Прим. № 1

ДЕРЖАВНА СЛУЖБА 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

17.11.17 № 04/02/03-2964

Державна регуляторна служба України
вул. Арсенальна, 9/11, м. Київ, 01011

Щодо погодження проекту наказу

З метою удосконалення вимог законодавства України у сфері захисту інформації Адміністрацією Державної служби спеціального зв'язку та захисту інформації України (далі – Адміністрація Держспецзв'язку) розроблено проект наказу «Про затвердження Змін до Вимог до форматів криптографічних повідомлень».

Просимо погодити проект наказу Адміністрації Держспецзв'язку згідно положень статті 21 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності».

Додатки:
1. Проект наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Змін до Вимог до форматів криптографічних повідомлень», № 04/02/03-2954 від 17.11.2017, прим. № 2 на 24 арк.;
2. Порівняльна таблиця до проекту наказу, № 04/02/03-2955 від 17.11.2017, прим. № 2 на 22 арк.
3. Аналіз регуляторного впливу до проекту наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Змін до Вимог до форматів криптографічних повідомлень», № 04/02/03-2958 від 17.11.2017, прим. № 1 на 8 арк.;
4. Повідомлення про оприлюднення проекту нормативно-правового акта, № 04/02/03-2959 від 17.11.2017, прим. № 1 на 1 арк.

Перший заступник Голови Служби О.М. Чаузов

прим. №2

ПРОЕКТ

АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Н А К А З

м. Київ

___.___.2017 № ____

Про затвердження Змін до Вимог до форматів криптографічних повідомлень

Відповідно до підпункту 2 пункту 3 Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 3 вересня 2014 року № 411, та з метою удосконалення законодавства у сфері електронного цифрового підпису

НАКАЗУЮ:

1. Затвердити Зміни до Вимог до форматів криптографічних повідомлень, затверджених наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 18 грудня 2012 року № 739, зареєстрованих у Міністерстві юстиції України 14 січня 2013 року за № 108/22640, що додаються.

2. Директору Департаменту захисту інформації Адміністрації Державної служби спеціального зв'язку та захисту інформації України у п'ятиденний строк після підписання цього наказу в установленому порядку забезпечити його подання на державну реєстрацію до Міністерства юстиції України.

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

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

Голова Служби Л.О. Євдоченко

Л.О. Євдоченко

ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України
___ _____ 2017 року № ___

Зміни

до Вимог до форматів криптографічних повідомлень

1. Розділ I викласти в такій редакції:

"1.1. Ці Вимоги визначають синтаксис (формат представлення) криптографічних повідомлень (зашифрованих даних) в електронній формі, а також протоколи узгодження ключів для засобів криптографічного захисту інформації (далі – КЗІ) та надійних засобів електронного цифрового підпису (далі – ЕЦП).

1.2. Положення цих Вимог є обов'язковими для засобів криптографічного захисту інформації (далі – КЗІ) та надійних засобів електронного цифрового підпису (далі – ЕЦП), призначених для забезпечення конфіденційності інформації з використанням сертифіката шифрування. Правильність реалізації у засобах КЗІ та надійних засобах ЕЦП, наведених у цих Вимогах форматів і протоколів, повинна бути підтверджена сертифікатом відповідності або позитивним експертним висновком за результатами державної експертизи у сфері криптографічного захисту інформації.

1.3. У цих Вимогах терміни вживаються у таких значеннях:

дані – повідомлення або частина повідомлення, яке не обробляють чи не змінюють у процесі обробки;

механізм узгодження ключа – статичний (Static-Static mode) або динамічний (Ephemeral-Static mode) механізм узгодження ключа, що визначений у цих Вимогах;

повідомлення "захищені дані" – повідомлення, що містить цифровий конверт;

протокол узгодження ключа – протокол Діффі-Геллмана обчислення ключа шифрування ключа (КШК) у циклічній групі поля або в групі точок еліптичної кривої;

симетричний ключ сеансу або ключ шифрування даних (КШД) – ключ сеансу, на якому здійснюється шифрування даних за визначеним у цих Вимогах алгоритмом криптографічного перетворення;

узгоджений ключ ("key agreement") або ключ шифрування ключа (КШК) – симетричний ключ, на якому здійснюється шифрування симетричного ключа сеансу;

цифровий конверт ("enveloped-data") – зашифровані дані типу "дані" ("data") або "підписані дані" ("signed-data") разом із зашифрованим симетричним ключем.

Інші терміни вживаються у значеннях, наведених у Законі України "Про електронний цифровий підпис", Порядку акредитації центру сертифікації ключів, затвердженому постановою Кабінету Міністрів України від 13 липня 2004 року № 903, Правилах посиленої сертифікації, затверджених наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13 січня 2005 року № 3, зареєстрованих у Міністерстві юстиції України 27 січня 2005 року за № 104/10384 (із змінами).

1.4. У цих Вимогах скорочення мають такі значення:

CMS – синтаксис криптографічного повідомлення (Cryptographic Message Syntax);

DH – протокол узгодження ключів Діффі-Геллмана (Diffie-Hellman), що базується на криптографічних перетвореннях у полі Галуа; може використовуватися також позначення FFC DH (Finite Field Cryptography Diffie-Hellman);

ECDH – протокол Діффі-Геллмана (Diffie-Hellman), що базується на криптографічних перетвореннях у групі точок еліптичної кривої; може використовуватися також позначення ECC DH (Elliptic Curve Cryptography Diffie-Hellman);

ДКЕ – довгостроковий ключовий елемент.

1.5. Ці Вимоги базуються на рекомендаціях Комітету із інженерних питань Інтернету RFC 3370 "Cryptographic Message Syntax (CMS) Algorithms", August 2002 (далі – RFC 3370); RFC 3852 "Cryptographic Message Syntax (CMS)", July 2004 (далі – RFC 3852); RFC 5652 "Cryptographic Message Syntax (CMS)", September 2009 (далі – RFC 5652), національному стандарті України ДСТУ ISO/IEC 11770-3:2015 "Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми із застосуванням асиметричних методів" (далі – ДСТУ ISO/IEC 11770-3:2015) та встановлюють особливості застосування в них криптографічних алгоритмів, визначених стандартами ГОСТ 34.310-95 "Информационная технология. Криптографическая защита информации. Процессы выработки и проверки электронной цифровой подписи на базе ассиметричного криптографического алгоритма" (далі – ГОСТ 34.310-95), ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння" (далі – ДСТУ 4145-2002), ДСТУ ГОСТ 28147:2009 "Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования" (далі – ДСТУ ГОСТ 28147:2009), ДСТУ 7624:2014 "Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення" (далі – ДСТУ 7624:2014), ДСТУ ISO/IEC 10118-3:2015 "Інформаційні технології. Методи захисту.

Геш-функції. Частина 3. Спеціалізовані геш-функції" (далі – ДСТУ ISO/IEC 10118-3:2015).

При застосуванні міжнародних алгоритмів ЕЦП застосовуються вимоги RFC 3370, RFC 3852, RFC 5652, ISO/IEC 11770-3, ISO/IEC 10118-3.

1.6. Якщо у Вимогах є розбіжності з RFC 3370, RFC 3852, RFC 5652 та ДСТУ ISO/IEC 11770-3:2015, то застосовуються положення цих Вимог.

1.7. Обмеження та рекомендації щодо застосування довжин ключів у криптографічних повідомленнях "захищені дані" визначаються чинним законодавством.

1.8. Ці Вимоги розроблено з урахуванням 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), Вимог до формату посиленого сертифіката відкритого ключа, затверджених наказом Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 серпня 2012 року № 1236/5/453, зареєстрованих у Міністерстві юстиції України 20 серпня 2012 року за № 1398/21710 (далі – Вимоги до формату посиленого сертифіката відкритого ключа), Вимог до формату списку відкликаних сертифікатів, затверджених наказом Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 серпня 2012 року № 1236/5/453, зареєстрованих у Міністерстві юстиції України 20 серпня 2012 року за № 1400/21712 (далі – Вимоги до формату списку відкликаних сертифікатів), Вимог до формату підписаних даних, затверджених наказом Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 серпня 2012 року № 1236/5/453,

зареєстрованих у Міністерстві юстиції України 20 серпня 2012 року за № 1401/21713 (далі – Вимоги до формату підписаних даних).

1.9. У цих Вимогах повинні застосовуватися криптографічні алгоритми, що застосовуються у Вимогах до формату посиленого сертифіката відкритого ключа. Режими роботи криптографічних алгоритмів встановлюються цими Вимогами.".

2. У розділі II:

пункт 2.5 викласти в такій редакції:

"2.5. Повідомлення, що містить цифровий конверт, має тип даних "enveloped-data" ("захищені дані"). Повідомлення типу "захищені дані" входять у повідомлення типу "ContentInfo".

Об'єктний ідентифікатор

id-envelopedData OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 3}

вказує на те, що структура "ContentInfo" містить дані типу "захищені дані".

Приклади ASN.1 структури "захищені дані" розміщуються на офіційному веб-сайті Державної служби спеціального зв'язку та захисту інформації України.";

абзац другий пункту 2.6 розділу II виключити.

