Прим. № 1

АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

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

19.08.2020 № 04/02/03-2182

Державні органи
(згідно зі списком на розсилку)

Про погодження проєкту наказу
Адміністрації Держспецзв'язку

Надсилаємо на погодження проєкт наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації», підготовлений відповідно до частин першої та другої статті 23 Закону України «Про стандартизацію».

Додатки: 1. Проєкт наказу на 16 арк.
2. Пояснювальна записка та прогноз впливу разом на 5 арк.
3. Аналіз регуляторного впливу проєкту наказу на 7 арк., тільки на першу адресу.
4. Повідомлення про оприлюднення на 1 арк., тільки на першу адресу.

Голова Служби Юрій ЩИГОЛЬ

Вик. Гаврилов Р.В.
281 96 99

0.31

028288

ПРОЄКТ

Прим. № ___

Про затвердження 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», 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 № 411, та з метою приведення нормативно-правових актів криптографічного захисту інформації у відповідність до законодавства

НАКАЗУЮ:

1. Затвердити такі, що додаються:

1) перелік стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації (далі – Перелік);

до н 04/02/03-2182

2) Технічні специфікації до RFC 5652.

2. Установити, що:

1) у засобах криптографічного захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, реалізуються криптоалгоритми та криптопротоколи, які є національними стандартами в обсязі функцій безпеки згідно з Переліком, якщо інше не встановлено нормативно-правовими актами;

2) стандарти, визначені пунктом 3 розділу I та пунктом 5 розділу V Переліку, застосовуються лише для забезпечення сумісності із засобами криптографічного захисту інформації, введеними в експлуатацію до набрання чинності цим наказом.

3. Визнати таким, що втратив чинність, наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 18 грудня 2012 року № 739 «Про затвердження Вимог до форматів криптографічних повідомлень», зареєстрований в Міністерстві юстиції України 14 січня 2013 року за № 108/22640 (зі змінами).

4. 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.

5. Цей наказ набирає чинності з дня його офіційного опублікування.

6. Контроль за виконанням цього наказу покласти на першого заступника Голови Державної служби спеціального зв'язку та захисту інформації України.

Голова Служби Юрій ЩИГОЛЬ

Юрій ЩИГОЛЬ

ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України
__ _____ 20__ року № _____

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, 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, IDT) "Інформаційні технології. Методи захисту. Режими роботи n-бітних блокових шифрів".

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, 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/IEC9796-3:2006, 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, 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 15946-5:2019 (ISO/IEC 15946-5:2017) "Інформаційні технології. Методи захисту. 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".

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

ДСТУ ISO/IEC 9797-2:2015 (ISO/IEC 9797-2:2011, IDT) "Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (MACs). Частина 2. Механізми що використовують спеціалізовану 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 10118-3:2005 (ISO/IEC 10118-3:2004; Cor 1:2011, 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) "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”.

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

1. ДСТУ ISO/IEC 9798-2:2015 (ISO/IEC 9798-2:2008; Cor 3:2013, IDT) “Інформаційні технології. Методи захисту. Автентифікація об’єктів. Частина 2. Механізми, що використовують симетричні алгоритми шифрування”.

2. ДСТУ ISO/IEC 9798-3:2002 (ISO/IEC 9798-3:1998; Cor 1:2009; Cor 2:2012) “Інформаційні технології. Методи захисту. Автентифікація суб’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 11770-2:2015 (ISO/IEC 11770-2:2008; Cor 1:2009, IDT) “Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми з використанням симетричних методів”.

2. ДСТУ ISO/IEC 11770-3:2015 (ISO/IEC 11770-3:2008; Cor 1:2009, IDT) “Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми з використанням асиметричних методів”.

3. ДСТУ ISO/IEC 11770-4:2015 (ISO/IEC 11770-4:2008; Cor 1:2009, IDT) “Інформаційні технології. Методи захисту. Керування ключами. Частина 4. Механізми , засновані на нестійких секретах”.

4. ДСТУ ISO/IEC 11770-5:2015 (ISO/IEC 11770-5:2008, IDT) “Інформаційні технології. Методи захисту. Керування ключами. Частина 5. Керування груповими 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, IDT) “Інформаційні технології. Методи захисту. Генерування випадкових бітів”.

2. ДСТУ ISO/IEC 20543 "Інформаційні технології. Методи захисту. Методи тестування та аналізу для генерування випадкових бітів".

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

1. ДСТУ ISO/IEC 11770-2:2015 (ISO/IEC 11770-2:2008; Cor 1:2009, IDT) "Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми з використанням симетричних методів".

2. ДСТУ ISO/IEC 11770-3:2015 (ISO/IEC 11770-3:2008; Cor 1:2009, IDT) "Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми з використанням асиметричних методів".

X. Стандарти, що визначають вимоги до тестових метрик пом'якшення неінвазійних атак (non-invasive attack mitigation test metrics)

1. ДСТУ ISO/IEC 20085-1 "Методи захисту ІТ. Вимоги до засобів тестування та методів калібрування засобів тестування для застосування у методах тестування пом'якшення неінвазійних атак на криптографічні модулі. Частина 1. Методи та засоби тестування".

2. ДСТУ ISO/IEC 20085-2 "Методи захисту ІТ. Вимоги до засобів тестування та методів калібрування засобів тестування для застосування у методах тестування пом'якшення неінвазійних атак на криптографічні модулі. Частина 2. Методи та прилади тестового калібрування".

XI. 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, затверджених наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від _____ № ___ «Про затвердження переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації», зареєстрованим в Міністерстві юстиції України _____ за № ___.

