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

11.03.2013 № 05/02/02-811

ЕКСПЕРТНИЙ ВИСНОВОК

Виданий: Приватному акціонерному товариству "Інститут інформаційних технологій" (код ЄДРПОУ 22723472)

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 11.03.2013 № 108.

Об'єкт експертизи: Модуль криптографічний "Гряда-61" (ТУ У 30.0-22723472-002:2007).

Розроблений (виготовлений): Приватним акціонерним товариством "Інститут інформаційних технологій" (код ЄДРПОУ 22723472).

Експертний заклад: Адміністрація Державної служби спеціального зв'язку та захисту інформації України.

Висновки:

1. В об'єкті експертизи правильно реалізовані криптографічні алгоритми ДСТУ ГОСТ 28147:2009 (в режимі простої заміни, гамування, гамування із зворотнім зв'язком та обчислення імітовставки).
2. В об'єкті експертизи алгоритм гешування відповідає алгоритму ГОСТ 34.311-95.
3. В об'єкті експертизи алгоритми формування, перевіряння та генерації параметрів ЕЦП у поліноміальному базисі відповідає алгоритму ДСТУ 4145-2002.
4. В об'єкті експертизи алгоритм розподілу ключових даних відповідає алгоритму, що наведений у документі "Методика розподілу ключових даних на основі протоколу Діффі-Гелмана в групі точок еліптичної кривої та формат представлення криптографічних повідомлень" (ЄААД.468244.020 Д1.04).
5. Об'єкт експертизи відповідає вимогам технічного завдання (ЄААД.469535.044 ТЗ) та технічних умов (ТУ У 30.0-22723472-002:2007) в частині реалізації функцій криптографічних перетворень.
6. 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, які виготовлено відповідно до технічних умов (ТУ У 30.0-22723472-002:2007).

Термін дії експертного висновку: до 11.03.2018.

Перший заступник Голови Служби О.Г. Цуркан

Копія вірна

УКРАЇНА ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО «ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ» №22723472