3. У главі 3 розділу III:

у пункті 3.2:

абзац перший підпункту 3.2.1 викласти в такій редакції:

"3.2.1. Статичний механізм узгодження ключів ("Static-Static mode") – узгодження ключів за протоколом Діффі-Геллмана, при якому як відправник,

так і одержувач мають статичну ключову пару, відкритий ключ якої засвідчено в акредитованому центрі сертифікації ключів.";

абзац перший підпункту 3.2.2 викласти в такій редакції:

"3.2.2. При динамічному механізмі узгодження ключа для формування узгодженого ключа відправник повинен використовувати особистий сеансовий ключ відправника і відкритий ключ одержувача. Одержувач повинен використовувати особистий ключ одержувача і відкритий сеансовий ключ відправника, що отримується від відправника, при кожному сеансі в полі "originatorKey" структури "RecipientInfo".";

у пункті 3.7:

підпункт 3) підпункту 3.7.4 викласти в такій редакції:

"3) ідентифікаційні дані відправника:

при застосуванні статичного механізму узгодження ключів Діффі-Геллмана як ідентифікатора відправника повинні використовуватися ім'я емітента сертифіката (центру сертифікації) та серійний номер сертифіката відкритого ключа відправника "issuerAndSerialNumber" або ідентифікатор відкритого ключа відправника "subjectKeyIdentifier";

при застосуванні динамічного механізму узгодження ключів Діффі-Геллмана як ідентифікаційних даних відправника застосовується його відкритий сеансовий ключ (маркер), що генерується відправником та міститься в полі "originatorKey";

при застосуванні динамічного механізму узгодження ключів у циклічній групі поля поле "algorithm" в "originatorKey" повинно мати таке значення:

Gost34310WithGost34311 OBJECT IDENTIFIER ::= { iso(1) member-body(2) Ukraine(804) root (2) security(1) cryptography(1) ua-pki (1) alg(1) asym(3) Gost34310WithGost34311(2)}.

Відповідно до RFC 3370 параметрів алгоритму поля "algorithm" в "originatorKey" не повинно бути.

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

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

Відкритий ключ ГОСТ 34.310-95 кодується як ціле відповідно до Вимог до формату посиленого сертифіката відкритого ключа.

При застосуванні 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)} .

Параметри алгоритму поля “algorithm” в “originatorKey” повинні бути ASN.1 NULL.

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 – це 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.";

у підпункті 3.7.5:

абзац другий підпункту 3) після цифр "34.311-95" доповнити словами та цифрами "Информационная технология. Криптографическая защита информации. Функция хеширования" (далі – ГОСТ 34.311-95)".

підпункт 4) викласти в такій редакції:

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

з використанням геш-функції ДСТУ 7564:2014 "Інформаційні технології. Криптографічний захист інформації. Функція гешування" (далі – 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) };

з використанням відповідно до ДСТУ ISO/IEC 10118-3:2015, ISO/IEC 10118-3 геш-функцій SHA-1 (тільки для розшифрування даних, шифрування яких здійснювалось до 01 січня 2014 року), SHA-224, SHA-256, SHA-384, SHA-512:

алгоритми з кофакторним множенням:

“id-dhSinglePass-cofactorDH-sha1kdf-scheme”;

“id-dhSinglePass-cofactorDH-sha224kdf-scheme”;

“id-dhSinglePass-cofactorDH-sha256kdf-scheme”;

“id-dhSinglePass-cofactorDH-sha384kdf-scheme”;

“id-dhSinglePass-cofactorDH-sha512kdf-scheme”;

алгоритми без кофакторного множення:

“id-dhSinglePass-stdDH-sha1kdf-scheme”;

“id-dhSinglePass-stdDH-sha224kdf-scheme”;

“id-dhSinglePass-stdDH-sha256kdf-scheme”;

“id-dhSinglePass-stdDH-sha384kdf-scheme”;

“id-dhSinglePass-stdDH-sha512kdf-scheme”;

dhSinglePass-cofactorDH-sha1kdf-scheme OBJECT IDENTIFIER ::= { iso(1) identified-organization(3) tc68(133) country(16) x9(840) x9-63(63) chemes(0) 3};

dhSinglePass-cofactorDH-sha224kdf-scheme OBJECT IDENTIFIER ::= {iso(1) identified-organization(3) certicom(132) schemes(1) 14 0 };

dhSinglePass-cofactorDH-sha256kdf-scheme OBJECT IDENTIFIER ::= {iso(1) identified-organization(3) certicom(132) schemes(1) 14 1 };

dhSinglePass-cofactorDH-sha384kdf-scheme OBJECT IDENTIFIER ::= {iso(1) identified-organization(3) certicom(132) schemes(1) 14 2 };

dhSinglePass-cofactorDH-sha512kdf-scheme OBJECT IDENTIFIER ::= {iso(1) identified-organization(3) certicom(132) schemes(1) 14 3 };

dhSinglePass-stdDH-sha1kdf-scheme OBJECT IDENTIFIER ::= { iso(1) identified-organization(3) tc68(133) country(16) x9(840) x9-63(63) chemes(0) 2};

dhSinglePass-stdDH-sha224kdf-scheme OBJECT IDENTIFIER ::= {iso(1) identified-organization(3) certicom(132) schemes(1) 11 0 };

dhSinglePass-stdDH-sha256kdf-scheme OBJECT IDENTIFIER ::= {iso(1) identified-organization(3) certicom(132) schemes(1) 11 1 };

dhSinglePass-stdDH-sha384kdf-scheme OBJECT IDENTIFIER ::= {iso(1) identified-organization(3) certicom(132) schemes(1) 11 2 };

dhSinglePass-stdDH-sha512kdf-scheme OBJECT IDENTIFIER ::= {iso(1) identified-organization(3) certicom(132) schemes(1) 11 3 };

протоколи узгодження ключа, визначені ідентифікаторами згідно з позицією 4 підпункту 3.7.5 пункту 3.7 глави 3 розділу IV цих Вимог, застосовуються як для статичного, так і для динамічного механізму узгодження ключа. При цьому ознакою динамічного механізму є не нульове значення поля “originatorKey” відповідно до абзацу третього позиції 3 підпункту 3.7.4 пункту 3.7 глави 3 розділу IV цих Вимог;

протоколи узгодження ключа, а саме ZZ-функція та KDF-функція, у групі точок еліптичної кривої визначені у розділі V цих Вимог.”.

4. У розділі V:

главу 2 викласти в такій редакції:

“2. Протокол узгодження ключа Діффі-Геллмана, що виконується відправником:

отримати параметри відкритого ключа одержувача (із сертифіката відкритого ключа);

у разі наявності сертифіката відкритого ключа відправника порівняти параметри відкритого ключа відправника з параметрами відкритого ключа одержувача;

у разі еквівалентності параметрів установити статичний механізм узгодження ключа, в іншому випадку встановити динамічний механізм узгодження ключа та виконати обчислення ключової пари, використовуючи алгоритм та відповідні параметри ключа одержувача;

виконати обчислення спільного секрету (ZZ) для визначеного протоколу в циклічній групі поля або в групі точок еліптичної кривої;

виконати обчислення ключа шифрування ключа КШК (KDF – Key Derivation Function).";

пункт 5.3 глави 5 викласти в такій редакції:

"5.3. Перетворення елемента поля Z на рядок байтів ZZ.

Для використання у функціях формування ключа (KDF-функціях) спільного секрету Z, отриманого згідно з пунктом 5.1 глави 5 розділу V та абзацом четвертим пункту 5.2 глави 5 розділу V цих Вимог, необхідно перетворити елемент поля Z на рядок байтів ZZ (Field-Element-to-Octet-String Conversion). Таке перетворення повинно виконуватися так:

Нехай Z є елементом поля Fq чи поля F(2m). Результатом перетворення є рядок байтів ZZ довжини L.

Якщо Z є елементом поля Fq, то воно є додатним цілим числом, тобто двійковим (бітовим) рядком (bit string). У цьому випадку L дорівнює значенню log(q)/8, заокругленому в більшу сторону до найближчого цілого числа, де log – логарифм за основою 2. Якщо Z є елементом поля F(2m), то воно є двійковим (бітовим) рядком довжини m, що є зображенням додатного цілого числа у системі числення за основою 2. У цьому випадку L дорівнює значенню m/8, заокругленому в більшу сторону до найближчого цілого числа. Позначимо ціле число від Z як ZI.

Виконати перетворення цілого ZI на рядок байтів ZZ у форматі Big-Endian. Одержаний рядок ZZ повинен мати довжину L байтів; при перетворенні старші нульові байти числа ZI не повинні відкидатися. Перетворення цілого ZI на рядок байтів ZZ у форматі Little-Endian наведено у підпункті 3.14.2 пункту 3.14 розділу III Вимог до формату посиленого сертифіката відкритого ключа. Формат Big-Endian має зворотний порядок байтів щодо формату Little-Endian.

При прямому розміщенні байтів (Big-Endian) старший повинен зберігатися за найменшою адресою (як байт з найменшим індексом байт-масиву), а при зворотному розміщенні (Little-Endian) – за найбільшою, тобто за найменшою адресою повинен розміщуватися молодший байт.

