Прим. № 1

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

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

20.01.2020 № 04/03/02-133 На № _____ від _____

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 20.01.2020 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 17.01.2020 № 438.

Об'єкт експертизи: КЛЮЧІ ЕЛЕКТРОННІ «SECURE TOKEN-338».

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).

1. В об'єкті експертизи криптографічні алгоритми реалізовано відповідно до вимог ДСТУ ГОСТ 28147:2009, ДСТУ 7624:2014 (Калина-128/128, Калина-128/256) у режимах ECB, CFB, CMAC, CBC, KW), ДСТУ 7564:2014 (у режимах Купина-384, Купина-512), ГОСТ 34.311-95, ДСТУ 4145-2002 (у поліноміальному та оптимальному нормальному базисах, з довжиною ключа 163-509 біт).
2. В об'єкті експертизи алгоритм генерації випадкових послідовностей відповідає додатку А ДСТУ 4145-2002.
3. В об'єкті експертизи правильно реалізовано криптографічні алгоритми шифрування TDEA, AES, DES, визначені ДСТУ ISO/IEC 18033-3:2015 (в режимах CBC, ECB і CFB, визначених ДСТУ ISO/IEC 10116:2015).
4. В об'єкті експертизи правильно реалізовано криптографічний алгоритм гешування SHA-1, SHA-256, визначені ДСТУ ISO/IEC 10118-3:2005.
5. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування RSA, визначений в PKCS#1 v2.1 RSA Cryptography Standard (за схемою RSAES-PKCS1-v1_5).
6. В об'єкті експертизи правильно реалізовано криптографічний алгоритм електронного цифрового підпису RSA, визначений PKCS#1 v2.1 «RSA Cryptography Standard» (за схемами RSASSA-PSS, RSASSA-PKCS1-v1_5, з довжиною ключа 1024-4096 біт).
7. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного цифрового підпису ECDSA, визначений ДСТУ ISO/IEC 14888-3:2015, з довжиною ключа 192-521 біт.
8. В об'єкті експертизи алгоритм вироблення імітовставки (MAC) згідно алгоритму DES, TDES реалізовано відповідно до FIPS PUB 81 Federal Information Processing Standards Publication 81 (в режимі MAC-CBC).

9. В об'єкті експертизи алгоритм вироблення імітовставки (MAC) згідно алгоритму AES реалізовано відповідно до NIST 800-38A NIST Special Publication (в режимі MAC-CBC).
10. В об'єкті експертизи правильно реалізовано алгоритм вироблення імітовставки (CMAC) згідно алгоритму AES відповідно до NIST Special Publication 800-38B (в режимі CMAC).
11. 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».
12. В об'єкті експертизи обчислення спільного секрету для криптографічного протоколу 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, та ДСТУ ISO/IEC 15946-3:2006.
13. Об'єкт експертизи відповідає вимогам технічного завдання ТЗ.АЧСА.467649.062-01 із Доповненням № 1 до нього в частині реалізації функцій криптографічних перетворень.
14. Об'єкт експертизи, як засіб криптографічного захисту виду «В» (категорій «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.
15. Об'єкт експертизи, як засіб криптографічного захисту виду «В» (категорії «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 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 26.2-32248356-029:2020.

Термін дії експертного висновку – до 17.01.2025.

Голова Служби

Валентин ПЕТРОВ

Прим. № 1

АДМІНІСТРАЦІЯ ДЕРЖСПЕЦЗВ'ЯЗКУ

Департамент захисту інформації
(ДЗІ Адміністрації Держспецзв'язку)
вул. Солом'янська, 13, м. Київ, Україна, 03110,
тел./факс (044) 281-96-82
e-mail: dzi@cip.gov.ua

Директору ТОВ «АВТОР»
Миколі САКОВИЧУ
e-mail: avtor@avtor.ua

_____ № _____

На № 16/01-1 від 16.01.2025

Щодо продовження терміну дії
експертних висновків

Шановний пане Миколо!

В Адміністрації Держспецзв'язку опрацьовано листа ТОВ «АВТОР» від 16.01.2024 № 16/01-1 щодо продовження терміну дії експертних висновків на засоби криптографічного захисту інформації «Ключі електронні «Secure Token-338» та «Карти мікропроцесорні «CryptoCard-338».