Т.в.о. директора Департаменту захисту інформації
Адміністрації Державної служби спеціального
зв'язку та захисту інформації України
полковник Ігор СТЕЛЬНИК

ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України
__ _____ 202__ року № _____

ТЕХНІЧНІ СПЕЦИФІКАЦІЇ
до RFC 5652

1. Ці технічні специфікації доповнюють рекомендації Комітету із інженерних питань Інтернету RFC 5652 "Cryptographic Message Syntax (CMS)" (далі RFC 5652) в частині формування повідомлення типу "ContentInfo", що містить дані типу "enveloped-data" ("захищені дані"), з використанням законодавства у сфері електронних довірчих послуг та вітчизняних криптографічних алгоритмів, визначених національними стандартами:

ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння" (далі – ДСТУ 4145-2002);

ДСТУ 7564:2014 "Інформаційні технології. Криптографічний захист інформації. Функція гешування" (далі – ДСТУ 7564:2014);

ДСТУ 7624:2014 "Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення" (далі – ДСТУ 7624:2014);

ДСТУ ГОСТ 28147:2009 "Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования" (далі – ДСТУ ГОСТ 28147:2009);

ГОСТ 34.311-95 "Информационная технология. Криптографическая защита информации. Функция хеширования" (далі – ГОСТ 34.311-95).

2. Доповнення до пункту 6.1 RFC 5652 "EnvelopedData Type"

Номер версії синтаксису, що визначається полем "Version" структури "EnvelopedData", повинен мати значення "2".

3. Доповнення до підпунктів 6.2.2 “KeyAgreeRecipientInfo” та 10.1.3 “KeyEncryptionAlgorithmIdentifier”:

1) під час застосування динамічного механізму узгодження ключів у групі точок еліптичної кривої поле “algorithm” поля “originatorKey” для алгоритму цифрового підпису ДСТУ 4145-2002 може мати такі значення:

для поліноміального базису:

Dstu4145WithDstu7564(256)pb OBJECT IDENTIFIER ::= {iso(1) member-body(2) Ukraine(804) root (2) security(1) cryptography(1) ua-pki (1) alg(1) asym (3) Dstu4145WithDstu7564(6) 256(1) pb(1)};

Dstu4145WithGost34311(pb) OBJECT IDENTIFIER ::= {iso(1) member-body(2) Ukraine(804) root(2) security(1) cryptography(1) ua-pki (1) alg(1) asym (3) Dstu4145WithGost34311(1) pb(1)};

для оптимального нормального базису:

Dstu4145WithDstu7564(256)onb OBJECT IDENTIFIER ::= {iso(1) member-body(2) Ukraine(804) root (2) security(1) cryptography(1) ua-pki (1) alg(1) asym (3) Dstu4145WithDstu7564(6) 256(1) onb(2)};

Dstu4145WithGost34311onb OBJECT IDENTIFIER ::= { iso(1) member-body(2) Ukraine(804) root (2) security(1) cryptography(1) ua-pki (1) alg(1) asym (3) Dstu4145WithGost34311(1) onb(2)};

2) параметри алгоритму поля “algorithm” в “originatorKey” повинні бути ASN.1 NULL;

3) поле “originatorKey publicKey” повинно містити відкритий ключ відправника (маркер), що має такий формат:

PublicKey:: = OCTET STRING, що інкапсулюється в BIT STRING.

Відкритий ключ ДСТУ 4145-2002 – послідовність байтів, яка є елементом основного поля (пункт 5.3 розділу 5 ДСТУ 4145-2002), який є стиснутим зображенням (пункт 6.9 розділу 6 ДСТУ 4145-2002) точки на еліптичній кривій. Розмір зображення в байтах дорівнює m/8, заокруглений до найближчого цілого у більшу сторону;

4) об’єктні ідентифікатори (OID) протоколу узгодження ключа в групі точок еліптичної кривої (ECDH):

з використанням геш-функції ДСТУ 7564:2014:

алгоритм з кофакторним множенням:

id-dhSinglePass-cofactorDH-Dstu7564kdf-scheme OBJECT IDENTIFIER ::= {iso(1) member-body(2) Ukraine(804) root(2) security(1) cryptography(1) ua-pki (1) alg (1) asym (3) dhSinglePass-cofactorDH- Dstu7564kdf (7) };

алгоритм без кофакторного множення:

id-dhSinglePass-stdDH- Dstu7564kdf-scheme OBJECT IDENTIFIER ::= {iso(1) member-body(2) Ukraine(804) root(2) security(1) cryptography(1) ua-pki (1) alg (1) asym (3) dhSinglePass- stdDH- Dstu7564kdf (8) };

з використанням геш-функції ГОСТ 34.311-95:

алгоритм з кофакторним множенням:

id-dhSinglePass-cofactorDH-gost34311kdf-scheme OBJECT IDENTIFIER ::= {iso(1) member-body(2) Ukraine(804) root(2) security(1) cryptography(1) ua-pki (1) alg (1) asym (3) dhSinglePass-cofactorDH-gost34311kdf (4) };

алгоритм без кофакторного множення:

id-dhSinglePass-stdDH-gost34311kdf-scheme OBJECT IDENTIFIER ::= {iso(1) member-body(2) Ukraine(804) root(2) security(1) cryptography(1) ua-pki (1) alg (1) asym (3) dhSinglePass- stdDH-gost34311kdf (5) };

5) параметри протоколу узгодження ключа в групі точок еліптичної кривої повинні бути визначені такою ASN.1 структурою:

```
ECDHParameters ::= SEQUENCE {
q           INTEGER,
FR          INTEGER,
a           INTEGER,
b           INTEGER,
G           ECPoint,
n           INTEGER,
h           INTEGER,
dke         OCTET STRING OPTIONAL},
```

де q – довжина поля (field size) у бітах, що дорівнює степеню основного поля (m);