Приклади перетворення елемента поля на рядок байтів у форматі Big-Endian, обчислення спільного секрету ZZ у циклічній групі простого поля та у групі точок еліптичної кривої розміщуються на офіційному веб-сайті Державної служби спеціального зв'язку та захисту інформації України.";

у главі 6:

у пункті 6.3:

у підпункті 1) слова та цифри "(додаток А.2. Функція формування ключа ANSI X9.42)" виключити;

підпункт 7) викласти у такій редакції:

"7) Приклади обчислення ключа КШК у циклічній групі поля розміщуються на офіційному веб-сайті Державної служби спеціального зв'язку та захисту інформації України.";

у пункті 6.4:

у підпункті 1) слова та цифри "(додаток А.3. Функція формування ключа ANSI X9.63)" виключити;

підпункт 3) викласти в такій редакції:

"3) структура "SharedInfo":

```
SharedInfo ::= SEQUENCE {
keyInfo          AlgorithmIdentifier,
entityUInfo      [0] EXPLICIT OCTET STRING OPTIONAL,
suppPubInfo      [2] EXPLICIT OCTET STRING};";
```

в абзаці третьому підпункту 4) слова "довжина "partyAInfo" замінити словами "довжина "entityUInfo";

у підпункті 5) слово "partyAInfo" замінити словом "entityUInfo";

підпункт 6) викласти у такій редакції:

“6) Приклади обчислення ключа КШК в групі точок еліптичної кривої розміщуються на офіційному веб-сайті Державної служби спеціального зв’язку та захисту інформації України.”.

5. Розділ VI викласти в такій редакції:

“VI. Алгоритм захисту ключа шифрування даних “KeyWrapAlgorithm”

1. 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”.

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).

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).

2. Призначення алгоритму “KeyWrapAlgorithm”

Алгоритм “KeyWrapAlgorithm” призначений для шифрування ключових даних чи інших даних, що підлягають захисту, та забезпечення цілісності зашифрованих ключових даних.

3. Ідентифікатор алгоритму захисту ключа шифрування даних “KeyWrapAlgorithm” вказується як параметр поля “EnvelopedData RecipientInfos KeyAgreeRecipientInfo keyEncryptionAlgorithm” згідно з позицією 1 підпункту 3.7.5 пункту 3.7 глави 3 розділу IV цих Вимог.

4. Ключ узгодження КШК формується за алгоритмами узгодження ключа DH або ECDH:

KeyWrapAlgorithm ::= AlgorithmIdentifier.

5. Синтаксис “KeyWrapAlgorithm”

5.1. 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.

5.2. 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 (ДКЕ) відповідно до ДСТУ ГОСТ 28147:2009.

6. При використанні "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.

Використання "Dstu7624Wrap" або "GOST28147Wrap" з параметрами алгоритму, що не є NULL, не є предметом цих Вимог.

7. 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) }.

8. Алгоритми "GOST28147Wrap" та "Dstu7624Wrap"

8.1. Усі структури, які задіяні в процесах зашифрування (пункти 8.2, 8.5 глави 8 розділу VI цих Вимог) і розшифрування (пункти 8.3, 8.6 глави 8 розділу VI цих Вимог), повинні бути представлені у форматі Little-Endian.

8.2. 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" – це 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". Особливості ініціалізації щодо "dke" наведено у пункті 8.4 глави 8 розділу VI цих Вимог;

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 при обчисленні “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”, що 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”, що 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).

8.3. 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” – це 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”, що 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 – це IV, усі інші – це 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”, що 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 – це контрольна сума ICV, усі інші перші – це 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 при обчисленні “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”.

8.4. При використанні “GOST28147Wrap” як алгоритму захисту ключа шифрування ключів КШК у структурі “захищені дані” (“EnvelopedData”) “dke” (довгостроковий ключовий елемент) визначається з параметрів алгоритму відкритого ключа одержувача.

Якщо значення “dke” немає в параметрах алгоритму відритого ключа, то повинно братися за умовчанням значення ДКЕ № 1 Переліку ДКЕ, які рекомендуються до застосування у засобах КЗІ, наведеному у додатку 1 до Інструкції № 114.

8.5. 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* таким чином, 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" – це ключ шифрування даних КШД);

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

IV1 – фіксована синхропосилка, двійковий рядок довжиною 256 із значенням "6973271D6E611D06616715046C65504C2020004F6D68011F65610C0C73734714".

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).

8.6. 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" – це 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*.

9. Приклади обчислення імітовставки за ДСТУ 7624:2014 та за ДСТУ ГОСТ 28147:2009 розміщуються на офіційному веб-сайті Державної служби спеціального зв'язку та захисту інформації України.

10. Приклади обчислення GOST28147Wrap та Dstu7624Wrap розміщуються на офіційному веб-сайті Державної служби спеціального зв'язку та захисту інформації України.".

6. Розділ VII викласти в такій редакції:

“VII. Алгоритм захисту даних (повідомлення) “contentEncryptionAlgorithm”

7.1. Об’єктні ідентифікатори алгоритмів шифрування даних

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 по шифротексту відповідно до розділу 8 ДСТУ 7624:2014) та “Калина-256/256-CFB” (режим гамування зі зворотним зв’язком по шифрограмі 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)}.

7.2. 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.

7.3. Параметри алгоритму ДСТУ 7624:2014

Dstu7624Parameters::= SEQUENCE {

iv OCTET STRING (SIZE (32))},

де “iv” – вектор ініціалізації, що обирається випадково.”.

7. Пункти 8.2, 8.3 розділу VIII виключити.

8. У тексті Вимог до форматів криптографічних повідомлень (далі – Вимоги) слова та цифри “ДСТУ ГОСТ 28147:2009” замінити словами та цифрами “ДСТУ ГОСТ 28147:2009”.

9. У тексті Вимог слова та цифри “ДСТУ ISO/IEC 11770-3:2002” замінити словами та цифрами “ДСТУ ISO/IEC 11770-3:2015”.

10. У тексті Вимог слова та цифри “ДСТУ ISO/IEC 15946-3:2006” замінити словами та цифрами “ДСТУ ISO/IEC 11770-3:2015”.

Директор Департаменту захисту інформації
Адміністрації Державної служби спеціального
зв’язку та захисту інформації України А.І. Пушкарьов

04/02/03-2954
14.11.12

Прим. № 2

ПОРІВНЯЛЬНА ТАБЛИЦЯ

до проекту наказу Адміністрації Держспецзв'язку «Про затвердження Змін до Вимог до форматів криптографічних повідомлень»

Зміст положення (норми) чинного законодавства	Зміст положення (норми) проекту акта
ДСТУ ГОСТ 28147-2009	**ДСТУ ГОСТ 28147:2009**
ДСТУ ISO/IEC 11770-3:2002	**ДСТУ ISO/IEC 11770-3:2015**
ДСТУ ISO/IEC 15946-3:2006	**ДСТУ ISO/IEC 11770-3:2015**
I. Загальні положення	
1.1. Ці Вимоги визначають синтаксис (формат представлення) криптографічних повідомлень (зашифрованих даних) в електронній формі, а також протоколи, **які повинні застосовуватися для цього синтаксису з метою** узгодження ключів. **Установлення єдиних форматів криптографічних повідомлень має на меті визначення технічних умов щодо забезпечення сумісності засобів криптографічного захисту інформації різних розробників.**	1.1. Ці Вимоги визначають синтаксис (формат представлення) криптографічних повідомлень (зашифрованих даних) в електронній формі, а також протоколи **узгодження ключів для засобів криптографічного захисту інформації (далі – КЗІ) та надійних засобів електронного цифрового підпису (далі – ЕЦП).**
1.2. Положення цих Вимог є обов'язковими для засобів криптографічного захисту інформації (далі – КЗІ) та надійних засобів електронного цифрового підпису (далі – ЕЦП), **що використовуються в системах електронного документообігу.** Правильність реалізації у засобах КЗІ та ЕЦП наведених у цих Вимогах форматів і протоколів повинна бути підтверджена позитивним експертним висновком за результатами державної експертизи у сфері криптографічного захисту інформації.	1.2. Положення цих Вимог є обов'язковими для засобів КЗІ та надійних засобів ЕЦП, **призначених для забезпечення конфіденційності інформації з використанням сертифіката шифрування.** Правильність реалізації у засобах КЗІ та надійних засобах ЕЦП, наведених у цих Вимогах форматів і протоколів, повинна бути підтверджена сертифікатом відповідності або позитивним експертним висновком за результатами державної експертизи у сфері криптографічного захисту інформації.
1.3. У цих Вимогах терміни вживаються у таких значеннях: ... симетричний ключ сеансу або ключ шифрування даних (КШД) – ключ сеансу, на якому здійснюється шифрування даних за алгоритмом, **визначеним у ДСТУ ГОСТ 28147-2009;** ...	1.3. У цих Вимогах терміни вживаються у таких значеннях: ... симетричний ключ сеансу або ключ шифрування даних (КШД) – ключ сеансу, на якому здійснюється шифрування даних за **визначеним у цих Вимогах** алгоритмом **криптографічного перетворення;** ...

