Прим. №__

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

_____ № _____ На № _____ від _____

Державна регуляторна служба України

Щодо погодження проєкту наказу

Відповідно до вимог статті 21 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності» надсилаємо для розгляду та погодження проєкт наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про внесення змін до Переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації» (далі – проєкт наказу).

Додатки: 1. Проєкт наказу на 9 арк.
2. Пояснювальна записка до проєкту наказу на 3 арк.
3. Аналіз регуляторного впливу до проєкту наказу на 7 арк.
4. Повідомлення про оприлюднення до проєкту наказу на 1 арк.

Голова Служби Юрій ЩИГОЛЬ

Анастасія Корчагіна 281 97 47

АНАЛІЗ РЕГУЛЯТОРНОГО ВПЛИВУ

до проєкту наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про внесення змін до Переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації»

I. Визначення проблеми

На сьогодні розроблення, виробництво та експлуатація засобів криптографічного захисту інформації здійснюються:

відповідно до вимог Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації (далі – Положення № 141), затвердженого наказом Адміністрації Держспецзв'язку від 20.07.2007 № 141;

відповідно до вимог Технічного регламенту засобів криптографічного захисту інформації (далі – ТР КЗІ), затвердженого постановою Кабінету Міністрів України від 21 жовтня 2020 року № 991.

Відповідно до частин першої та другої статті 23 Закону України «Про стандартизацію», пункту 10 ТР КЗІ, пункту 12 розділу ІІ Положення № 141, підпунктом 1 пункту 2 наказу Адміністрації Держспецзв'язку від 27 жовтня 2020 року № 687, зареєстрованим в Мін'юсті 21.12.2020 за № 1272/35555 (далі – Наказ № 687), встановлено, що у засобах криптографічного захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом (далі – засоби КЗІ), реалізуються криптоалгоритми та криптопротоколи, які є національними стандартами в обсязі функцій безпеки згідно з Переліком стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації (далі – Перелік), якщо інше не встановлено нормативно-правовими актами.

Водночас деякі національні стандарти, зазначені у Переліку, не є чинними у зв'язку з прийняттям оновлених версій та поправок до них.

Тому потребує врегулювання питання актуалізації Переліку шляхом його оновлення та доповнення.

Метою прийняття проєкту наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про внесення змін до Переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації» (далі – проєкт наказу) є актуалізація Переліку.

Основними показниками, що характеризують обсяги ринку засобів КЗІ є:

кількість розробників засобів КЗІ;

кількість органів з оцінки відповідності;

кількість експертних закладів;

кількість виданих декларацій про відповідність;

кількість виданих експертних висновків.

На цей час показники, що характеризують обсяги ринку засобів КЗІ, мають такі значення:

кількість розробників засобів КЗІ – 33;

кількість органів з оцінки відповідності – 0;

кількість експертних закладів – 7;

кількість виданих декларацій про відповідність – 0;

кількість виданих експертних висновків (середній показник на рік) – 70.

Припускається, що кількість користувачів засобів КЗІ (фізичні особи – громадяни, юридичні особи у тому числі суб'єкти господарювання) складає понад 10 млн. осіб.

Протягом останніх 5 років видано 348 експертних висновків за результатами державної експертизи у сфері КЗІ, що в середньому становить 70 висновки на рік:

Рік	2018	2019	2020	2021	2022
Кількість програмних засобів КЗІ	23	19	13	21	7
Кількість програмно-апаратних засобів КЗІ	41	37	49	80	58
Загальна кількість засобів КЗІ	64	56	62	101	65

Основні групи, на які проблема справляє вплив:

Групи	**Так**	**Ні**
Громадяни	Так	
Держава	Так	
Суб'єкти господарювання	Так	

Проблема не може бути розв'язана за допомогою ринкових механізмів, оскільки це не буде відповідати вимогам чинного законодавства України.

II. Цілі державного регулювання

Проєкт Наказу розроблено з метою актуалізації Переліку шляхом внесення таких змін до його розділів:

доповнення стандартами, що введенні вперше (16) та змінами до них (2);

доповнення стандартів поправками (1);

доповнення стандартів змінами (5);

заміни стандартів новими версіями (11) та змінами до них (2).

