Прим. № 1

АДМІНІСТРАЦІЯ
ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ
(АДМІНІСТРАЦІЯ ДЕРЖСПЕЦЗВ'ЯЗКУ)

вул. Солом'янська, 13, м. Київ, 03110, тел. (044) 281-93-08, факс: (044) 281-94-83,
e-mail: info@cip.gov.ua, сайт: www.cip.gov.ua, код згідно з ЄДРПОУ 34620942

20.11.2023 № 04/05/01-1121/ВС1 На № _____ від _____

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 20.11.2023 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 17.11.2023 № 595.

Об'єкт експертизи: Криптомодуль мережний «Гряда-301» ЄААД.469535.049, ЄААД.469535.240, ЄААД.469535.241, ЄААД.469535.243.

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 7624-2014 (у режимах «Калина-256/256-CFB», «Калина-256/256-CBC», «Калина-256/256-CMAC»), ДСТУ 4145-2002 (у поліноміальному базисі з довжиною ключа 163-509 біт), ДСТУ 7564-2014 (у режимі «Купина-256»), ГОСТ 28147-89 (у режимах простої заміни, гамування зі зворотнім зв'язком та обчислення імітовставки), ГОСТ 34.311-95.
2. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного підпису ECDSA, визначений ДСТУ ISO/IEC 14888-3:2019.
3. В об'єкті експертизи правильно реалізовано криптографічний алгоритм електронного підпису RSA, визначений PKSC#1 v.2.1 «RSA Cryptography Standard» (за схемою RSASSA-PKCSl-vl_5).
4. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-1, SHA-256, SHA-384, SHA-512, визначені ДСТУ ISO/IEC 10118-3:2023.
5. В об'єкті експертизи правильно реалізовано криптографічний алгоритм гешування SHA-224, визначений FIPS PUB 180-4 Federal Information Processing Standards Publication.
6. В об'єкті експертизи правильно реалізовано протоколи узгодження ключів типу Діффі-Геллмана (DH, ECDH), визначені ДСТУ ISO/IEC 11770-3:2023.
7. Методи захисту, реалізовані в об'єкті експертизи, відповідають вимогам до засобів криптографічного захисту інформації класу Б2 (захист від порушника другого рівня), визначеним в Положенні про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженому наказом Адміністрації Державної служби

спеціального зв'язку та захисту інформації України від 20.07.2007 № 141, зареєстрованим в Міністерстві юстиції України 30.07.2007 за № 862/14129.
8. Об'єкт експертизи відповідає вимогам технічного завдання ЄААД.469535.049 ТЗ із Доповненням № 8 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, виготовлені відповідно до технічних умов ТУ У 26.2-22723472-003:2017 зі Зміною № 1:2023.

Термін дії експертного висновку – до 17.11.2028.

Голова Служби Юрій ЩИГОЛЬ

Прим. № 1

АДМІНІСТРАЦІЯ
ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ
(АДМІНІСТРАЦІЯ ДЕРЖСПЕЦЗВ'ЯЗКУ)

вул. Солом'янська, 13, м. Київ, 03110, тел. (044) 281-93-08, факс: (044) 281-94-83,
e-mail: info@cip.gov.ua, сайт: www.cip.gov.ua, код згідно з ЄДРПОУ 34620942

20.11.2023 № 04/05/02-1122/ВС1 На № _____ від _____

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 20.11.2023 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 17.11.2023 № 595.

Об'єкт експертизи: Криптомодуль мережний «Гряда-301» ЄААД.469535.049, ЄААД.469535.240, ЄААД.469535.241, ЄААД.469535.243.

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 реалізовано механізми, які забезпечують виконання функціональних вимог безпеки, що визначені ДСТУ EN 419211-2:2016 (EN 419211-2:2013 IDT) «Профілі захисту для пристроїв створення безпечного підпису. Частина 2. Пристрій з генерацією ключів».
2. В об'єкті експертизи реалізовано механізми, які забезпечують виконання функціональних вимог безпеки, що визначені ДСТУ EN 419211-5:2016 (EN 419211-5:2013 IDT) «Профілі захисту для пристроїв створення безпечного підпису. Частина 5. Розширення для пристроїв з генерацією ключів та довіреним каналом для застосування створення підпису».
3. Об'єкт експертизи може бути використаний в якості засобу кваліфікованого електронного підпису чи печатки для надання електронних довірчих послуг.

Особливі умови (рекомендації):

1. Експертний висновок свідчить про реалізацію в об'єкті експертизи механізмів, які забезпечують виконання функціональних вимог безпеки, в обсязі виконуваних функцій (за призначенням), згідно ДСТУ EN 419211-1:2016 (EN 419211-1:2014 IDT) «Профілі захисту для пристроїв створення безпечного підпису. Частина 1. Огляд».

2. Реалізовані в об'єкті експертизи криптографічні алгоритми наведено у експертному висновку від 20.11.2023 № 04/05/02-1121/ВС1.

Термін дії експертного висновку – до 17.11.2028.

Голова Служби Юрій ЩИГОЛЬ