Продовження таблиці

Зміст положення (норми) чинного законодавства	Зміст положення (норми) проекту акта
1.5. Ці Вимоги розроблено з урахуванням 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); Вимог до формату посиленого сертифіката відкритого ключа, затверджених наказом Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 серпня 2012 року № 1236/5/453, зареєстрованих у Міністерстві юстиції України 20 серпня 2012 року за № 1398/21710 (далі – Вимоги до формату посиленого сертифіката відкритого ключа); Вимог до формату списку відкликаних сертифікатів, затверджених наказом Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 серпня 2012 року № 1236/5/453, зареєстрованих у Міністерстві юстиції України 20 серпня 2012 року за № 1400/21712 (далі – Вимоги до формату списку відкликаних сертифікатів); Вимог до формату підписаних даних, затверджених наказом Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 серпня 2012 року № 1236/5/453, зареєстрованих у Міністерстві юстиції України 20 серпня 2012 року за № 1401/21713 (далі – Вимоги до формату підписаних даних); ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння" (далі – ДСТУ 4145-2002); ДСТУ ISO/IEC 11770-3:2002 "Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми із застосуванням асиметричних методів" (далі – ДСТУ ISO/IEC 11770-3:2002);	**1.5. Ці Вимоги базуються на рекомендаціях Комітету із інженерних питань Інтернету RFC 3370 «Cryptographic Message Syntax (CMS) Algorithms», August 2002 (далі – RFC 3370); RFC 3852 «Cryptographic Message Syntax (CMS)», July 2004 (далі – RFC 3852); RFC 5652 «Cryptographic Message Syntax (CMS)», September 2009 (далі – RFC 5652), національному стандарті України ДСТУ ISO/IEC 11770-3:2015 "Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми із застосуванням асиметричних методів" (далі – ДСТУ ISO/IEC 11770-3:2015) та встановлюють особливості застосування в них криптографічних алгоритмів, визначених стандартами ГОСТ 34.310-95 "Информационная технология. Криптографическая защита информации. Процессы выработки и проверки электронной цифровой подписи на базе ассиметричного криптографического алгоритма" (далі – ГОСТ 34.310-95),** **ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння" (далі – ДСТУ 4145-2002), ДСТУ ГОСТ 28147:2009 "Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования" (далі – ДСТУ ГОСТ 28147:2009), ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення» (далі – ДСТУ 7624:2014), ДСТУ ISO/IEC 10118-3:2015 "Інформаційні технології. Методи захисту. Геш-функції. Частина 3. Спеціалізовані геш-функції" (далі – ДСТУ ISO/IEC 10118-3:2015).** **При застосуванні міжнародних алгоритмів ЕЦП застосовуються вимоги RFC 3370, RFC 3852, RFC 5652, ISO/IEC 11770-3, ISO/IEC 10118-3.**

Продовження таблиці

Зміст положення (норми) чинного законодавства	Зміст положення (норми) проекту акта
ДСТУ ISO/IEC 15946-3:2006 "Інформаційні технології. Методи захисту. Криптографічні методи, що ґрунтуються на еліптичних кривих. Частина 3. Установлення ключів" (далі – ДСТУ ISO/IEC 15946-3:2006); ДСТУ ГОСТ 28147-2009 "Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования" (далі – ДСТУ ГОСТ 28147-2009); ДСТУ ISO/IEC 10118-3:**2005** "Інформаційні технології. Методи захисту. Геш-функції. Частина 3. Спеціалізовані геш-функції" (далі – ДСТУ ISO/IEC 10118-3:**2015**); ГОСТ 34.310-95 "Информационные технологии. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе ассиметричного криптографического алгоритма" (далі – ГОСТ 34.310-95); ГОСТ 34.311-95 "Информационная технология. Криптографическая защита информации. Функция хеширования" (далі – ГОСТ 34.311-95); RFC 2631 "Diffie-Hellman Key Agreement Method", June 1999 (далі – RFC 2631); RFC 3370 "Cryptographic Message Syntax (CMS) Algorithms", August 2002 (далі – RFC 3370); RFC 3852 "Cryptographic Message Syntax (CMS)", July 2004 (далі – RFC 3852); RFC 5652 "Cryptographic Message Syntax (CMS)", September 2009 (далі – RFC 5652).	
1.6. Якщо у Вимогах є розбіжності з нормативними документами, зазначеними у пункті 1.5 цього розділу, то застосовуються положення цих Вимог.	1.6. Якщо у Вимогах є розбіжності з **RFC 3370, RFC 3852, RFC 5652 та ДСТУ ISO/IEC 11770-3:2015**, то застосовуються положення цих Вимог.

Продовження таблиці

Зміст положення (норми) чинного законодавства	Зміст положення (норми) проекту акта
-	1.8. Ці Вимоги розроблено з урахуванням 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); Вимог до формату посиленого сертифіката відкритого ключа, затверджених наказом Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 серпня 2012 року № 1236/5/453, зареєстрованих у Міністерстві юстиції України 20 серпня 2012 року за № 1398/21710 (далі – Вимоги до формату посиленого сертифіката відкритого ключа); Вимог до формату списку відкликаних сертифікатів, затверджених наказом Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 серпня 2012 року № 1236/5/453, зареєстрованих у Міністерстві юстиції України 20 серпня 2012 року за № 1400/21712 (далі – Вимоги до формату списку відкликаних сертифікатів); Вимог до формату підписаних даних, затверджених наказом Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 серпня 2012 року № 1236/5/453, зареєстрованих у Міністерстві юстиції України 20 серпня 2012 року за № 1401/21713 (далі – Вимоги до формату підписаних даних).
-	1.9. У цих Вимогах повинні застосовуватися криптографічні алгоритми, що застосовуються у Вимогах до формату посиленого сертифіката відкритого ключа. Режими роботи криптографічних алгоритмів встановлюються цими Вимогами.

Продовження таблиці

Зміст положення (норми) чинного законодавства	Зміст положення (норми) проекту акта
II. Типи повідомлень	
2.5. Повідомлення, що містить цифровий конверт, має тип даних “enveloped-data” (“захищені дані”). Повідомлення типу “захищені дані” входять у повідомлення типу “ContentInfo”. Об’єктний ідентифікатор id-envelopedData OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 3} вказує на те, що структура “ContentInfo” містить дані типу “захищені дані”. **Приклад ASN.1 структури “захищені дані” наведено в додатку 1 до цих Вимог.**	2.5. Повідомлення, що містить цифровий конверт, має тип даних “enveloped-data” (“захищені дані”). Повідомлення типу “захищені дані” входять у повідомлення типу “ContentInfo”. Об’єктний ідентифікатор id-envelopedData OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 3} вказує на те, що структура “ContentInfo” містить дані типу “захищені дані”. **Приклади ASN.1 структури “захищені дані” розміщуються на офіційному веб-сайті Державної служби спеціального зв’язку та захисту інформації України.**
2.6. Криптографічне повідомлення “захищені дані” містить у собі інші типи повідомлень, а саме: “дані” (“data”) або “підписані дані” (“signed-data”)”. **При внесенні в криптографічне повідомлення “захищені дані” повідомлення типу “дані” автентифікація відправника цих даних не забезпечується, якщо використовується динамічний механізм узгодження ключів. Динамічний механізм узгодження ключів наведено у підпункті 3.2.2 пункту 3.2 глави 3 розділу III цих Вимог. При внесенні в повідомлення “захищені дані” повідомлення типу “підписані дані” завжди забезпечується автентифікація відправника цих даних.**	2.6. Криптографічне повідомлення “захищені дані” містить у собі інші типи повідомлень, а саме: “дані” (“data”) або “підписані дані” (“signed-data”)”.
III. Процедура формування та розкриття «захищених даних»	
3.2.1. Статичний механізм узгодження ключів (“Static-Static mode”) – узгодження ключів за протоколом Діффі-Геллмана, при якому як відправник, так і одержувач мають статичну ключову пару, відкритий ключ якої засвідчено в акредитованому центрі сертифікації ключів. Тим самим цей статичний механізм забезпечує автентифікацію відправника повідомлення типу “захищені дані”.	**3.2.1. Статичний механізм узгодження ключів (“Static-Static mode”) – узгодження ключів за протоколом Діффі-Геллмана, при якому як відправник, так і одержувач мають статичну ключову пару, відкритий ключ якої засвідчено в акредитованому центрі сертифікації ключів.**