III. Визначення та оцінка альтернативних способів досягнення цілей

1. Визначення альтернативних способів

Вид альтернативи	Опис альтернативи
Альтернатива 1	*Прийняття проекту постанови*
Альтернатива 2	*Збереження чинного регулювання*

2. Оцінка вибраних альтернативних способів досягнення цілей

Оцінка впливу на сферу інтересів держави

Вид альтернативи	Вигоди	Витрати
Альтернатива 1. *Прийняття проекту наказу*	Високі, передбачає приведення у відповідність регуляторного акта, у який вносяться зміни, принципам державної регуляторної політики	Додаткових витрат не потребує
Альтернатива 2. *Збереження чинного регулювання*	Відсутні, оскільки дана ситуація призведе до застосування в Україні нечинних стандартів	Додаткових витрат не потребує

Оцінка впливу на сферу інтересів громадян

Вид альтернативи	Вигоди	Витрати
Альтернатива 1. *Прийняття проекту наказу*	Високі, використання для захисту персональних даних громадян сучасних засобів КЗІ	Додаткових витрат не потребує
Альтернатива 2. *Збереження чинного регулювання*	Відсутні, використання для захисту персональних даних громадян застарілих засобів КЗІ	Ризики компрометації засобів КЗІ через їх невідповідність сучасним вимогам, що може призвести до моральних та економічних витрат.

Оцінка впливу на сферу інтересів суб'єктів господарювання

Оцінка впливу на сферу інтересів суб'єктів господарювання

Під час визначення впливу на сферу інтересів суб’єктів господарювання доцільно розглянути такі фактори, зокрема:

вплив на продуктивність та конкурентоспроможність суб’єктів господарювання;

вплив на інновації та розвиток.

Показник	Великі	Середні	Малі	Мікро	Разом
Кількість суб’єктів господарювання, що підпадають під дію регулювання (розробники засобів КЗІ та експертні заклади), одиниць	14	19	-	-	33
Питома вага групи у загальній кількості, відсотків	42%	58%	-	-	100%

Вид альтернативи	Вигоди	Витрати
Альтернатива 1 Прийняття проєкту Наказу	Прийняття проєкту Наказу матиме такий вплив на інтереси суб’єктів господарювання: забезпечення відповідності засобів КЗІ вимогам національних стандартів у сфері захисту інформації, гармонізованих з міжнародними; можливість реалізації у засобах КЗІ нових технологій (криптографічних алгоритмів та протоколів), що запроваджуються новими стандартами.	Оскільки проєктом Технічного регламенту засобів КЗІ передбачено перехідний період у застосуванні введених в експлуатацію засобів КЗІ протягом терміну дії відповідного йому позитивного експертного висновку за результатами державної експертизи у сфері КЗІ, а також право розробника самостійно вибирати нормативні документи з переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах КЗІ, додаткові витрати не передбачені.
Альтернатива 2 Відсутність регулювання	Відсутність регулювання означає залишення існуючого стану справ, що не передбачає жодних вигод для суб’єктів господарювання	Втрата міжнародного ринку через зниження конкурентноспроможності засобів КЗІ.

IV. Вибір найбільш оптимального альтернативного способу досягнення цілей

За результатами аналізу альтернативних способів досягнення цілей державного регулювання здійснено вибір оптимального альтернативного способу з урахуванням системи бальної оцінки ступеня досягнення визначених цілей.

Бал результативності визначається за чотирибальною системою оцінки ступеня досягнення визначених цілей державного регулювання.

Рейтинг результативності (досягнення цілей під час вирішення проблеми)	Бал результативності (за чотирибальною системою оцінки)	Коментарі щодо присвоєння відповідного бала
Альтернатива 1 Прийняття проєкту Наказу	4	Цілі прийняття регуляторного акта можуть бути досягнуті повною мірою (проблема більше існувати не буде). Прийняття проєкту Наказу сприятиме: забезпеченню відповідності засобів КЗІ вимогам національних стандартів у сфері захисту інформації, гармонізованих з міжнародними; реалізації у засобах КЗІ нових технологій (криптографічних алгоритмів та протоколів), що запроваджуються новими стандартами.
Альтернатива 2 Відсутність регулювання	1	Цілі прийняття регуляторного акта не можуть бути досягнуті (проблема продовжить існувати). Відсутність регулювання передбачає залишення існуючого стану справ та призведе до невідповідності вітчизняних засобів КЗІ вимогам міжнародних стандартів у сфері захисту інформації, що підвищує ризик порушення захисту інформації, що може завдати збитків володільцю інформації. Також знижується конкурентноспроможність вітчизняних засобів КЗІ по відношенню до іноземних.