FR – індикатор представлення поля або зведений поліном (reduction polynomial);

a та b – два елементи поля, які визначають криву (коефіцієнти рівняння еліптичної кривої);

G – базова точка еліптичної кривої (Base Point) з координатами (xG, yG);

n – порядок базової точки (order of the point) G;

h – кофактор, еквівалентний порядку кривої, поділеному на n (для еліптичних кривих з ДСТУ 4145-2002 h = 2 (якщо параметр еліптичної кривої a=1) або h = 4 (якщо параметр еліптичної кривої a=0));

значенням точки еліптичної кривої ECPoint повинен бути рядок байтів, який є закодованою точкою еліптичної кривої:

ECPoint ::= OCTET STRING;

процедура кодування точки (Point-to-Octet-String Conversion):

вхідними даними є точка еліптичної кривої P = (Xp, Yp), яка не є нульовою;

вихідними даними є рядок байтів PO – зображення у нестисненому форматі (uncompressed form) точки P як рядка байтів;

байт PC = 0x04 (ознака нестисненого формату);

результуючий рядок байтів PO повинен бути об'єднанням (конкатенацією): PO = PC || Xp || Yp.

Рядком байтів для представлення нульового елемента групи точок еліптичної кривої O = (0, 0) (infinity) повинен бути один нульовий байт: PO = 0x00;

процедура обчислення FR:

поліномом є примітивний многочлен, що наведений у таблиці 1 ДСТУ 4145-2002. Значенням зведеного полінома є ціле число як рядок бітів;

для оптимального нормального базису FR = 0;

обчислення значення FR для поліноміального базису, де: m – ступінь основного поля, ks[len] – масив цілих чисел ks[0]=k3, ks[1]=k2, ks[2]=k1, що є ступенями примітивного многочлена. Поліном має вигляд x^m + x^k3 + x^k2 + x^k1 + 1, де: m > k3 > k2 > k1 >= 1, len – довжина масиву ks, для тричлена (trinomial) len = 1 та для п'ятичлена (pentanomial) len = 3, якщо len = 1, то k2 = k1 = 0;

для визначення FR як рядка бітів необхідно:

встановити FR = 1 (встановити біт 0);

встановити у FR біт m та відповідно біти k1, k2, k3;

6) при визначенні механізму узгодження ключів повинна виконуватися операція порівняння загальносистемних параметрів "ECDHParameters" покомпонентно (еквівалентність параметрів q, FR) або як порівняння масивів байтів DER-кодованої структури "ECDHParameters". Якщо загальносистемні параметри еквівалентні, застосовується статичний механізм узгодження ключів, в інших випадках – динамічний;

7) формат сертифіката відкритого ключа, призначеного для узгодження симетричного ключа шифрування (далі – сертифікат шифрування), повинен відповідати вимогам законодавства у сфері електронних довірчих послуг.

Сертифікат шифрування повинен мати розширення "використання ключа", що має об'єктний ідентифікатор id-ce-keyUsage OBJECT IDENTIFIER::= {id-ce 15}із значенням "узгодження ключа" ("keyAgreement").

4. Доповнення до підпункту 10.1.4 "ContentEncryptionAlgorithmIdentifier" та пункту 12 "Security Considerations":

1) як алгоритм шифрування даних "contentEncryptionAlgorithm" структури "EncryptedContentInfo" можуть використовуватися алгоритми:

ДСТУ 7624:2014 у режимах "Калина-256/256-OFB" (режим гамування зі зворотним зв'язком за шифротекстом відповідно до розділу 8 ДСТУ 7624:2014) та "Калина-256/256-CFB" (режим гамування зі зворотним зв'язком за шифрограмою відповідно до розділу 11 ДСТУ 7624:2014), які мають такі об'єктні ідентифікатори:

id-Dstu7624ofb(256) OBJECT IDENTIFIER ::= {iso(1) member-body(2) Ukraine(804) root(2) security(1) cryptography(1) ua-pki (1) alg (1) sym (1) dstu7624 (3) ofb (6) 256(2)};

id-Dstu7624cfb(256) OBJECT IDENTIFIER ::= {iso(1) member-body(2) Ukraine(804) root(2) security(1) cryptography(1) ua-pki (1) alg (1) sym (1) dstu7624 (3) cfb (3) 256(2)};

ДСТУ ГОСТ 28147:2009 в режимах "id-gost28147-ofb" (режим гамування, розділ 3 ДСТУ ГОСТ 28147:2009) та "id-gost28147-cfb" (режим гамування зі зворотним зв'язком, розділ 4 ДСТУ ГОСТ 28147:2009), які мають такі об'єктні ідентифікатори:

id-gost28147-ofb OBJECT IDENTIFIER ::= {iso(1) member-body(2) Ukraine(804) root(2) security(1) cryptography(1) ua-pki(1) alg(1) sym(1) gost28147(1) ofb(2)};

id-gost28147-cfb OBJECT IDENTIFIER ::= {iso(1)member-body(2) Ukraine(804) root(2) security(1) cryptography(1) ua-pki(1) alg(1) sym(1) gost28147(1) cfb(3)};

2) параметри алгоритму ДСТУ ГОСТ 28147:2009:

GOST28147Parameters ::= SEQUENCE {
iv OCTET STRING (SIZE (8)),
dke OCTET STRING (SIZE (64)) },

де "iv" – вектор ініціалізації, що обирається випадково;

"dke" – довгостроковий ключовий елемент (ДКЕ) для ДСТУ ГОСТ 28147:2009, що відповідає вимогам Інструкції № 114;

3) параметри алгоритму ДСТУ 7624:2014:

Dstu7624Parameters::= SEQUENCE {
iv OCTET STRING (SIZE (32))},

де "iv" – вектор ініціалізації, що обирається випадково;

