Прим. № 1

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

тел. (044) 281-92-10, факс: (044) 281-94-83, e-mail: info@dsszzi.gov.ua

21.12.2018 № 04/03/02-4980

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 21.12.2018 м. Київ

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 21.12.2018 № 377.

Об'єкт експертизи: IP-шифратори «Канал-201/301/401» ТУ У 26.2-22723472-009:2018 зі складу Комплексу криптографічного захисту інформації у IP-мережах «ІІТ Захист IP-потоку-2» ЄААД.468244.093.

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

Експертний заклад: Адміністрація Державної служби спеціального зв'язку та захисту інформації України (код ЄДРПОУ 34620942).

Висновки:

1. В об'єкті експертизи правильно реалізовано криптографічні алгоритми, визначені ДСТУ ГОСТ 28147:2009, ДСТУ 4145-2002, ГОСТ 34.311-95.
2. В об'єкті експертизи правильно реалізовано протокол автономного узгодження ключів в групі точок еліптичної кривої типу Діффі-Геллмана (KANIDH), визначений п. 8.2 ДСТУ ISO/IEC 15946-3:2006.
3. В об'єкті експертизи алгоритм генерації ключових даних відповідає документу «Методика генерації ключових даних» ЄААД.468244.020 Д1.05.
4. В об'єкті експертизи правильно реалізовано механізми взаємної автентифікації, визначені ДСТУ ISO/IEC 9798-3.
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, що 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 у Міністерстві юстиції України 20.08.2012 за № 1398/21710.
6. В об'єкті експертизи формат захищених даних та криптографічний протокол Діффі-Геллмана, що базується на криптографічних перетвореннях у групі точок еліптичної кривої (ECDH), що 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 у 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, формати транспортних контейнерів особистих ключів електронного цифрового підпису та особистих ключів шифрування, формати контейнерів зберігання особистих ключів електронного цифрового підпису, особистих ключів шифрування та сертифікатів відкритих ключів, прикладний програмний інтерфейс, які реалізовані, створюються 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 часткового технічного завдання ЄААД.469535.088/090/091 із Доповненням № 1 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 ЄААД 469535.088 (IP-шифратор «Канал-201»), ЄААД 469535.239 (IP-шифратор «Канал-201» (мікро-пристрій)), ЄААД 469535.090 (IP-шифратор «Канал-301), ЄААД 469535.091 (IP-шифратор «Канал-401) виготовлені відповідно до технічних умов ТУ У 26.2-22723472-009:2018.

Термін дії експертного висновку – до 21.12.2023.

Перший заступник Голови Служби О.М. Чаузов