Рейтинг результативності	**Вигоди (підсумок)**	**Витрати (підсумок)**	**Обґрунтування відповідного місця альтернативи у рейтингу**
1. Прийняття проекту наказу	Підвищення рівня безпеки засобів КЗІ	Додаткових витрат не потребує	Проблема більше існувати не буде
2. Залишення існуючої ситуації без змін	Немає	Додаткових витрат не потребує	Проблема продовжує існувати

V. Механізми та заходи, які забезпечать розв’язання визначеної проблеми

Основним механізмами, які забезпечують розв’язання визначеної проблеми, є оновлення Переліку.

VI. Оцінка виконання вимог регуляторного акта залежно від ресурсів, якими розпоряджаються органи виконавчої влади чи органи місцевого

самоврядування, фізичні та юридичні особи, які повинні проваджувати або виконувати ці вимоги

З огляду на те, що питома вага суб'єктів малого підприємництва (малих та мікропідприємств разом) у загальній кількості суб'єктів господарювання, на яких поширюється регулювання, не перевищує 10 відсотків розрахунок витрат на запровадження державного регулювання для суб'єктів малого підприємництва не проводився.

Бюджетні витрати на адміністрування регулювання для суб'єктів великого і середнього підприємництва не передбачаються.

VII. Обґрунтування запропонованого строку дії регуляторного акта

Строк дії проєкту Наказу не обмежений у часі.

Зміна строку дії проєкту Наказу можлива у разі прийняття змін до нього, прийняття змін до нормативно-правових актів, що мають вищу юридичну силу, які стосуються цієї сфери регулювання, або визнання зазначених актів такими, що втратили чинність

Проєктом Наказу передбачено набирання чинності з 1 січня 2024 року.

VIII. Визначення показників результативності дії регуляторного акта

Показники результативності дії регуляторного акта:

кількість розробників засобів КЗІ;

кількість засобів КЗІ, що мають документ про відповідність Технічному регламенту засобів КЗІ;

кількість засобів КЗІ, що мають позитивний експертний висновок за результатами державної експертизи у сфері КЗІ;

рівень поінформованості суб'єктів господарювання (високий, оскільки проєкт Наказу розміщено на офіційному вебсайті Держспецзв'язку).

IX. Визначення заходів, за допомогою яких здійснюватиметься відстеження результативності дії регуляторного акта

Відповідно до законодавства здійснюється базове, повторне та періодичне відстеження результативності регуляторного акта у строки, встановлені статтею 10 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності».

Базове відстеження результативності проєкту Наказу буде здійснюватися через рік після набрання чинності зазначеним Наказом, оскільки планується використовувати статистичний метод відстеження та статистичні дані.

Повторне відстеження планується здійснити через рік після проведення базового відстеження на основі порівняння показників базового та повторного відстеження.

Періодичні відстеження планується здійснювати раз на три роки, починаючи з дня проведення повторного відстеження. Установлені показники результативності акта порівнюватимуться із значеннями аналогічних показників, що встановлені під час повторного відстеження.

Джерело даних: статистичні дані, отримані від Національного агентства з акредитації України та в рамках надання Адміністрацією Держспецзв'язку адміністративної послуги щодо видачі ліцензії на провадження діяльності у сфері КЗІ та видачі позитивного експертного висновку за результатами державної експертизи у сфері КЗІ.

Виконавець заходів з відстеження результативності проєкту Наказу – Адміністрація Держспецзв'язку.

Голова Служби **Юрій ЩИГОЛЬ**

«___» _____ 2023 року

ПРОЄКТ

Прим. № ___

АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ’ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Н А К А З

м. Київ

____ _____ 20____року №_____

Про внесення змін до Переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації

Відповідно до пункту 24 частини першої статті 14 Закону України «Про Державну службу спеціального зв’язку та захисту інформації України», підпункту 7 пункту 4, пункту 10 Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03 вересня 2014 року № 411, з метою приведення переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації у відповідність до вимог законодавства у сфері технічного регулювання та стандартизації

НАКАЗУЮ:

1. Внести зміни до Переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації, затвердженого наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 27 жовтня 2020 року № 687, зареєстрованого у Міністерстві юстиції України 21 грудня 2020 року за № 1272/35555, виклавши його у новій редакції, що додається.