4) для шифрування ключових даних чи інших даних, що підлягають захисту, при формуванні "захищених даних" повинен застосовуватися алгоритм захисту ключа шифрування даних "KeyWrapAlgorithm";

5) алгоритм захисту ключа шифрування даних "KeyWrapAlgorithm" ґрунтується на стандарті ДСТУ 7624:2014, що позначається як "Dstu7624Wrap", або ДСТУ ГОСТ 28147:2009, що позначається як "GOST28147Wrap";

6) алгоритм криптографічного перетворення за ДСТУ 7624:2014 застосовується у режимі "Калина-256/256-CFB-256" (гамування зі зворотним зв'язком за шифртекстом відповідно до розділу 8 ДСТУ 7624:2014);

7) алгоритм криптографічного перетворення за ДСТУ ГОСТ 28147:2009 застосовується у режимі CFB (гамування зі зворотним зв'язком відповідно до розділу 4 ДСТУ ГОСТ 28147:2009);

8) алгоритм "KeyWrapAlgorithm", що ґрунтується на стандарті ДСТУ 7624:2014, має такий синтаксис:

Dstu7624WrapParameters ::= CHOICE {
NULL, parameters Dstu7624Parameters},
Dstu7624Parameters::= SEQUENCE {
iv OCTET STRING (SIZE (32))},

де "iv" – вектор ініціалізації, що обирається випадково;

9) алгоритм "KeyWrapAlgorithm", що ґрунтується на стандарті ДСТУ ГОСТ 28147:2009, має такий синтаксис:

GOST28147WrapParameters ::= CHOICE {
NULL, parameters GOST28147Parameters},
GOST28147Parameters ::= SEQUENCE {
iv OCTET STRING (SIZE (8)),
dke OCTET STRING (SIZE (64)) },

де "iv" – вектор ініціалізації, що обирається випадково;

“dke” – довгостроковий ключовий елемент (далі - ДКЕ) відповідно до ДСТУ ГОСТ 28147:2009.

За відсутності ДКЕ в параметрах криптоалгоритму використовується ДКЕ № 1 з переліку ДКЕ, які рекомендуються до застосування у засобах КЗІ, наведеного у додатку 1 до Інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації, затвердженої наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 12 червня 2007 року № 114, зареєстрованої в Міністерстві юстиції України 25 червня 2007 року за № 729/13996 (далі – Інструкція № 114).

Спосіб представлення ДКЕ № 1 повинен відповідати вимогам до технічних засобів, процесів їх створення, використання та функціонування у складі інформаційно-телекомунікаційних систем під час надання кваліфікованих електронних довірчих послуг, встановлених у нормативно-правових актах Мін’юсту та Адміністрації Держспецзв’язку;

10) під час використання “Dstu7624Wrap” або “GOST28147Wrap” як алгоритму захисту ключа шифрування ключів КШК у структурі “захищені дані” (“EnvelopedData”) параметри алгоритму повинні бути NULL.

Значення ДКЕ для алгоритму “GOST28147Wrap” повинно братися з відкритого ключа одержувача;

11) поле “algorithm” повинно містити об’єктний ідентифікатор:

для алгоритму “Dstu7624Wrap”:

id-dstu7624-wrap OBJECT IDENTIFIER ::= { iso(1) member-body(2) Ukraine(804) root(2) security(1) cryptography(1) ua-pki (1) alg (1) sym (1) dstu7624 (3) wrap(11) };

для алгоритму “GOST28147Wrap”:

id-gost28147-wrap OBJECT IDENTIFIER ::= { iso(1) member-body(2) Ukraine(804) root(2) security(1) cryptography(1) ua-pki (1) alg (1) sym (1) gost28147(1) wrap(5) };

12) процес зашифрування (Key Wrap) алгоритму “GOST28147Wrap”

Вхідними даними процесу зашифрування є:

“dke” – довгостроковий ключовий елемент (ДКЕ);

“KEK” – ключ шифрування ключа (КШК);

“CEK” – ключові дані для зашифрування (в операції формування “захищені дані” – ключ шифрування даних КШД).

Вихідними даними процесу зашифрування є “result” – зашифровані ключові дані.

Процес зашифрування виконується за такими етапами:

виконати ініціалізацію алгоритму вхідними даними “dke” та “KEK”;

обчислити контрольну суму ключових даних “CEK”. Контрольна сума ключових даних (позначена як “ICV”) призначена для контролю правильності розшифрування зашифрованих ключових даних та обчислюється як імітовставка довжини 32 біти (“MAC32”) згідно з розділом 5 ДСТУ ГОСТ 28147:2009.

Значення “dke” та ключ під час обчислення “KEK” беруться ті, що встановлені під час виконання етапів процесу зашифрування:

ICV = MAC32(CEK, dke, KEK) [4 байти];

виконати конкатенацію ключових даних з отриманою контрольною сумою:

CEKICV = CEK || ICV;

згенерувати випадкові 8 байтів як вектор ініціалізації (синхропосилка, позначено як "IV");

виконати зашифрування даних "CEKICV" алгоритмом ДСТУ ГОСТ 28147:2009 у режимі гамування зі зворотним зв'язком (GOST28147-CFB), використовуючи "dke" та ключ "KEK", встановлені на кроці 1, і вектор ініціалізації "IV", отриманий за результатами виконання позиції 4 цього пункту:

TEMP1 = GOST28147-CFB_encrypt(CEKICV, IV, dke, KEK).

Довжина вихідних даних "TEMP1" дорівнює довжині "CEKICV";

виконати конкатенацію:

TEMP2 = IV || TEMP1;

виконати реверсне перетворення порядку байтів TEMP2 так, що перший байт TEMP2 стає останнім байтом. Результат перетворення позначимо TEMP3;

зашифрувати TEMP3 алгоритмом ДСТУ ГОСТ 28147:2009 у режимі гамування зі зворотним зв'язком (GOST28147-CFB), використовуючи "dke" та ключ "KEK", встановлені під час виконання позиції 1 цього пункту, та вектор ініціалізації "IV1":

IV1 = 4a dd a2 2c 79 e8 21 05 (4a – молодший байт).

