Прим. № 1

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

вул. Солом'янська, 13, м. Київ, 03680,
тел. (044) 281-90-10, факс: (044) 226-26-83, e-mail: info@dsszzi.gov.ua

26.12.2012 № 05/02/02-5541

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 25.12.2012 № 102.

Об'єкт експертизи: Апаратно-програмний засіб криптографічного захисту інформації "Електронний ключ "Кристал-1".

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 (у режимі простої заміни та обчислення імітовставки), ГОСТ 34.311-95, ДСТУ 4145-2002.
2. Реалізація алгоритму розподілу ключових даних в об'єкті експертизи відповідає "Методиці розподілу ключових даних на основі протоколу Діффі-Гелмана в групі точок еліптичної кривої" № 85 від 01.11.2004р.
3. Процедури статистичного тестування випадкових послідовностей з виходу генератору випадкових сигналів відповідають "Методиці генерації ключових даних" № 85 від 01.11.2004р.
4. Об'єкт експертизи відповідає вимогам технічного завдання (ЄААД.469535.040 ТЗ), в частині реалізації функцій криптографічних перетворень.
5. 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 30.0-22723472-001:2007.

Термін дії експертного висновку: до 25.12.2017.

В.о. Голови Служби О.Г. Цуркан

АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ * Ідентифікаційний код 34620942 *