2. Директору Департаменту захисту інформації Адміністрації Державної служби спеціального зв’язку та захисту інформації України забезпечити подання цього наказу в установленому порядку на державну реєстрацію до Міністерства юстиції України.

3. Цей наказ набирає чинності з 01 січня 2024 року.

4. Контроль за виконанням цього наказу покласти на заступника Голови Державної служби спеціального зв’язку та захисту інформації України згідно з розподілом обов’язків.

Голова Служби
бригадний генерал Юрій ЩИГОЛЬ

ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України 27 жовтня 2020 року № 687

(у редакції наказу Адміністрації Державної служби спеціального зв’язку та захисту інформації України
від _____ № _____)

**Перелік стандартів та технічних специфікацій,
дозволених для реалізації в засобах криптографічного захисту інформації**

I. Стандарти, що визначають вимоги до блокових шифрів (block ciphers)

1. ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення»

2. ДСТУ ISO/IEC 18033-3:2015 (ISO/IEC 18033-3:2010/Amd 1:2021, IDT) «Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 3. Блокові шифри»

ДСТУ ISO/IEC 18033-3:2015 (ISO/IEC 18033-3:2010, IDT)/Зміна № 1:2023 (ISO/IEC 18033-3:2010/Amd 1:2021, IDT) «Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 3. Блокові шифри»

3. ДСТУ ГОСТ 28147:2009 «Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования».

4. ДСТУ ISO/IEC 10116:2019 (ISO/IEC 10116:2017/Amd 1:2021, IDT) «Інформаційні технології. Методи захисту. Режими роботи n-бітних блокових шифрів»

ДСТУ ISO/IEC 10116:2019 (ISO/IEC 10116:2017, IDT)/Зміна № 1:2023 (ISO/IEC 10116:2017/Amd 1:2021, IDT) «Інформаційні технології. Методи захисту. Режими роботи n-бітних блокових шифрів»

5. ДСТУ ISO/IEC 18033-7:2023 (ISO/IEC 18033-7:2022, IDT) Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 7. Настроювані блокові шифри»

6. ДСТУ ISO/IEC 19772:2022 (ISO/IEC 19772:2020, IDT) «Інформаційна безпека. Автентифіковане шифрування»

II. Стандарти, що визначають вимоги до потокових шифрів (stream ciphers)

1. ДСТУ 8845:2019 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення»

2. ДСТУ ISO/IEC 18033-4:2015 (ISO/IEC 18033-4:2011/Amd 1:2020, IDT) «Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 4. Потокові шифри»

ДСТУ ISO/IEC 18033-4:2015 (ISO/IEC 18033-4:2011, IDT)/Зміна № 1:2023 (ISO/IEC 18033-4:2011/Amd 1:2020, IDT) «Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 4. Потокові шифри»

III. Стандарти, що визначають вимоги до асиметричних криптографічних алгоритмів та методів (asymmetric algorithms and techniques)

1. ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння»

2. ДСТУ ISO/IEC 9796-2:2015 (ISO/IEC 9796-2:2010, IDT) «Інформаційні технології. Методи захисту. Схеми цифрового підпису, які забезпечують відновлення повідомлення. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел»

3. ДСТУ ISO/IEC 9796-3:2015 (ISO/IEC 9796-3:2006, IDT) «Інформаційні технології. Методи захисту. Схеми цифрового підпису, які забезпечують відновлення повідомлення. Частина 3. Механізми, що ґрунтуються на дискретному логарифмі»

4. ДСТУ ISO/IEC 14888-2:2015 (ISO/IEC 14888-2:2008/Cor 1:2015, IDT) «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел»

ДСТУ ISO/IEC 14888-2:2015 (ISO/IEC 14888-2:2008, IDT)/Поправка № 1:2023 (ISO/IEC 14888-2:2008/Cor 1:2015, IDT) «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел»

5. ДСТУ ISO/IEC 14888-3:2019 (ISO/IEC 14888-3:2018, IDT) «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми, що ґрунтуються на дискретному логарифмуванні»