Результатом зашифрування алгоритмом GOST28147Wrap є:

result = GOST28147-CFB_encrypt(TEMP3, IV1, dke, KEK);

13) процес розшифрування (Key Unwrap) алгоритму GOST28147Wrap

Вхідними даними процесу розшифрування є:

"result" – зашифровані ключові дані;

"dke" – довгостроковий ключовий елемент (ДКЕ);

"KEK" – ключ шифрування ключа (КШК).

Вихідними даними процесу розшифрування є:

"CEK" – ключові дані (в операції формування "захищені дані" – ключ шифрування даних КШД).

Процес розшифрування виконується за такими етапами:

виконати ініціалізацію алгоритму вхідними даними "dke" та "KEK". Особливості ініціалізації щодо "dke" наведено у пункті 8.4 глави 8 розділу VI цих Вимог;

виконати розшифрування "result" на алгоритмі ДСТУ ГОСТ 28147:2009 у режимі гамування зі зворотним зв'язком (GOST28147-CFB), використовуючи "dke" та ключ "KEK", встановлені під час виконання етапу, зазначеного у позиції 1 цього пункту, та вектор ініціалізації "IV1":

IV1 = 4a dd a2 2c 79 e8 21 05 (4a – молодший байт);

TEMP3 = GOST28147-CFB_decrypt(result, IV1, dke, KEK);

виконати реверсне перетворення порядку байтів TEMP3 так, що перший байт TEMP3 стає останнім байтом. Результат перетворення позначимо TEMP2;

відокремити складові у TEMP2 (перші 8 байтів – IV, усі інші – TEMP1):

TEMP2 = IV || TEMP1;

виконати розшифрування TEMP1 алгоритмом ДСТУ ГОСТ 28147:2009 у режимі гамування зі зворотним зв'язком (GOST28147-CFB), використовуючи "dke" та ключ "KEK", встановлені під час виконання етапу, зазначеного у позиції 1 цього пункту, та вектор ініціалізації "IV", отриманий за результатами виконання етапу, зазначеного у позиції 3 цього пункту:

CEKICV = GOST28147-CFB_decrypt(TEMP1, IV, dke, KEK);

відокремити складові у CEKICV (останні 4 байти – контрольна сума ICV, усі інші перші – ключові дані CEK):

CEKICV = CEK || ICV;

обчислити контрольну суму ("ICV1") отриманих ключових даних "CEK" як імітовставку довжини 32 біти ("MAC32") згідно з розділом 5 ДСТУ ГОСТ 28147:2009.

Значення "dke" та ключ під час обчислення "KEK" беруться ті, що встановлені під час виконання етапу, зазначеного у позиції 1 цього пункту:

ICV1 = MAC32(CEK, dke, KEK) [4 байти];

порівняти контрольну суму "ICV", отриману за результатами виконання етапу, зазначеного у позиції 6 цього пункту, з контрольною сумою "ICV1", отриманою за результатами виконання етапу, зазначеного у позиції 7 цього пункту.

У разі нееквівалентності зазначених контрольних сум припинити подальше оброблення з результатом "помилка розшифрування ключа".

У разі еквівалентності зазначених контрольних сум повернути як результат розшифрування алгоритму "GOST28147Wrap" отримане значення ключового матеріалу "CEK";

14) під час використання "GOST28147Wrap" як алгоритму захисту ключа шифрування ключів КШК у структурі "захищені дані" ("EnvelopedData") "dke" (довгостроковий ключовий елемент) визначається з параметрів алгоритму відкритого ключа одержувача;

15) процес зашифрування (Key Wrap) алгоритму Dstu7624Wrap

Умовні позначення:

CMAC(T,K) – функція обчислення імітовставки (контрольної суми) за алгоритмом "Калина-256/256-CMAC-256" (розділ 9 ДСТУ 7624:2014) повідомлення T на основі ключа K;

E(T,K,S) – функція шифрування повідомлення T на основі ключа K та синхропосилки S;

D(T,K,S) – функція розшифрування повідомлення T на основі ключа K та синхропосилки S;

REV(T) – функція реверсного перетворення порядку байтів повідомлення T так, що останній байт стає першим;

X||Y – операція конкатенації блоків X та Y;

L(T,N) – функція отримання молодших N-двійкових розрядів повідомлення T;

R(T,N) – функція отримання старших N-двійкових розрядів повідомлення T;

l(T) – функція отримання довжини повідомлення T.

Вхідні параметри:

KEK – ключ шифрування ключа (КШК), двійковий рядок довжиною 256;

CEK – ключові дані для шифрування (в операції формування "захищені дані" – ключ шифрування даних КШД);

IV – синхропосилка, двійковий рядок довжиною 256, генерація здійснюється перед використанням алгоритму;

IV1 – фіксована синхропосилка, двійковий рядок довжиною 256 із значенням "6973271D6E611D06616715046C65504C2020004F6D68011F65610C0 C73734714".

Вихідні параметри:

RES – зашифровані ключові дані.

Алгоритм:

виконати такі обчислення:

ICV = CMAC(CEK,KEK)

CEKICV = CEK||ICV

TEMP1 = E(CEKIV,KEK,IV)

TEMP2 = IV||TEMP1

TEMP3 = REV(TEMP2)

RES = E(TEMP3, KEK,IV1);

16) процес розшифрування (Key Unwrap) алгоритму Dstu7624Wrap

Вхідні параметри:

KEK – ключ шифрування ключа (КШК), двійковий рядок довжиною 256;

RES – зашифровані ключові дані;

IV1 – фіксована синхропосилка, двійковий рядок довжиною 256 із значенням "6973271D6E611D06616715046C65504C2020004F6D68011F65610C0 C73734714".