Продовження таблиці

Зміст положення (норми) чинного законодавства	Зміст положення (норми) проекту акта
Статичний механізм узгодження ключів може використовуватися лише у випадку, коли параметри криптографічного алгоритму статичної ключової пари відправника еквівалентні параметрам криптографічного алгоритму статичної ключової пари одержувача. Якщо зазначені параметри не еквівалентні, повинен застосовуватися динамічний механізм узгодження ключів. При статичному механізмі узгодження ключа для формування узгодженого ключа відправник повинен використовувати особистий ключ відправника та відкритий ключ одержувача. Одержувач повинен використовувати особистий ключ одержувача та відкритий ключ відправника. Відкриті ключі відправника та одержувача обираються із посилених сертифікатів відкритих ключів (сертифікатів шифрування).	Статичний механізм узгодження ключів може використовуватися лише у випадку, коли параметри криптографічного алгоритму статичної ключової пари відправника еквівалентні параметрам криптографічного алгоритму статичної ключової пари одержувача. Якщо зазначені параметри не еквівалентні, повинен застосовуватися динамічний механізм узгодження ключів. При статичному механізмі узгодження ключа для формування узгодженого ключа відправник повинен використовувати особистий ключ відправника та відкритий ключ одержувача. Одержувач повинен використовувати особистий ключ одержувача та відкритий ключ відправника. Відкриті ключі відправника та одержувача обираються із посилених сертифікатів відкритих ключів (сертифікатів шифрування).
3.2.2. **Динамічний механізм узгодження ключів ("Ephemeral-Static mode") – узгодження ключів за протоколом Діффі-Геллмана, при якому одержувач має статичну ключову пару, відкритий ключ якої зазначено у посиленому сертифікаті відкритого ключа, а відправник генерує нову (сеансову/динамічну) ключову пару для кожного повідомлення і посилає відкритий ключ цієї пари одержувачу, використовуючи поле "originatorKey" структури "RecipientInfo".** При цьому параметри криптографічного алгоритму динамічної ключової пари відправника повинні бути еквівалентні параметрам криптографічного алгоритму статичної ключової пари одержувача. При динамічному механізмі узгодження ключа для формування узгодженого ключа відправник повинен використовувати особистий ключ відправника і відкритий ключ одержувача. Одержувач повинен використовувати особистий ключ одержувача і відкритий ключ відправника, що отримується від відправника, при кожному сеансі у полі "originatorKey" структури "RecipientInfo".	3.2.2. **При динамічному механізмі узгодження ключа для формування узгодженого ключа відправник повинен використовувати особистий сеансовий ключ відправника і відкритий ключ одержувача. Одержувач повинен використовувати особистий ключ одержувача і відкритий сеансовий ключ відправника, що отримується від відправника, при кожному сеансі в полі "originatorKey" структури "RecipientInfo".** При цьому параметри криптографічного алгоритму динамічної ключової пари відправника повинні бути еквівалентні параметрам криптографічного алгоритму статичної ключової пари одержувача. При динамічному механізмі узгодження ключа для формування узгодженого ключа відправник повинен використовувати особистий ключ відправника і відкритий ключ одержувача. Одержувач повинен використовувати особистий ключ одержувача і відкритий ключ відправника, що отримується від відправника, при кожному сеансі у полі "originatorKey" структури "RecipientInfo".

Продовження таблиці

Зміст положення (норми) чинного законодавства	Зміст положення (норми) проекту акта
Особливості кодування параметрів протоколу узгодження ключа визначено у главі 4 розділу V цих Вимог. Протокол узгодження ключів Діффі-Геллмана в циклічній групі поля використовується для ключових пар (відправника та одержувача), що відповідають ГОСТ 34.310-95 (але тільки за умови використання в режимі з довжиною модуля Р 1024). Протокол узгодження ключів Діффі-Геллмана в групі точок еліптичної кривої використовується для ключових пар (відправника та одержувача), що відповідають ДСТУ 4145-2002.	Особливості кодування параметрів протоколу узгодження ключа визначено у главі 4 розділу V цих Вимог. Протокол узгодження ключів Діффі-Геллмана в циклічній групі поля використовується для ключових пар (відправника та одержувача), що відповідають ГОСТ 34.310-95 (але тільки за умови використання в режимі з довжиною модуля Р 1024). Протокол узгодження ключів Діффі-Геллмана в групі точок еліптичної кривої використовується для ключових пар (відправника та одержувача), що відповідають ДСТУ 4145-2002.
3.7.4. Поля структури "KeyAgreeRecipientInfo": ... 3) ідентифікаційні дані відправника: при застосуванні статичного механізму узгодження ключів Діффі-Геллмана як ідентифікатора відправника повинні використовуватися ім'я емітента сертифіката (центру сертифікації) та серійний номер сертифіката відкритого ключа відправника "issuerAndSerialNumber" або ідентифікатор відкритого ключа відправника "subjectKeyIdentifier"; при застосуванні динамічного механізму узгодження ключів Діффі-Геллмана як ідентифікаційних даних відправника застосовується його відкритий сеансовий ключ (маркер), що генерується відправником та міститься в полі "originatorKey"; при застосуванні динамічного механізму узгодження ключів у циклічній групі поля поле "algorithm" в "originatorKey" повинно мати таке значення: Gost34310WithGost34311 OBJECT IDENTIFIER ::= { iso(1) member-body(2) Ukraine(804) root (2) security(1) cryptography(1) ua-pki (1) alg(1) asym(3) Gost34310WithGost34311(2)}. Відповідно до RFC 3370 параметрів алгоритму поля "algorithm" в "originatorKey" не повинно бути. Поле "originatorKey publicKey" повинно містити відкритий ключ відправника (маркер), що має такий формат: PublicKey:: = INTEGER, що інкапсулюється в BIT STRING.	3.7.4. Поля структури "KeyAgreeRecipientInfo": ... 3) ідентифікаційні дані відправника: при застосуванні статичного механізму узгодження ключів Діффі-Геллмана як ідентифікатора відправника повинні використовуватися ім'я емітента сертифіката (центру сертифікації) та серійний номер сертифіката відкритого ключа відправника "issuerAndSerialNumber" або ідентифікатор відкритого ключа відправника "subjectKeyIdentifier"; при застосуванні динамічного механізму узгодження ключів Діффі-Геллмана як ідентифікаційних даних відправника застосовується його відкритий сеансовий ключ (маркер), що генерується відправником та міститься в полі "originatorKey"; при застосуванні динамічного механізму узгодження ключів у циклічній групі поля поле "algorithm" в "originatorKey" повинно мати таке значення: Gost34310WithGost34311 OBJECT IDENTIFIER ::= { iso(1) member-body(2) Ukraine(804) root (2) security(1) cryptography(1) ua-pki (1) alg(1) asym(3) Gost34310WithGost34311(2)}. Відповідно до RFC 3370 параметрів алгоритму поля "algorithm" в "originatorKey" не повинно бути. Поле "originatorKey publicKey" повинно містити відкритий ключ відправника (маркер), що має такий формат: PublicKey:: = INTEGER, що інкапсулюється в BIT STRING.

Продовження таблиці

Зміст положення (норми) чинного законодавства	Зміст положення (норми) проекту акта
Відкритий ключ ГОСТ 34.310-95 кодується як ціле відповідно до Вимог до формату посиленого сертифіката відкритого ключа. При застосуванні 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: Dstu4145PBAlgo 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: Dstu4145ONBAlgo 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)}. Параметри алгоритму поля "algorithm" в "originatorKey" повинні бути ASN.1 NULL. 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 – це 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;	Відкритий ключ ГОСТ 34.310-95 кодується як ціле відповідно до Вимог до формату посиленого сертифіката відкритого ключа. При застосуванні 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)} . Параметри алгоритму поля "algorithm" в "originatorKey" повинні бути ASN.1 NULL. 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 – це 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;

Продовження таблиці

Зміст положення (норми) чинного законодавства	Зміст положення (норми) проекту акта
3.7.5. Особливості синтаксису структури "KeyAgreeRecipientInfo": … 3) об'єктні ідентифікатори (OID) протоколу узгодження ключа у циклічній групі поля: протокол узгодження ключа у циклічній групі поля з використанням геш-функції **ГОСТ 34.311-95** позначається через ідентифікатор "id-DH-ua". Протокол узгодження ключа у циклічній групі поля з використанням геш-функції ГОСТ 34.311-95 є обов'язковим алгоритмом, який застосовується як для статичного, так і для динамічного механізму узгодження ключа; при цьому ознакою динамічного механізму є ненульове значення поля "originatorKey" (відповідно до абзацу третього позиції 3 підпункту 3.7.4 пункту 3.7 глави 3 розділу IV цих Вимог): id-DH-ua OBJECT IDENTIFIER ::= { iso(1) member-body(2)Ukraine(804) root(2) security(1) cryptography(1) ua-pki(1)alg (1) asym (3) DH-ua(3) }; для протоколів узгодження ключа у циклічній групі поля з використанням геш-функції SHA-1 відповідно до ДСТУ ISO/IEC 10118-3:2005 та RFC 2631 (тільки для сумісності з реалізаціями засобів КЗІ, що були розроблені до прийняття цих Вимог) використовуються такі ідентифікатори: "id-SSDH" – необов'язковий, застосовується для статичного механізму узгодження ключа; "id-ESDH" – необов'язковий, застосовується для динамічного механізму узгодження ключа; id-SSDH OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) smime(16) alg(3) 10 }; id-ESDH OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) smime(16) alg(3) 5 }; протоколи узгодження ключа, а саме: ZZ-функція та KDF-функція, у циклічній групі поля визначені у розділі V цих Вимог;	3.7.5. Особливості синтаксису структури "KeyAgreeRecipientInfo": … 3) об'єктні ідентифікатори (OID) протоколу узгодження ключа у циклічній групі поля: протокол узгодження ключа у циклічній групі поля з використанням геш-функції **ГОСТ 34.311-95 "Информационная технология. Криптографическая защита информации. Функция хеширования" (далі – ГОСТ 34.311-95)** позначається через ідентифікатор "id-DH-ua". Протокол узгодження ключа у циклічній групі поля з використанням геш-функції ГОСТ 34.311-95 є обов'язковим алгоритмом, який застосовується як для статичного, так і для динамічного механізму узгодження ключа; при цьому ознакою динамічного механізму є ненульове значення поля "originatorKey" (відповідно до абзацу третього позиції 3 підпункту 3.7.4 пункту 3.7 глави 3 розділу IV цих Вимог): id-DH-ua OBJECT IDENTIFIER ::= { iso(1) member-body(2)Ukraine(804) root(2) security(1) cryptography(1) ua-pki (1)alg (1) asym (3) DH-ua(3) }; для протоколів узгодження ключа у циклічній групі поля з використанням геш-функції SHA-1 відповідно до ДСТУ ISO/IEC 10118-3:2005 та RFC 2631 (тільки для сумісності з реалізаціями засобів КЗІ, що були розроблені до прийняття цих Вимог) використовуються такі ідентифікатори: "id-SSDH" – необов'язковий, застосовується для статичного механізму узгодження ключа; "id-ESDH" – необов'язковий, застосовується для динамічного механізму узгодження ключа; id-SSDH OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) smime(16) alg(3) 10 }; id-ESDH OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) smime(16) alg(3) 5 }; протоколи узгодження ключа, а саме: ZZ-функція та KDF-функція, у циклічній групі поля визначені у розділі V цих Вимог;