6. ДСТУ ISO/IEC 15946-5:2023 (ISO/IEC 15946-5:2022, IDT) «Інформаційні технології. Криптографічні методи на основі еліптичних кривих. Частина 5. Генерування еліптичних кривих»

7. ДСТУ ISO/IEC 18033-2:2015 (ISO/IEC 18033-2:2006, IDT) «Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 2. Асиметричні шифри»

ДСТУ ISO/IEC 18033-2:2015 (ISO/IEC 18033-2:2006, IDT)/Зміна № 1:2023 (ISO/IEC 18033-2:2006/Amd 1:2017, IDT) «Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 2. Асиметричні шифри»

8. ДСТУ ISO/IEC 13888-3:2023 (ISO/IEC 13888-3:2020, IDT) «Інформаційні технології. Неспростовність. Частина 3. Механізми із застосуванням асиметричних методів»

9. ДСТУ ISO/IEC 18033-5:2017 (ISO/IEC 18033-5:2015, IDT) «Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 5. Шифри, що ґрунтуються на ідентифікаційних даних»

ДСТУ ISO/IEC 18033-5:2017/Зміна № 1:2023 (ISO/IEC 18033-5:2015/Amd 1:2021, IDT) «Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 5. Шифри, що ґрунтуються на ідентифікаційних даних»

10. ДСТУ ETSI TR 103 616:2022 (ETSI TR 103 616 V1.1.1 (2021–09), IDT) «Кібербезпека. Квантово-безпечні підписи»

11. ДСТУ ETSI TR 103 823:2022 (ETSI TR 103 823 V1.1.2 (2021–10), IDT) «Кібербезпека. Квантово-безпечне шифрування з відкритим ключем та інкапсуляція ключів»

12. ДСТУ ISO/IEC 18033-6:2022 (ISO/IEC 18033-6:2019, IDT) «Інформаційні технології. Методи убезпечення. Алгоритми шифрування. Частина 6. Гомоморфне шифрування» (з обмеженнями у застосуванні).

Алгоритм визначений пунктом 6.2 ДСТУ ISO/IEC 18033-6:2022 не рекомендується до застосування.

13. ДСТУ 8961:2019 «Інформаційні технології. Криптографічний захист інформації. Алгоритми асиметричного шифрування та інкапсуляції ключів»

14. ДСТУ 9041:2020 «Інформаційні технології. Криптографічний захист інформації. Алгоритм шифрування коротких повідомлень, що ґрунтується на скручених еліптичних кривих Едвардса»

IV. Стандарт, що визначає вимоги до кодів автентифікації повідомлень (message authentication codes)

ДСТУ ISO/IEC 9797-2:2023 (ISO/IEC 9797-2:2021, IDT) «Інформаційні технології. Коди автентифікації повідомлень (MACs). Частина 2. Механізми, що застосовують спеціальну геш-функцію»

V. Стандарти, що визначають вимоги до геш-функцій (hash functions)

1. ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція ґешування»

2. ДСТУ ISO/IEC 10118-2:2015 (ISO/IEC 10118-2:2010; Cor 1:2011, IDT) «Інформаційні технології. Методи захисту. Геш-функції. Частина 2. Геш-функції, що використовують n-бітний блоковий шифр»

3. ДСТУ ISO/IEC 10118-3:2023 (ISO/IEC 10118-3:2018, IDT) «Інформаційні технології. Методи захисту. Геш-функції. Частина 3. Спеціалізовані геш-функції»

4. ДСТУ ISO/IEC 10118-4:2015 (ISO/IEC 10118-4:1998; Cor 1:2014; Amd 1:2014, IDT), IDT) «Інформаційні технології. Методи захисту. Геш-функції. Частина 4. Геш-функції, що використовують модульну арифметику»

5. ГОСТ 34.311-95 «Информационная технология. Криптографическая защита информации. Функция хэширования»

6. ДСТУ ISO/IEC 9797-3:2015 (ISO/IEC 9797-3:2011, IDT) «Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (MACs). Частина 3. Механізми, що використовують універсальну геш-функцію»

ДСТУ ISO/IEC 9797-3:2015 (ISO/IEC 9797-3:2011, IDT)/Зміна № 1:2023 (ISO/IEC 9797-3:2011/Amd1:2020, IDT) «Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (MACs). Частина 3. Механізми, що використовують універсальну геш-функцію»