Вихідні параметри:

CEK – ключові дані для шифрування (в операції формування "захищені дані" – ключ шифрування даних КШД).

Алгоритм:

виконати такі обчислення:

TEMP3 = E(RES,KEK,IV1)

TEMP2 = REV(TEMP3)

IV=L(TEMP2,256)

TEMP1=R(TEMP2,l(TEMP2)−256)

CEKICV = E(TEMP1,KEK,IV)

CEK = L(CEKICV,l(CEKICV)−256)

ICV = R(CEKICV, 256)

ICV1 = CMAC(CEK,KEK).

Порівняти контрольні суми ICV, ICV1. У разі нееквівалентності зазначених контрольних сум припинити подальше оброблення з результатом “помилка розшифрування ключа”.

У разі еквівалентності зазначених контрольних сум повернути як результат розшифрування алгоритму Dstu7624Wrap отримане значення ключового матеріалу *CEK*.

Т.в.о. директора 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 затвердження переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації»

1. Резюме

Метою прийняття наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації» (далі – проєкт Наказу) є приведення нормативно-правових актів Адміністрації Державної служби спеціального зв'язку та захисту інформації України у відповідність до вимог законодавства у сфері технічного регулювання та стандартизації.

2. Проблема, яка потребує роз'яснення

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 (далі – Положення № 141), затвердженого наказом Адміністрації Держспецзв'язку від 20.07.2007 № 141 (далі – Наказ № 141).

Відповідно до пункту 12 розділу II 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.

Частинами першою та другою статті 23 Закону України «Про стандартизацію» визначено, що національні стандарти та кодекси усталеної практики застосовуються безпосередньо чи шляхом посилання на них в інших документах. Національні стандарти та кодекси усталеної практики застосовуються на добровільній основі, крім випадків, якщо обов'язковість їх застосування встановлена нормативно-правовими актами.

Тому потребує врегулювання питання застосування у засобах КЗІ обов'язкових стандартів, що забезпечить відповідність їх суттєвим вимогам технічного регламенту.

Також потребують викладення у новий спосіб, запропонований проєктом Наказу, норми до форматів криптографічних повідомлень.

Так, Вимоги до форматів криптографічних повідомлень (далі - Вимоги), затверджені наказом Адміністрації Держспецзв'язку від 18 грудня 2012 року № 739 «Про затвердження вимог до форматів криптографічних повідомлень» (далі - Наказ № 739), розроблені на основі RFC 5652 «Cryptographic Message Syntax (CMS)».

Проєктом Наказу передбачено застосування RFC 5652 «Cryptographic Message Syntax (CMS)» з технічними специфікаціями щодо використання вітчизняних криптографічних алгоритмів, норми яких ідентичні Вимогам.

3. Суть акта

Проєктом Наказу передбачено затвердження переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації (далі – Перелік).

Водночас надіслано листа до ТК 20 «Інформаційні технології» та ДП «УкрНДНЦ» про необхідність прийняття (перевидання) національних стандартів методом обкладинки, зазначених у пунктах 1, 2 розділу VI, пункті 2 розділу VIII та пунктах 1, 2 розділу X Переліку.

4. Вплив на бюджет

Реалізація Наказу не потребує додаткових матеріальних та інших витрат.

5. Позиція заінтересованих сторін

Прогноз впливу реалізації Наказу на ключові інтереси заінтересованих сторін додається.

За предметом правового регулювання Наказ не стосується:

питань функціонування місцевого самоврядування, прав та інтересів територіальних громад, місцевого та регіонального розвитку;

соціально-трудової сфери;

прав осіб з інвалідністю;

сфери наукової та науково-технічної діяльності.

З метою проведення громадського обговорення проєкт Наказу буде розміщено на офіційному вебсайті Держспецзв'язку.

6. Прогноз впливу

Реалізація Наказу справлятиме вплив на ринкове середовище, забезпечення прав та інтересів суб'єктів господарювання (розробників засобів КЗІ).

З огляду на зазначене відповідно до статті 8 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності» до проєкту Наказу підготовлено аналіз регуляторного впливу.

За предметом правового регулювання проєкт Наказу не матиме впливу на:

розвиток регіонів;

ринок праці;

громадське здоров'я;

екологію та навколишнє природне середовище.

7. Позиція заінтересованих органів

Проєкт Наказу потребує погодження з Міністерством розвитку економіки, торгівлі та сільського господарства України, Міністерством цифрової трансформації України, Державною регуляторною службою, Антимонопольним комітетом України, Національним банком України, Міністерством освіти і науки України, Державним комітетом телебачення та радіомовлення України, Національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації, Державною службою України з питань безпечності харчових продуктів та захисту споживачів, Міністерством фінансів України.

8. Ризики та обмеження

У проєкті Наказу немає положень, що стосуються прав та свобод, гарантованих Конвенцією про захист прав людини і основоположних свобод.

За своєю суттю проєкт Наказу не має впливу на забезпечення рівних прав та можливостей жінок і чоловіків.

У проєкті Наказу не вказано правил і процедур, які можуть містити ризики вчинення корупційних правопорушень.

Проєкт Наказу не потребує проведення громадської антикорупційної експертизи.

У проєкті Наказу немає положень, які містять ознаки дискримінації.

Проєкт Наказу не потребує проведення громадської антидискримінаційної експертизи.