За результатами опрацювання інформуємо, що з урахуванням правового режиму воєнного стану в Україні, на підставі рішення Експертної комісії з питань проведення державної експертизи в сфері криптографічного захисту інформації Держспецзв'язку (протокол засідання від 27.03.2022 № 536), термін дії експертних висновків: від 20.01.2020 № 04/03/02-133, від 14.04.2021 № 04/05/02-1000 на «Ключі електронні «Secure Token-338» та від 20.01.2020 № 04/03/02-134, від 14.04.2021 № 04/05/02-999 на «Карти мікропроцесорні «CryptoCard-338» продовжено на шість місяців, а саме до 17.07.2025.

Додатково пропонуємо опрацювати питання своєчасного подання до Адміністрації Держспецзв'язку заявок на проведення державної експертизи в сфері КЗІ засобів криптографічного захисту інформації «Ключі електронні «Secure Token-338» та «Карти мікропроцесорні «CryptoCard-338» з урахуванням вимог п. 2.3.18 Положення про державну експертизу в сфері криптографічного захисту інформації, затвердженого наказом Адміністрації Держспецзв'язку від 23.06.2008 № 100, зареєстрованим в Мін'юсті 16.07.2008 за № 651/15342 (зі змінами).

З повагою

Директор Департаменту Олександр ГРИЩЕНКО

Анжеліка ГОРЛИНСЬКА 281-97-77

UB
Адміністрація Держспецзв'язку
№04/04/02-727/2025 від 24.01.2025
КЕП: Грищенко О. О. 24.01.2025 16:38
10E3F0
Сертифікат дійсний з 05.03.2024 12:37 до 05.03.2026 12:37

АДМІНІСТРАЦІЯ ДЕРЖСПЕЦЗВ'ЯЗКУ
Департамент захисту інформації
ДЗІ Адміністрації Держспецзв'язку

вул. Солом'янська, 13, м. Київ, 03110,
тел. (044) 281-96-82,
e-mail: aparat@cip.gov.ua,
web: cip.gov.ua
Код ЄДРПОУ 34620942

ТОВ «АВТОР»

e-mail: avtor@avtor.ua

від _____ 20__ р. № _____ На
№ _10/07-02_____ від _____10.07.2025 р.

Щодо продовження терміну дії експертних висновків

В Адміністрації Держспецзв'язку опрацьовано листа ТОВ «АВТОР» від 10.07.2025 № 10/07-02 щодо продовження терміну дії експертних висновків на засоби криптографічного захисту інформації ключі електронні «Secure Token-338» (далі – вироби «Secure Token-338») та карти мікропроцесорні «CryptoCard-338» (далі – вироби «CryptoCard-338»).

З урахуванням правового режиму воєнного стану в Україні, терміни дії експертних висновків від 20.01.2020 № 04/03/02-133 та від 14.04.2021 № 04/05/02-1000 на вироби «Secure Token-338», а також експертних висновків від 20.01.2020 № 04/03/02-134 та від 14.04.2021 № 04/05/02-999 на вироби «CryptoCard-338» продовжено до 17.01.2026.

Додатково інформуємо, що згідно вимог пункту 2.3.18 Положення про державну експертизу в сфері криптографічного захисту інформації, затвердженого наказом Адміністрації Держспецзв'язку від 23.06.2008 № 100, зареєстрованим в Мін'юсті 16.07.2008 за № 651/15342 (зі змінами), замовнику рекомендується не пізніше як за шість місяців до закінчення терміну дії діючого експертного висновку надіслати до Адміністрації Держспецзв'язку заявку на проведення державної експертизи об'єкта експертизи.

Варто також зазначити, що з моменту проведення державної експертизи в сфері криптографічного захисту інформації виробів «Secure Token-338» та «CryptoCard-338» відбулися зміни законодавства, зокрема у сфері електронної ідентифікації, електронних довірчих послуг та щодо технічних вимог до засобів, призначених для надання послуг електронної ідентифікації та електронних довірчих послуг.