VI. Стандарти, що визначають вимоги до автентифікації сутності (entity authentication)

1. ДСТУ ISO/IEC 9798-2:2021 (ISO/IEC 9798-2:2019, IDT) «Інформаційні технології. Методи безпеки IT. Автентифікація об’єктів. Частина 2. Механізми, що використовують автентифіковане шифрування»

2. ДСТУ ISO/IEC 9798-3:2021 (ISO/IEC 9798-3:2019, IDT) «Інформаційні технології. Методи безпеки ІТ. Автентифікація об’єктів. Частина 3. Механізми з використанням методу цифрового підпису»

3. ДСТУ ISO/IEC 9798-4:2015 (ISO/IEC 9798-4:1999; Cor 1:2009; Cor 2:2012, IDT) «Інформаційні технології. Методи захисту. Автентифікація об’єктів. Частина 4. Методи, що використовують криптографічну перевірочну функцію»

4. ДСТУ ISO/IEC 9798-5:2015 (ISO/IEC 9798-5:2009, IDT) «Інформаційні технології. Методи захисту. Автентифікація об’єктів. Частина 5. Механізми, що використовують методи нульової обізнаності»

5. ДСТУ ISO/IEC 9798-6:2015 (ISO/IEC 9798-6:2010, IDT) «Інформаційні технології. Методи захисту. Автентифікація об’єктів. Частина 6. Механізми, що використовують ручне передавання даних»

VII. Стандарти, що визначають вимоги до управління ключами (key management)

1. ДСТУ ISO/IEC 11770-2:2019 (ISO/IEC 11770-2:2018, IDT) «Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми із застосуванням симетричних методів»

2. ДСТУ ISO/IEC 11770-3:2023 (ISO/IEC 11770-3:2021, IDT) «Інформаційні технології. Керування ключами. Частина 3. Механізми із застосуванням асиметричних методів»

3. ДСТУ ISO/IEC 11770-4:2019 (ISO/IEC 11770-4:2017, IDT) «Інформаційні технології. Методи захисту. Керування ключами. Частина 4. Механізми, ґрунтовані на нестійких секретах»

ДСТУ ISO/IEC 11770-4:2019 (ISO/IEC 11770-4:2017, IDT)/Зміна № 1:2023 (ISO/IEC 11770-4:2017/Amd 1:2019, IDT) «Інформаційні технології. Методи захисту. Керування ключами. Частина 4. Механізми, ґрунтовані на нестійких секретах»

ДСТУ ISO/IEC 11770-4:2019 (ISO/IEC 11770-4:2017, IDT)/Зміна № 2:2023 (ISO/IEC 11770-4:2017/Amd 2:2021, IDT) «Інформаційні технології. Методи захисту. Керування ключами. Частина 4. Механізми, ґрунтовані на нестійких секретах»

4. ДСТУ ISO/IEC 11770-5:2023 (ISO/IEC 11770-5:2020, IDT) «Інформаційні технології. Керування ключами. Частина 5. Керування груповими ключами»

5. ДСТУ ISO/IEC 11770-6:2018 (ISO/IEC 11770-6:2016, IDT) «Інформаційні технології. Методи захисту. Керування ключами. Частина 6. Утворення ключів»

6. ДСТУ ISO/IEC 11770-7:2023 (ISO/IEC 11770-7:2021, IDT) «Інформаційні технології. Керування ключами. Частина 7. Міждоменний автентифікований обмін ключами на основі пароля»

7. ДСТУ 8961:2019 «Інформаційні технології. Криптографічний захист інформації. Алгоритми асиметричного шифрування та інкапсуляції ключів»

8. ДСТУ ETSI TR 103 823:2022 (ETSI TR 103 823 V1.1.2 (2021–10), IDT) «Кібербезпека. Квантово-безпечне шифрування з відкритим ключем та інкапсуляція ключів»

9. ДСТУ ETSI TR 103 570:2022 (ETSI TR 103 570 V1.1.1 (2017–10), IDT) «Кібербезпека. Квантово-безпечний обмін ключами»

VIII. Стандарти, що визначають вимоги до випадкової генерації біт (random bit generation)

1. ДСТУ ISO/IEC 18031:2015 (ISO/IEC 18031:2011; Cor 1:2014, Amd 1:2017, IDT) «Інформаційні технології. Методи захисту. Генерування випадкових бітів»