Проєкт Наказу не передбачає надання державної допомоги суб'єктам господарювання, тому дія Закону України «Про державну допомогу суб'єктам господарювання» не поширюється на проєкт Наказу та не поширюється на підтримку суб'єктів господарювання. У зв'язку з цим відповідне рішення Антимонопольного комітету України, передбачене зазначеним Законом, не потребується.

9. Підстава розроблення акта

Проєкт Наказу розроблено на виконання:

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 № 411.

Голова Державної служби спеціального
зв'язку та захисту інформації України
підполковник Юрій ЩИГОЛЬ
«18» 08 2020 року

ПРОГНОЗ ВПЛИВУ

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

1. Суть проєкту акта

Проєкт наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації» спрямовано на приведення нормативно-правових актів Адміністрації Держспецзв'язку у відповідність до вимог законодавства у сфері технічного регулювання та стандартизації.

2. Вплив проєкту акта на ключові інтереси заінтересованих сторін

Заінтересована сторона	Ключовий інтерес	Очікуваний (позитивний чи негативний) вплив на ключовий інтерес із зазначенням передбачуваної динаміки змін основних показників (у числовому або якісному вимірі)		Пояснення (чому саме реалізація акта призведе до очікуваного впливу)
		короткостроковий вплив (до року)	середньостроковий вплив (більше року)	
Громадяни (користувачі засобів КЗІ)	Можливість використання засобів КЗІ, що відповідають сучасним вимогам у сфері захисту інформації	**Очікуваний позитивний вплив:** підвищення рівня довіри до засобів КЗІ	**Очікуваний позитивний вплив:** підвищення рівня довіри до засобів КЗІ	Реалізація акта призведе до забезпечення належного захисту конфіденційної інформації користувачів внаслідок наявності якісних засобів КЗІ
Суб'єкти господарювання (кваліфіковані надавачі електронних довірчих послуг)	Можливість розроблення засобів КЗІ, що відповідають сучасним вимогам у сфері захисту інформації	**Очікуваний позитивний вплив:** 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 шляхом	**Очікуваний позитивний вплив:** 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 шляхом	Частинами першою та другою статті 23 Закону України «Про стандартизацію» визначено, що національні стандарти та кодекси усталеної практики застосовуються безпосередньо чи шляхом посилання на них в інших документах. Національні стандарти та кодекси усталеної практики застосовуються на добровільній основі, крім випадків, якщо обов'язковість їх застосування встановлена нормативно-правовими актами. Відповідно до пункту 12 розділу II Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженого наказом Адміністрації Держспецзв'язку від 20.07.2007 № 141 (далі – Положення № 141) у

		затвердження технічних специфікацій; забезпечення технологічної нейтральності національних технічних рішень, що використовуються у сфері КЗІ, а також недопущення їх дискримінації.	затвердження технічних специфікацій; забезпечення технологічної нейтральності національних технічних рішень, що використовуються у сфері КЗІ, а також недопущення їх дискримінації.	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.
Держава	Взаємоузгодження вимог законодавства, дотримання принципів державної регуляторної політики	**Очікуваний позитивний вплив:** створення умов для розроблення засобів КЗІ відповідно до вимог законодавства у сфері технічного регулювання та оцінки відповідності	**Очікуваний позитивний вплив:** створення умов для розроблення засобів КЗІ відповідно до вимог законодавства у сфері технічного регулювання та оцінки відповідності	Частинами першою та другою статті 23 Закону України «Про стандартизацію» визначено, що національні стандарти та кодекси усталеної практики застосовуються безпосередньо чи шляхом посилання на них в інших документах. Національні стандарти та кодекси усталеної практики застосовуються на добровільній основі, крім випадків, якщо обов'язковість їх застосування встановлена нормативно-правовими актами. Відповідно до пункту 12 розділу II 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.

АНАЛІЗ РЕГУЛЯТОРНОГО ВПЛИВУ
проєкту наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації»

І. Визначення проблеми

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 (далі – Положення № 141), затвердженого наказом Адміністрації Держспецзв'язку від 20.07.2007 № 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.

Частинами першою та другою статті 23 Закону України «Про стандартизацію» визначено, що національні стандарти та кодекси усталеної практики застосовуються безпосередньо чи шляхом посилання на них в інших документах. Національні стандарти та кодекси усталеної практики застосовуються на добровільній основі, крім випадків, якщо обов'язковість їх застосування встановлена нормативно-правовими актами.

Тому потребує врегулювання питання застосування у засобах КЗІ обов'язкових стандартів, що забезпечить відповідність їх суттєвим вимогам технічного регламенту.

Також потребують викладення у новий спосіб запропонований проєктом Наказу норми до форматів криптографічних повідомлень.

Так, Вимоги до форматів криптографічних повідомлень (далі - Вимоги), затверджені наказом Адміністрації Держспецзв'язку від 18 грудня 2012 року № 739 «Про затвердження вимог до форматів криптографічних повідомлень» (далі - Наказ № 739), розроблені на основі RFC 5652 «Cryptographic Message Syntax (CMS)».

Проєктом Наказу передбачено застосування RFC 5652 «Cryptographic Message Syntax (CMS)» з технічними специфікаціями щодо використання вітчизняних криптографічних алгоритмів, норми яких ідентичні Вимогам.

Основними показниками, що характеризують обсяги ринку засобів КЗІ, призначених для захисту конфіденційної інформації, є:

кількість розробників засобів КЗІ;

кількість засобів КЗІ, що мають чинні експертні висновки у сфері КЗІ;

кількість щорічно виданих експертних висновків на засоби КЗІ за останні 6 років.

На цей час провадять діяльність з розроблення засобів КЗІ 12 суб'єктів господарювання.