Продовження таблиці

Зміст положення (норми) чинного законодавства	Зміст положення (норми) проекту акта
4) об'єктні ідентифікатори (OID) протоколу узгодження ключа в групі точок еліптичної кривої (ECDH):	4) об'єктні ідентифікатори (OID) протоколу узгодження ключа в групі точок еліптичної кривої (ECDH):
	з використанням геш-функції ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція гешування» (далі – 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", алгоритм без кофакторного множення "id-dhSinglePass-stdDH-gost34311kdf-scheme": 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) };	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) };
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) };	
з використанням відповідно до ДСТУ ISO/IEC 15946-3:2006, ДСТУ ISO/IEC 10118-3:2005 геш-функцій SHA-1 (тільки для розшифрування даних, шифрування яких здійснювалось до 01 січня 2014 року), SHA-224, SHA-256, SHA-384, SHA-512:	**з використанням відповідно до ДСТУ ISO/IEC 10118-3:2015, ISO/IEC 10118-3** геш-функцій SHA-1 (тільки для розшифрування даних, шифрування яких здійснювалось до 01 січня 2014 року), SHA-224, SHA-256, SHA-384, SHA-512:
алгоритми з кофакторним множенням:	алгоритми з кофакторним множенням:
...	...
алгоритми без кофакторного множення:	алгоритми без кофакторного множення:
...	...

Продовження таблиці

Зміст положення (норми) чинного законодавства	Зміст положення (норми) проекту акта
протоколи узгодження ключа, визначені ідентифікаторами, згідно з **абзацами першим та другим позиції 4** підпункту 3.7.5 пункту 3.7 глави 3 розділу IV цих Вимог, застосовуються як для статичного, так і для динамічного механізму узгодження ключа. При цьому ознакою динамічного механізму є не нульове значення поля "originatorKey" відповідно до абзацу третього позиції 3 підпункту 3.7.4 пункту 3.7 глави 3 розділу IV цих Вимог;	протоколи узгодження ключа, визначені ідентифікаторами згідно з **позицією 4** підпункту 3.7.5 пункту 3.7 глави 3 розділу IV цих Вимог, застосовуються як для статичного, так і для динамічного механізму узгодження ключа. При цьому ознакою динамічного механізму є не нульове значення поля "originatorKey" відповідно до абзацу третього позиції 3 підпункту 3.7.4 пункту 3.7 глави 3 розділу IV цих Вимог;
V. Протокол узгодження ключа Діффі-Геллмана	
2. Протокол узгодження ключа Діффі-Геллмана, що виконується відправником: **отримати параметри ключа відправника та ключа одержувача (із сертифікатів відкритих ключів);** **порівняти параметри ключа відправника з параметрами ключа одержувача;** **у разі еквівалентності параметрів установити статичний механізм узгодження ключа та перейти до кроку, зазначеного в абзаці шостому цього протоколу;** **у разі нееквівалентності параметрів установити динамічний механізм узгодження ключа та відправнику виконати обчислення ключової пари, використовуючи алгоритм та відповідні параметри ключа одержувача;** виконати обчислення спільного секрету (ZZ) для визначеного протоколу в циклічній групі поля або в групі точок еліптичної кривої; виконати обчислення ключа шифрування ключа КШК (KDF – Key Derivation Function).	2. Протокол узгодження ключа Діффі-Геллмана, що виконується відправником: **отримати параметри відкритого ключа одержувача (із сертифіката відкритого ключа);** **у разі наявності сертифіката відкритого ключа відправника порівняти параметри відкритого ключа відправника з параметрами відкритого ключа одержувача;** **у разі еквівалентності параметрів установити статичний механізм узгодження ключа, в іншому випадку встановити динамічний механізм узгодження ключа та виконати обчислення ключової пари, використовуючи алгоритм та відповідні параметри ключа одержувача;** виконати обчислення спільного секрету (ZZ) для визначеного протоколу в циклічній групі поля або в групі точок еліптичної кривої; виконати обчислення ключа шифрування ключа КШК (KDF –Key Derivation Function).
5. Обчислення спільного секрету 5.1. Обчислення спільного секрету у циклічній групі поля (DH) ґрунтується на RFC 2631 та **ДСТУ ISO/IEC 11770-3:2002** і виконується таким чином: ...	5. Обчислення спільного секрету 5.1. Обчислення спільного секрету у циклічній групі поля (DH) ґрунтується на RFC 2631 та **ДСТУ ISO/IEC 11770-3:2015** і виконується таким чином: ...

Продовження таблиці

Зміст положення (норми) чинного законодавства	Зміст положення (норми) проекту акта
5.2. Обчислення спільного секрету в групі точок еліптичної кривої (ECDH). Обчислення спільного секрету з кофакторним множенням у групі точок еліптичної кривої ґрунтується на **ДСТУ ISO/IEC 15946-3:2006.** ...	5.2. Обчислення спільного секрету в групі точок еліптичної кривої (ECDH). Обчислення спільного секрету з кофакторним множенням у групі точок еліптичної кривої ґрунтується на **ДСТУ ISO/IEC 11770-3:2015.** ...
5.3. Перетворення елемента поля Z на рядок байтів ZZ. Для використання у функціях формування ключа (KDF-функціях) спільного секрету Z, отриманого згідно з пунктом 5.1 глави 5 розділу V та абзацом четвертим пункту 5.2 глави 5 розділу V цих Вимог, необхідно перетворити елемент поля Z на рядок байтів ZZ (Field-Element-to-Octet-String Conversion). Таке перетворення повинно виконуватися таким чином: Нехай Z є елементом поля Fq чи поля F(2m). Результатом перетворення є рядок байтів ZZ довжини L. Якщо Z є елементом поля Fq, то воно є додатним цілим числом, тобто двійковим (бітовим) рядком (bit string); якщо Z є елементом поля F(2m), то воно є двійковим (бітовим) рядком довжини m, що є зображенням додатного цілого числа у системі числення за основою 2. Позначимо ціле число від Z як ZI. Виконати перетворення цілого ZI на рядок байтів ZZ у форматі Big-Endian. Перетворення цілого ZI на рядок байтів ZZ у форматі Little-Endian наведено у підпункті 3.14.2 пункту 3.14 розділу III Вимог до формату посиленого сертифіката відкритого ключа. Формат Big-Endian має зворотний порядок байтів щодо формату Little-Endian.	5.3. Перетворення елемента поля Z на рядок байтів ZZ. Для використання у функціях формування ключа (KDF-функціях) спільного секрету Z, отриманого згідно з пунктом 5.1 глави 5 розділу V та абзацом четвертим пункту 5.2 глави 5 розділу V цих Вимог, необхідно перетворити елемент поля Z на рядок байтів ZZ (Field-Element-to-Octet-String Conversion). Таке перетворення повинно виконуватися так: Нехай Z є елементом поля Fq чи поля F(2m). Результатом перетворення є рядок байтів ZZ довжини L. **Якщо Z є елементом поля Fq, то воно є додатним цілим числом, тобто двійковим (бітовим) рядком (bit string). У цьому випадку L дорівнює значенню log(q)/8, заокругленому в більшу сторону до найближчого цілого числа, де log - логарифм за основою 2. Якщо Z є елементом поля F(2m), то воно є двійковим (бітовим) рядком довжини m, що є зображенням додатного цілого числа у системі числення за основою 2. У цьому випадку L дорівнює значенню m/8, заокругленого в більшу сторону до найближчого цілого числа. Позначимо ціле число від Z як ZI.** Виконати перетворення цілого ZI на рядок байтів ZZ у форматі Big-Endian. **Одержаний рядок ZZ повинен мати довжину L байтів; при перетворенні старші нульові байти числа ZI не повинні відкидатися.** Перетворення цілого **ZI** на рядок байтів ZZ у форматі Little-Endian наведено у підпункті 3.14.2 пункту 3.14 розділу III Вимог до формату посиленого сертифіката відкритого ключа. Формат Big-Endian має зворотний порядок байтів щодо формату Little-Endian.