ДСТУ ISO/IEC 18031:2015 (ISO/IEC 18031:2011; Cor 1:2014, IDT)/Зміна № 1:2023 (ISO/IEC 18031:2011/Amd 1:2017, IDT) «Інформаційні технології. Методи захисту. Генерування випадкових бітів»

IX. Стандарти, що визначають вимоги до методів встановлення чутливих параметрів безпеки (sensitive security parameter establishment methods)

1. ДСТУ ISO/IEC 11770-2:2019 (ISO/IEC 11770-2:2018, IDT) «Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми із застосуванням симетричних методів»

2. ДСТУ ISO/IEC 11770-3:2023 (ISO/IEC 11770-3:2021, IDT) «Інформаційні технології. Керування ключами. Частина 3. Механізми із застосуванням асиметричних методів»

3. ДСТУ ISO/IEC 18032:2022 (ISO/IEC 18032:2020, IDT) «Інформаційні технології. Методи захисту. Генерування простого числа»

X. Стандарти та технічні специфікації, що визначають вимоги до форматів криптографічних повідомлень

RFC 5652 «Cryptographic Message Syntax (CMS)» з використання криптографічних алгоритмів згідно з RFC 3370 «Cryptographic Message Syntax (CMS) Algorithms» або Технічних специфікацій до RFC 5652

Директор Департаменту захисту інформації
Адміністрації Державної служби спеціального
зв’язку та захисту інформації України
полковник Ігор СТЕЛЬНИК

Прим. № ___

ПОЯСНЮВАЛЬНА ЗАПИСКА
до проєкту наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про внесення змін до Переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації»

1. Мета

Метою прийняття проєкту наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про внесення змін до Переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації» (далі – проєкт наказу) є приведення Переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації (далі – Перелік) у відповідність до вимог законодавства у сфері технічного регулювання та стандартизації.

2. Обґрунтування необхідності прийняття акта

На сьогодні розроблення, виробництво та експлуатація засобів криптографічного захисту інформації (далі – засоби КЗІ) здійснюються відповідно до вимог Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженого наказом Адміністрації Держспецзв'язку від 20 липня 2007 року № 141 (далі – Положення № 141).

Відповідно до пункту 12 розділу ІІ Положення № 141 у засобах КЗІ використовуються криптоалгоритми та криптопротоколи, які є національними стандартами, або ті, на які за результатами експертних досліджень Адміністрацією Держспецзв'язку видано позитивний експертний висновок.

На сьогодні в засобах КЗІ реалізуються криптоалгоритми та криптопротоколи, які є національними стандартами в обсязі функцій безпеки згідно з Переліком.

Водночас деякі національні стандарти, зазначені у Переліку, не є чинними у зв'язку з прийняттям оновлених версій та поправок до них.

Тому виникає потреба у врегулюванні питання актуалізації Переліку шляхом його оновлення та доповнення.

3. Основні положення проєкту акта

Проєктом наказу передбачено викладення Переліку у новій редакції.

4. Правові аспекти

Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»;

Закон України «Про стандартизацію»;

Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженого наказом Адміністрації Держспецзв'язку від 20 липня 2007 року № 141;

Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03 вересня 2014 року № 411;

Перелік стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації, затверджений наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 27 жовтня 2020 року № 687, зареєстрований у Міністерстві юстиції України 21 грудня 2020 року за № 1272/35555.

5. Фінансово-економічне обґрунтування

Реалізація проєкту наказу не потребує фінансування з державного та місцевого бюджетів.

6. Позиція заінтересованих сторін

Проєкт наказу розміщено на вебсайті Держспецзв’язку з метою його громадського обговорення.

Проєкт наказу не стосується питань функціонування місцевого самоврядування, прав та інтересів територіальних громад, місцевого та регіонального розвитку, прав осіб з інвалідністю, функціонування і застосування української мови як державної та не потребує погодження уповноваженими представниками всеукраїнських асоціацій органів місцевого самоврядування, всеукраїнськими громадськими організаціями осіб з інвалідністю, їх спілками.

Проєкт наказу не стосується соціально-трудової сфери та не потребує погодження зі Спільним представницьким органом репрезентативних всеукраїнських об’єднань профспілок на національному рівні та Спільним представницьким органом сторони роботодавців на національному рівні.

