Прим. № 1

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

вул. Солом'янська, 13, м. Київ, 03680,
тел. (044) 281-92-10, факс: (044) 281-94-83, e-mail: info@dsszzi.gov.ua

27.07.2015 р. № 05/02/02-3147

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 27.07.2015 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 27.07.2015 № 203.

Об'єкт експертизи: Програмний виріб "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 реалізовані криптографічні алгоритми, які визначені ДСТУ ГОСТ 28147:2009, ГОСТ 34.311-95, ДСТУ 4145-2002 (при реалізації в поліноміальному базисі).
2. В об'єкті експертизи правильно реалізований алгоритм генерації випадкових двійкових послідовностей, який визначений в додатку А ДСТУ 4145-2002.
3. В об'єкті експертизи правильно реалізований криптографічний протокол розподілу ключів KANIDH, який визначений в п.8.2 ДСТУ ISO/IEC 15946-3:2006.
4. 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.
5. 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.
6. 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.

7. Об'єкт експертизи відповідає вимогам технічного завдання UA.36049014.00002-01 90 01 із Доповненням № 1 UA.36049014.00002-01 90 02 і Доповненням № 2 UA.36049014.00002-01 90 03 до нього, в частині реалізації функцій криптографічних перетворень

8. 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 NET20
ElifeCrypto.dll*       D519E992 DE21A459 9BBDCA97 268CEC6F E95C7BC0 4951DD34 F1D80B75 EF76A5D5
ElifeCrypto.Plus.dll* D9789296 387E7F1C 8A91D7B3 30FCADC5 BA64AE4D EDBE3FF1 4A25657A A5C5057D

Каталог SL5
ElifeCrypto.dll*       CC29BE47 A6E59DD8 90E329E4 AE972A0A 44548EFE FEAF7A98 7190E8FB 63111927
ElifeCrypto.Plus.dll* 0ED2EE11 7213A3F6 F5AFD6BD 5E76A3A0 63C4F9EB 5172BD5A 35605F63 56EB1E83
```

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 27.07.2020.

Голова Служби Л.О. Євдоченко