Прим. № __

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

вул. Солом'янська , 13, м. Київ, 03110, тел. (044) 281-92-10, факс: (044) 281-94-83,
e-mail: info@dsszzi.gov.ua, сайт: www.dsszzi.gov.ua, код згідно з ЄДРПОУ 34620942

12.05.2021 № 04/05/02-1382 На № _____ від _____

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 12.05.2021 м. Київ

Виданий: Товариству з обмеженою відповідальністю «АВТОР» (код ЄДРПОУ 32248356)

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 12.05.2021 № 500.

Об'єкт експертизи: ПРИСТРОЇ ДЛЯ АВТОМАТИЧНОГО ОБРОБЛЕННЯ ІНФОРМАЦІЇ-КЛЮЧІ ЕЛЕКТРОННІ «SECURE TOKEN-337» АЧСА.467369.010, АЧСА.467369.012, АЧСА.467369.014, АЧСА.467369.024.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю «АВТОР» (код ЄДРПОУ 32248356).

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 (в режимах простої заміни, гамування із зворотним зв'язком та обчислення імітовставки), ГОСТ 34.311-95, ДСТУ 4145-2002 (у поліноміальному базисі з довжиною ключа 163-509 біт).
2. В об'єкті експертизи правильно реалізовано криптографічні алгоритми шифрування DES, TDEA, AES відповідно ДСТУ ISO/IEC 18033-3:2015 (в режимах ECB, CBC, CFB, визначені ДСТУ ISO/IEC 10116:2019).
3. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування RSA, визначений PKCS#1 v2.1 RSA Cryptography Standard (за схемою RSAES-PKCS1-v1_5 з довжиною ключа 1024, 1536, 2048 біт).
4. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного цифрового підпису RSA, визначений PKCS#1 v2.1 «RSA Cryptography Standard» (за схемою RSASSA-PKCSl-vl_5 з довжиною ключа 1024, 1536, 2048 біт).
5. В об'єкті експертизи правильно реалізовано криптографічний алгоритм гешування SHA-1, визначений в ДСТУ ISO/IEC 10118-3:2005.
6. В об'єкті експертизи правильно реалізовано алгоритм вироблення імітовставки (MAC) згідно алгоритму DES відповідно до FIPS PUB 81 Federal Information Processing Standards Publication 81 (в режимі роботи MAC-CBC).

7. В об'єкті експертизи правильно реалізовано алгоритм вироблення імітовставки (MAC) згідно алгоритму AES відповідно до NIST 800-38A NIST Special Publication (в режимі MAC-CBC).
8. В об'єкті експертизи правильно реалізовано алгоритм вироблення імітовставки (CMAC) згідно алгоритму AES відповідно до NIST Special Publication 800-38B (в режимі CMAC).
9. Порядок вироблення сеансових ключів для шифрування даних в об'єкті експертизи реалізовано відповідно до документа «Засоби КЗІ. Методика вироблення сеансового ключа, автентифікації, генерування випадкових послідовностей та контролю засобів КЗІ АЧСА.460709.001».
10. В об'єкті експертизи вироблення сеансових ключів для шифрування даних реалізовано відповідно до вимог IETF RFC 5652 «Cryptographic Massage Syntax (CMS)» з Технічними специфікаціями до них, які затверджені наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 27.10.2020 № 687 «Про затвердження переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації», зареєстрованого в Міністерстві юстиції України 21.12.2020 за № 1272/35555 (ECDH в поліноміальному базисі, з довжиною ключа 163-509 біт).
11. 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 № 141 від 20.07.2007, зареєстрованим в Міністерстві юстиції України 30.07.2007 за № 862/14129 (зі змінами).
12. Об'єкт експертизи відповідає вимогам Технічного завдання ТЗ.АЧСА.467649.041-01 із Доповненням № 1 до нього, в частині реалізації функцій криптографічних перетворень.
13. Об'єкт експертизи (як засіб криптографічного захисту інформації категорії «Ш», «К», «Р», «П») може бути використаний як складова частина при побудові засобів криптографічного захисту інформації видів «А» та «Б», призначених 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.
14. Об'єкт експертизи (як засіб криптографічного захисту інформації категорії «П», «К») може бути використаний як складова частина при побудові засобів криптографічного захисту інформації видів «А» та «Б», призначених для криптографічного захисту інформації з обмеженим доступом (крім інформації, що становить державну таємницю).

Особливі умови (рекомендації):
1. Ступень обмеження доступу до інформації, захист якої має забезпечуватися об'єктом експертизи, що використовується як складова частина при побудові засобів криптографічного захисту інформації видів «А» та «Б», визначається вимогами до відповідного комплексу.
2. Дія експертного висновку поширюється на зразки об'єкта експертизи, які виготовлені відповідно до технічних умов ТУ У 30.0-32248356-017:2011 із Сповіщенням АЧСА.02-2013 про зміну № 1 та Сповіщенням АЧСА.03-2016 про зміну № 2.

Термін дії експертного висновку – до 12.05.2026.

Голова Служби Юрій ЩИГОЛЬ

Прим. № __

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

вул. Солом'янська , 13, м. Київ, 03110, тел. (044) 281-92-10, факс: (044) 281-94-83,
e-mail: info@dsszzi.gov.ua, сайт: www.dsszzi.gov.ua, код згідно з ЄДРПОУ 34620942

12.05.2021 № 04/05/02-1383 На № _____ від _____

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 12.05.2021 м. Київ

Виданий: Товариству з обмеженою відповідальністю «АВТОР» (код ЄДРПОУ 32248356)

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 12.05.2021 № 500.

Об'єкт експертизи: ПРИСТРОЇ ДЛЯ АВТОМАТИЧНОГО ОБРОБЛЕННЯ ІНФОРМАЦІЇ – КЛЮЧІ ЕЛЕКТРОННІ «SECURE TOKEN-337» АЧСА.467369.010, АЧСА.467369.012, АЧСА.467369.014, АЧСА.467369.024.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю «АВТОР» (код ЄДРПОУ 32248356).

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 419211-3:2016 (EN 419211-3:2013 IDT) «Профілі захисту для пристроїв створення безпечного підпису. Частина 3. Пристрій з імпортом ключів».
3. В об'єкті експертизи реалізовано механізми, які забезпечують виконання функціональних вимог безпеки, що визначені ДСТУ EN 419211-4:2016 (EN 419211-4:2013 IDT) «Профілі захисту для пристроїв створення безпечного підпису. Частина 4. Розширення для пристроїв з генерацією ключів та довіреним каналом для застосування генерації сертифікатів».
4. 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».

5. В об’єкті експертизи реалізовано механізми, які забезпечують виконання функціональних вимог безпеки, що визначені ДСТУ EN 419211-6:2016 (EN 419211-6:2014 IDT) «Профілі захисту для пристроїв створення безпечного підпису. Частина 6. Розширення для пристроїв з імпортом ключів та довіреним каналом для застосування створення підпису».
6. 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 12.05.2021 № 04/05/02-1382.

Термін дії експертного висновку – до 12.05.2026.

Голова Служби Юрій ЩИГОЛЬ