Проєкт наказу не стосується сфери наукової та науково-технічної діяльності та не потребує розгляду Науковим комітетом Національної ради з питань розвитку науки і технологій.

7. Оцінка відповідності

Проєкт наказу не стосується зобов’язань України у сфері європейської інтеграції, не містить положень, що стосуються прав та свобод, гарантованих Конвенцією про захист прав людини і основоположних свобод.

Проєкт наказу не містить положень, які порушують принцип рівних прав та можливостей жінок і чоловіків, правил і процедур, пов’язаних з ризиками вчинення корупційних правопорушень та правопорушень, пов’язаних з корупцією, не створює підстав для дискримінації, не стосується інших ризиків та обмежень, які можуть виникнути під час реалізації проєкту наказу.

Громадська антикорупційна, громадська антидискримінаційна та громадська гендерно-правова експертизи проєкту наказу не проводилися.

8. Прогноз результатів

Реалізація проєкту наказу дозволить привести Перелік у відповідність до вимог законодавства у сфері технічного регулювання та стандартизації.

Реалізація проєкту наказу не матиме впливу на ринкове середовище, забезпечення захисту прав та інтересів суб'єктів господарювання, громадян і держави; розвиток регіонів, підвищення чи зниження спроможності територіальних громад; ринок праці, рівень зайнятості населення; громадське здоров'я, покращення чи погіршення стану здоров'я населення або його окремих груп; екологію та навколишнє природне середовище, обсяг природних ресурсів, рівень забруднення атмосферного повітря, води, земель, зокрема забруднення утвореними відходами, інші суспільні відносини.

Вплив на інтереси заінтересованих сторін:

Заінтересована сторона	Вплив реалізації акта на заінтересовану сторону	Пояснення очікуваного впливу
Адміністрація Державної служби спеціального зв'язку та захисту інформації	Позитивний	Забезпечення відповідності засобів КЗІ вимогам національних стандартів у сфері захисту інформації, гармонізованих з міжнародними; створення умов для сумісного використання міжнародних стандартів та вітчизняних криптографічних алгоритмів, забезпечення технологічної нейтральності національних технічних рішень, що використовуються у сфері КЗІ, а також недопущення їх дискримінації.
Суб'єкти господарювання (кваліфіковані надавачі електронних довірчих послуг)	Позитивний	

Голова Державної служби спеціального
зв'язку та захисту інформації України
бригадний генерал Юрій ЩИГОЛЬ
«___»_____2023 року

Державна служба спеціального зв’язку та захисту інформації України

Повідомлення про оприлюднення проєкту наказу Адміністрації Державної служби спеціального зв’язку та захисту інформації України «Про внесення змін до Переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації»

Регуляторна діяльність | Проєкти регуляторних актів

07.07.2023 15:26

1. Стислий виклад змісту проєкту акта

Проєкт наказу Адміністрації Державної служби спеціального зв’язку та захисту інформації України «Про внесення змін до Переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації» (далі – проєкт наказу) розроблено Адміністрацією Держспецзв'язку відповідно до пункту 24 частини першої статті 14 Закону України «Про Державну службу спеціального зв’язку та захисту інформації України», частин першої та другої статті 23 Закону України «Про стандартизацію», підпункту 7 пункту 4, пункту 10 Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03 вересня 2014 року N° 411, з метою приведення переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації у відповідність до вимог законодавства у сфері технічного регулювання та стандартизації.

Проєктом наказу передбачено викладення Переліку у новій редакції.

2. Адреси для зауважень та пропозицій до проєкту акта:

Адміністрації Державної служби спеціального зв’язку та захисту інформації України:
поштова: вул. Солом’янська, 13, м. Київ, 03680;
електронна: info@cip.gov.ua;

Державної регуляторної служби України:
поштова: вул. Арсенальна, 9/11, м. Київ, 01011;
електронна: inform@dkrp.gov.ua

3. Обраний спосіб оприлюднення проєкту акта

Проєкт наказу та аналіз регуляторного впливу розміщено на веб-сайті Держспецзв'язку.

4. Строк, протягом якого приймаються зауваження та пропозиції

Пропозиції та зауваження до проєкту наказу просимо надсилати протягом місяця з дати його оприлюднення.