Зокрема, 04.01.2021 втратив чинність наказ Адміністрації Держспецзв'язку від 18.12.2012 № 739 «Про затвердження Вимог до форматів криптографічних повідомлень», зареєстрований в Мін'юсті 14.01.2013 за № 108/22640, відповідність вимогам якого зазначена у експертних висновках від 20.01.2020 №№ 04/03/02-133 та 04/03/02-134.

Також з 01.04.2021 скасовано ДСТУ ISO/IEC 15946-3:2006 «Інформаційні технології. Методи захисту. Криптографічні методи, що ґрунтуються на еліптичних кривих. Частина 3. Установлення ключів» (ISO/IEC 15946-3:2002, IDT), відповідність вимогам якого зазначена у експертних висновках від 20.10.2020 від 20.01.2020 №№ 04/03/02-133 та 04/03/02-134 (на теперішній час вимоги до управління ключами із застосуванням асиметричних методів визначені ДСТУ ISO/IEC 11770-3:2023 «Інформаційні технології. Керування ключами. Частина 3. Механізми із застосуванням асиметричних методів» (ISO/IEC 11770-3:2021, IDT)).

Крім того, реалізація криптографічного алгоритму RSA (в тому числі, в частині вимог щодо довжини ключа), повинна відповідати положенням ДСТУ ETSI TS 119 312:2022 «Електронні підписи та інфраструктури (ESI). Криптографічні пакети» (ETSI TS 119 312 V1.4.2 (2022-02), IDT)).

Також варто зазначити, що наказом Мінцифри від 18.01.2024 № 12 «Про затвердження Особливостей надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката шифрування», зареєстрованим в Мін'юсті 05.02.2024 за № 176/41521, встановлено вимоги до засобів криптографічного захисту інформації, які забезпечують використання кваліфікованих сертифікатів шифрування.

Враховуючи зазначене, з урахуванням вимог пунктів 2.1.14, 2.3.18 та 2.3.19 Положення про державну експертизу в сфері криптографічного захисту інформації, затвердженого наказом Адміністрації Держспецзв'язку від 23.06.2008 № 100, зареєстрованим в Мін'юсті 16.07.2008 за № 651/15342 (зі змінами), пропонуємо опрацювати питання необхідності проведення державної експертизи в сфері криптографічного захисту інформації виробів «Secure Token-338» та «CryptoCard-338» для отримання нових експертних висновків, зокрема, в частині використання виробів «Secure Token-338» та «CryptoCard-338» за призначенням з урахуванням чинних вимог законодавства щодо криптографічного захисту інформації, електронної ідентифікації та електронних довірчих послуг.

Директор Департаменту Андрій ГОЛОВЕНКО

Роман Коробко 281-97-61

АДМІНІСТРАЦІЯ ДЕРЖСПЕЦЗВ'ЯЗКУ

Департамент захисту інформації
ДЗІ Адміністрації Держспецзв'язку

вул. Солом'янська, 13, м. Київ, 03110,
тел. (044) 281-96-82,
e-mail: aparat@cip.gov.ua,
web: cip.gov.ua
Код ЄДРПОУ 34620942

ТОВ «АВТОР»

e-mail: avtor@avtor.ua

від _____ 20__ р. № _____

На № _22/12-01_____ від _____22.12.2025 р.

Щодо подовження терміну дії
експертних висновків (додатково
до № 04/03/02-8091/2025 від 05.08.2025)

В Адміністрації Держспецзв'язку опрацьовано лист ТОВ «АВТОР» від 22.12.2025 № 22/12-01 щодо подовження терміну дії експертних висновків на ключі електронні «Secure Token-338» та карти мікропроцесорні «CryptoCard-338».

З урахуванням правового режиму воєнного стану в Україні, термін дії експертних висновків від 20.10.2020 № 04/03/02-133, від 14.04.2021 № 04/05/02-1000 на ключі електронні «Secure Token-338» та від 20.01.2020 № 04/03/02-134, від 14.04.2021 № 04/05/02-999 на карти мікропроцесорні «CryptoCard-338» подовжено до 17.07.2026.

Директор Департаменту Андрій ГОЛОВЕНКО

Яніна Ткаченко 281-97-61