Продовження таблиці

Зміст положення (норми) чинного законодавства	Зміст положення (норми) проекту акта
При прямому розміщенні байтів (Big-Endian) старший повинен зберігатися за найменшою адресою (як байт з найменшим індексом байт-масиву), а при зворотному розміщенні (Little-Endian) – за найбільшою, тобто за найменшою адресою повинен розміщуватися молодший байт.	При прямому розміщенні байтів (Big-Endian) старший повинен зберігатися за найменшою адресою (як байт з найменшим індексом байт-масиву), а при зворотному розміщенні (Little-Endian) – за найбільшою, тобто за найменшою адресою повинен розміщуватися молодший байт.
Приклади перетворення елемента поля на рядок байтів у форматі Big-Endian наведено в додатку 2 до цих Вимог. **Приклад обчислення спільного секрету ZZ у циклічній групі простого поля (FFC DH, ГОСТ 34.310-95, 1024 біти) наведено в додатку 3 до цих Вимог.** **Приклади обчислення спільного секрету ZZ у групі точок еліптичної кривої (ECDH) наведено в додатку 4 до цих Вимог.**	**Приклади перетворення елемента поля на рядок байтів у форматі Big-Endian, обчислення спільного секрету ZZ у циклічній групі простого поля та у групі точок еліптичної кривої розміщуються на офіційному веб-сайті Державної служби спеціального зв'язку та захисту інформації України.**
6. Використання функції формування ключа КШК (KDF-функція) … 6.3. KDF-функція у циклічній групі поля: 1) функція формування ключа (KDF-функція) у циклічній групі поля (DHKDF) ґрунтується на RFC 2631 та **ДСТУ ISO/IEC 15946-3:2006 (додаток А.2. Функція формування ключа ANSI X9.42);** …	6. Використання функції формування ключа КШК (KDF-функція) … 6.3. KDF-функція у циклічній групі поля: 1) функція формування ключа (KDF-функція) у циклічній групі поля (DHKDF) ґрунтується на RFC 2631 та **ДСТУ ISO/IEC 11770:2015;** …
7) приклади обчислення ключа КШК у циклічній групі поля: **приклади узгодження ключа з використанням геш-функції ГОСТ34.311-95 наведено у додатку 5 до цих Вимог. ДКЕ позначено через sBox (SBOX-1 – це ДКЕ № 1 Переліку ДКЕ, які рекомендуються до застосування у засобах КЗІ, наведеному у додатку 1 до Інструкції № 114);** **у наведених прикладах як KeyWrapAlgorithm ("algorithm") використовується ДСТУ ГОСТ 28147-2009 у режимі гамування ("id-gost28147-ofb", розділ VII цих Вимог) чи гамування зі зворотним зв'язком ("id-gost28147-cfb", розділ VII цих Вимог). Ці алгоритми не є Wrap-алгоритмами, що викладені у розділі VI цих Вимог, і використовуються тут лише для наведення прикладів.** **Сформований ключ КШК позначається у прикладах через KEK, його довжина в бітах – через keyLen.**	**7) Приклади обчислення ключа КШК у циклічній групі поля розміщуються на офіційному веб-сайті Державної служби спеціального зв'язку та захисту інформації України.**

Продовження таблиці

Зміст положення (норми) чинного законодавства	Зміст положення (норми) проекту акта
6.4. Використання KDF-функції в групі точок еліптичної кривої (ECDH): 1) функція формування ключа (KDF-функція) у циклічній групі поля грунтується на **ДСТУ ISO/IEC 15946-3:2002 (додаток А.3. Функція формування ключа ANSI X9.63)**; **…** **3) структура "SharedInfo":** **SharedInfo ::= SEQUENCE {** **keyInfo AlgorithmIdentifier,** **entityInfo [0] EXPLICIT OCTET STRING OPTIONAL,** **suppPubInfo [2] EXPLICIT OCTET STRING };** 4) поля структури "SharedInfo": "algorithm" – ідентифікатор алгоритму ключа шифрування ключа (KeyWrapAlgorithm), на якому повинен бути зашифрований ключ шифрування повідомлення (даних). Параметри алгоритму повинні бути NULL (ASN.1 NULL); "entityUInfo" – випадковий рядок (аналогічний полю "partyAInfo" структури "OtherInfo", наведеної у позиції 3 пункту 6.3 глави 6 розділу V цих Вимог), який генерує відправник. У CMS це значення розміщується в полі "ukm" ("UserKeyingMaterial") (закодоване як OCTET STRING) структури "KeyAgreeRecipientInfo". Довжина **"partyAInfo"** повинна бути 512 бітів (64 байти); "suppPubInfo" – довжина сформованого ключа КШК у бітах (аналогічно полю "suppPubInfo" структури "OtherInfo", наведеної у позиції 3 пункту 4.1 глави 4 розділу V), представлена як бітовий вектор (чотири байти) 32-бітного числа. Наприклад, ключ 192 біти повинен бути представлений як бітовий вектор "00 00 00 C0" (hex);	6.4. Використання KDF-функції в групі точок еліптичної кривої (ECDH): 1) функція формування ключа (KDF-функція) у циклічній групі поля грунтується на **ДСТУ ISO/IEC 11770:2015**; **…** **3) структура "SharedInfo":** **SharedInfo ::= SEQUENCE {** **keyInfo AlgorithmIdentifier,** **entityUInfo [0] EXPLICIT OCTET STRING OPTIONAL,** **suppPubInfo [2] EXPLICIT OCTET STRING };** 4) поля структури "SharedInfo": "algorithm" – ідентифікатор алгоритму ключа шифрування ключа (KeyWrapAlgorithm), на якому повинен бути зашифрований ключ шифрування повідомлення (даних). Параметри алгоритму повинні бути NULL (ASN.1 NULL); "entityUInfo" – випадковий рядок (аналогічний полю "partyAInfo" структури "OtherInfo", наведеної у позиції 3 пункту 6.3 глави 6 розділу V цих Вимог), який генерує відправник. У CMS це значення розміщується в полі "ukm" ("UserKeyingMaterial") (закодоване як OCTET STRING) структури "KeyAgreeRecipientInfo". Довжина **"entityUInfo"** повинна бути 512 бітів (64 байти); "suppPubInfo" – довжина сформованого ключа КШК у бітах (аналогічно полю "suppPubInfo" структури "OtherInfo", наведеної у позиції 3 пункту 4.1 глави 4 розділу V), представлена як бітовий вектор (чотири байти) 32-бітного числа. Наприклад, ключ 192 біти повинен бути представлений як бітовий вектор "00 00 00 C0" (hex);

Продовження таблиці

Зміст положення (норми) чинного законодавства	Зміст положення (норми) проекту акта
5) якщо параметр "entityUInfo" як необов'язковий не буде використовуватися, то у випадках А та Б для різних повідомлень буде формуватися один і той самий ключ шифрування КШК. Для уникнення цього у разі статичного механізму вимагається (а у разі динамічного – рекомендується) генерувати випадкове значення **partyAInfo** для кожного повідомлення та використовувати під час формування КШК; **6) приклади обчислення ключа КШК наведено у додатку 6 до цих Вимог. У наведених прикладах як KeyWrapAlgorithm (у прикладах "wrapAlgorithm") використовується ДСТУ ГОСТ 28147-2009 у режимі гамування ("id-gost28147-ofb", розділ VII цих Вимог) чи гамування зі зворотним зв'язком ("id-gost28147-cfb", розділ VII цих Вимог). Ці алгоритми не є Wrap-алгоритмами (які викладені у розділі VI цих Вимог) і використовуються лише для наведення прикладів.** **У прикладах використовується протокол узгодження з кофакторним множенням "id-dhSinglePass-cofactorDH-gost34311kdf-scheme".** **Сформований ключ КШК позначається у прикладах через KEK, його довжина в бітах – через keyLen.** **ДКЕ для геш-функції ГОСТ 34.311-95 позначено через sBox (SBOX-1 – це ДКЕ № 1 Переліку ДКЕ, які рекомендуються до застосування у засобах КЗІ, наведеному у додатку 1 до Інструкції № 114).**	5) якщо параметр "entityUInfo" як необов'язковий не буде використовуватися, то у випадках А та Б для різних повідомлень буде формуватися один і той самий ключ шифрування КШК. Для уникнення цього у разі статичного механізму вимагається (а у разі динамічного – рекомендується) генерувати випадкове значення **entityUInfo** для кожного повідомлення та використовувати під час формування КШК; **6) приклади обчислення ключа КШК в групі точок еліптичної кривої розміщуються на офіційному веб-сайті Державної служби спеціального зв'язку та захисту інформації України.**
VI. Алгоритм захисту ключа шифрування даних "KeyWrapAlgorithm"	
1. Алгоритм захисту ключа шифрування даних "KeyWrapAlgorithm", що ґрунтується на стандарті ДСТУ ГОСТ 28147-2009 та позначається як "GOST28147Wrap".	1. 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». **Алгоритм криптографічного перетворення за ДСТУ 7624:2014 застосовується у режимі «Калина-256/256-CFB-256» (гамування зі зворотним зв'язком за шифр текстом відповідно до розділу 8 ДСТУ 7624:2014).**