Протягом останніх 6 років видано 203 експертних висновки за результатами державної експертизи у сфері КЗІ, що в середньому становить 34 висновки на рік:

Рік	2014	2015	2016	2017	2018	2019	2014-2019
Кількість програмних засобів КЗІ	15	11	14	19	6	9	74
Кількість програмно-апаратних засобів КЗІ	39	23	20	7	17	23	129
Загальна кількість	54	34	34	26	23	32	203

Основні групи (підгрупи), на які проблема справляє вплив:

Групи (підгрупи)	Так	Ні
Громадяни		+
Держава		+
Суб'єкти господарювання	+	
у тому числі суб'єкти малого підприємництва		+

II. Цілі державного регулювання

Проєкт Наказу розроблено з метою приведення нормативно-правових актів Адміністрації Держспецзв'язку у відповідність до вимог законодавства у сфері технічного регулювання та стандартизації.

III. Визначення та оцінка альтернативних способів досягнення цілей

1. Визначення альтернативних способів

Під час розробки проєкту Наказу було розглянуто такі альтернативні способи досягнення визначених цілей державного регулювання:

Вид альтернативи	Опис альтернативи
Альтернатива 1 Прийняття проєкту Наказу	Прийняття проєкту Наказу передбачає продовження реформи законодавства у сфері КЗІ шляхом приведення у відповідність до вимог Закону України «Про технічні регламенти та оцінку відповідності». Так, проєктом Наказу пропонується: 1) унормувати застосування розробниками засобів КЗІ стандартів під час розроблення засобів КЗІ; 2) визнати таким, що втратив чинність, Наказ № 739.
Альтернатива 2	Відсутність регулювання передбачає залишення існуючого стану справ та зупинення реформи законодавства у сфері КЗІ, зокрема:

Відсутність регулювання	1) невстановлення вимог до функцій безпеки засобів КЗІ; 2) порушення вимог Законів України «Про технічні регламенти та оцінку відповідності» та «Про стандартизацію».

2. Оцінка вибраних альтернативних способів досягнення цілей

Оцінка впливу на сферу інтересів суб'єктів господарювання

Показник	Великі	Середні	Малі	Мікро	Разом
Кількість суб'єктів господарювання, що підпадають під дію регулювання, одиниць	0	12	0	0	12
Питома вага групи у загальній кількості, відсотків	0	100	0	0	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; створення умов для сумісного використання міжнародних стандартів та вітчизняних криптографічних алгоритмів шляхом затвердження технічних специфікацій; забезпечення технологічної нейтральності національних технічних рішень, що використовуються у сфері КЗІ, а також недопущення їх дискримінації.	Оскільки розробник має право 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	Додаткові витрати на розроблення власних технічних специфікацій та забезпечення сумісності 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	Прийняття проєкту Наказу сприятиме: забезпеченню відповідності засобів КЗІ вимогам національних стандартів у сфері захисту інформації, гармонізованих з міжнародними; створенню умов для сумісного використання міжнародних стандартів та вітчизняних криптографічних алгоритмів шляхом затвердження технічних специфікацій; забезпеченню технологічної нейтральності національних технічних рішень, що використовуються у сфері КЗІ, а також недопущенню їх дискримінації.
Альтернатива 2 Відсутність регулювання	1	Відсутність регулювання передбачає залишення існуючого стану справ та зупинення реформи законодавства у сфері криптографічного захисту інформації, що 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
Альтернатива 1 Прийняття проєкту Наказу	Прийняття проєкту Наказу сприятиме: забезпеченню відповідності засобів КЗІ вимогам національних стандартів у сфері захисту інформації, гармонізованих з міжнародними; створенню умов для сумісного використання міжнародних стандартів	Витрат немає	Продовження реформи законодавства у сфері електронного цифрового підпису з метою забезпечення належного рівня захисту інформації та персональних

	та вітчизняних криптографічних алгоритмів шляхом затвердження технічних специфікацій; забезпеченню технологічної нейтральності національних технічних рішень, що використовуються у сфері КЗІ, а також недопущенню їх дискримінації.		даних в процесі здійснення електронного документообігу та електронної ідентифікації, а також створення умов для транскордонної сертифікації зокрема з країнами ЄС
Альтернатива 2 Відсутність регулювання	Відсутність регулювання означає залишення існуючого стану справ, що не передбачає жодних вигод для держави, громадян та суб'єктів господарювання	Можливі витрати	Відсутність регулювання передбачає залишення існуючого стану справ та зупинення реформи законодавства у сфері КЗІ, що може спричинити додаткові витрати володільців інформації (з державного бюджету, громадян, а також збитки для суб'єктів господарювання), пов'язані із порушенням захисту інформації у зв'язку з використанням засобів КЗІ, що реалізують застарілі стандарти

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

Основним механізмами, які забезпечують розв'язання визначеної проблеми, є затвердження переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації (далі – Перелік).

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

Проєкт Наказу набирає чинності з дня його офіційного опублікування.

VIII. Визначення показників результативності дії регуляторного акта

Показники результативності дії регуляторного акта:

кількість розробників 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 провести 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 Державної служби спеціального зв'язку та захисту інформації України підполковник Юрій ЩИГОЛЬ

«18» 08 2020 року

Повідомлення про оприлюднення
проєкту наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації»

1. Стислий виклад змісту проєкту акта

Проєкт наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації» розроблено відповідно до частини першої та другої статті 23 Закону України «Про стандартизацію» з метою приведення нормативно-правових актів Адміністрації Державної служби спеціального зв'язку та захисту інформації України у відповідність до вимог законодавства у сфері технічного регулювання та стандартизації.

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@dsszzi.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 вебсайті Держспецзв'язку.

4. Строк, протягом якого приймаються зауваження та пропозиції

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

Голова Державної служби спеціального
зв'язку та захисту інформації України
підполковник Юрій ЩИГОЛЬ

«18» 08 2020 р.

ДР № 04/02/03-2182