Каталог NET
ElifeCrypto.dll       8C3EBDCC 9E86B20C 992E3588 EE95C0FA F3427266 1D7CE07F 52A16810 73F28F7E
ElifeCrypto.Plus.dll  696D23D0 DA2409C8 27A6B6A3 A0E08AEF EDF01135 C48B1954 4A5C2AE4 C6E4AF15

Каталог Silverlight
ElifeCrypto.dll       EECDCD9F 97C3BADE FAA579D9 607065BD 32978C49 276F9555 D2923175 3C81DE78
ElifeCrypto.Plus.dll  DE70F2AB 68BE193A FF01B5D3 7BF5A150 911A1D79 E711E484 4BBFCB12 8CB7A422

Каталог Java
cgprov.jar            B78003D5 849E5DE2 F060287B 0561B827 84A7642C 589E4DEE 2CC94A2A 9430571D
```

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 07.12.2022.

Перший заступник Голови Служби О.М. Чаузов