Продовження таблиці

Зміст положення (норми) чинного законодавства	Зміст положення (норми) проекту акта
	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).
2. Призначення алгоритму "GOST28147Wrap". Алгоритм GOST28147Wrap призначений для шифрування ключових даних чи інших даних, що підлягають захисту (далі - "ключові дані"), використовуючи стандарт ДСТУ ГОСТ 28147-2009 у режимі CFB (гамування із зворотним зв'язком, відповідно до розділу 4 ДСТУ ГОСТ 28147-2009) (далі - GOST28147-CFB). Алгоритм "GOST28147Wrap" призначений також для забезпечення цілісності зашифрованих ключових даних. Алгоритм захисту "GOST28147Wrap" є обов'язковим для використання.	**2. Призначення алгоритму "KeyWrapAlgorithm"** **Алгоритм "KeyWrapAlgorithm" призначений для шифрування ключових даних чи інших даних, що підлягають захисту, та забезпечення цілісності зашифрованих ключових даних.**
5. Синтаксис "KeyWrapAlgorithm" алгоритму **GOST28147Wrap:** 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 (ДКЕ) відповідно до	**5. Синтаксис "KeyWrapAlgorithm"** **5.1. 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.* 5.2. 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 (ДКЕ) відповідно до

Продовження таблиці

Зміст положення (норми) чинного законодавства	Зміст положення (норми) проекту акта
ДСТУ ГОСТ 28147-2009.	ДСТУ ГОСТ 28147:2009.
6. При використанні "GOST28147Wrap" як алгоритму захисту ключа шифрування ключів КШК у структурі "захищені дані" ("EnvelopedData") параметри алгоритму повинні бути NULL. При цьому значення ДКЕ для алгоритму повинно братися з відкритого ключа одержувача. Використання "GOST28147Wrap" з параметрами алгоритму, що не є NULL, не є предметом цих Вимог.	6. **При використанні «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.** **Використання Dstu7624Wrap» або «GOST28147Wrap» з параметрами алгоритму, що не є NULL, не є предметом цих Вимог.**
7. Для алгоритму GOST28147Wrap поле "algorithm" повинно містити **об'єктний ідентифікатор "id-gost28147-wrap":** 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) }.	7. 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) }.
8. Алгоритм GOST28147Wrap Усі структури, які задіяні в процесах зашифрування (пункт 8.2 глави 8 розділу VI цих Вимог) і розшифрування (пункт 8.3 глави 8 розділу VI цих Вимог), повинні бути представлені у форматі Little-Endian.	8. Алгоритми GOST28147Wrap та **Dstu7624Wrap** 8.1. Усі структури, які задіяні в процесах зашифрування (пункти 8.2, **8.5** глави 8 розділу VI цих Вимог) і розшифрування (пункти 8.3, **8.6** глави 8 розділу VI цих Вимог), повинні бути представлені у форматі Little-Endian.
8.2. Процес зашифрування (Key Wrap) ... **Вихідними даними процесу зашифрування є:** **"result" – зашифровані ключові дані.** ...	8.2. Процес зашифрування (Key Wrap) **алгоритму GOST28147Wrap** ... **Вихідними даними процесу зашифрування є "result" – зашифровані ключові дані.** ...
8.3. Процес розшифрування (Key Unwrap) ...	8.3. Процес розшифрування (Key Unwrap) **алгоритму GOST28147Wrap** ...

Продовження таблиці

Зміст положення (норми) чинного законодавства	Зміст положення (норми) проекту акта
-	**8.5. 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 таким чином, 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» – це ключ шифрування даних КШД);** IV – **синхропосилка, двійковий рядок довжиною 256, генерація здійснюється перед використанням алгоритму;**

Продовження таблиці

Зміст положення (норми) чинного законодавства	Зміст положення (норми) проекту акта
	*IV*1 – фіксована синхропосилка, двійковий рядок довжиною 256 із значенням «6973271D6E611D06616715046C65504C2020004F6D68011F65610C0C73734714». Вихідні параметри: *RES* – зашифровані ключові дані; Алгоритм: Виконати такі обчислення: $ICV = CMAC(CEK, KEK)$ $CEKICV = CEK \parallel ICV$ $TEMP1 = E(CEKIV, KEK, IV)$ $TEMP2 = IV \parallel TEMP1$ $TEMP3 = REV(TEMP2)$ $RES = E(TEMP3, KEK, IV1)$.
-	8.6. Процес розшифрування (Key Unwrap) алгоритму Dstu7624Wrap Вхідні параметри: *KEK* – ключ шифрування ключа (КШК), двійковий рядок довжиною 256; *RES* – зашифровані ключові дані; *IV*1 – фіксована синхропосилка, двійковий рядок довжиною 256 із значенням «6973271D6E611D06616715046C65504C2020004F6D68011F65610C0C73734714». Вихідні параметри: *CEK* – ключові дані для шифрування (в операції формування «захищені дані» – це ключ шифрування даних КШД); Алгоритм:

Продовження таблиці

Зміст положення (норми) чинного законодавства	Зміст положення (норми) проекту акта
	Виконати такі обчислення: $TEMP3 = E(RES, KEK, IV1)$ $TEMP2 = REV(TEMP3)$ $IV = L(TEMP2,256)$ $TEMP1 = R(TEMP2, I(TEMP2) - 256)$ $CEKICV = E(TEMP1, KEK, IV)$ $CEK = L(CEKICV, I(CEKICV) - 256)$ $ICV = R(CEKICV,256)$ $ICV1 = CMAC(CEK, KEK)$. **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 **.**
9. Приклади обчислення імітовставки ДСТУ ГОСТ 28147-2009 наведено в додатку 7 до цих Вимог.	**9. Приклади обчислення імітовставки за ДСТУ 7624:2014 та за ДСТУ ГОСТ 28147:2009 розміщуються на офіційному веб-сайті Державної служби спеціального зв'язку та захисту інформації України.**
10. Приклади обчислення за алгоритмом "GOST28147Wrap" наведено в додатку 8 до цих Вимог.	**10. Приклади обчислення** GOST28147Wrap та **Dstu7624Wrap розміщуються на офіційному веб-сайті Державної служби спеціального зв'язку та захисту інформації України.**
VII. Алгоритм захисту даних (повідомлення) «contentEncryptionAlgorithm»	
7.1. Об'єктні ідентифікатори алгоритмів ДСТУ ГОСТ 28147-2009. **Як алгоритм захисту (шифрування) даних "contentEncryptionAlgorithm" структури "EncryptedContentInfo" можуть використовуватися алгоритми ДСТУ ГОСТ 28147-2009 у таких 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);**	**7.1. Об'єктні ідентифікатори алгоритмів шифрування даних** **Як алгоритм шифрування даних "contentEncryptionAlgorithm" структури "EncryptedContentInfo" можуть використовуватися алгоритми:**

Продовження таблиці

Зміст положення (норми) чинного законодавства	Зміст положення (норми) проекту акта
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) }.	ДСТУ 7624:2014 у режимах «Калина-256/256-OFB» (режим гамування зі зворотним зв'язком по шифротексту відповідно до розділу 8 ДСТУ 7624:2014) та «Калина-256/256-CFB» (режим гамування зі зворотним зв'язком по шифрограмі 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) }.
7.2. Параметри алгоритмів 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.	7.2. 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.

Продовження таблиці

Зміст положення (норми) чинного законодавства	Зміст положення (норми) проекту акта
-	**7.3. Параметри алгоритму ДСТУ 7624:2014** **Dstu7624Parameters::= SEQUENCE {** **iv OCTET STRING (SIZE (32))},** **де "iv" – вектор ініціалізації, що обирається випадково.**
VIII. Сертифікат шифрування	
8.2. Сертифікат шифрування, призначений для протоколу узгодження ключа Діффі-Геллмана в циклічній групі простого поля, повинен бути посиленим сертифікатом відкритого ключа алгоритму ГОСТ 34.310-95 з довжиною 1024 біти.	-
8.3 Сертифікат шифрування, призначений для алгоритму узгодження ключа Діффі-Геллмана в групі точок еліптичної кривої, повинен бути посиленим сертифікатом відкритого ключа алгоритму ДСТУ 4145-2002.	-

Директор Департаменту захисту інформації
Адміністрації Державної служби спеціального
зв'язку та захисту інформації України А.І. Пушкарьов

04/02/03-2955
17.11.17

Прим. № 1

АНАЛІЗ РЕГУЛЯТОРНОГО ВПЛИВУ
проекту наказу Адміністрації Держспецзв'язку «Про затвердження Змін до Вимог до форматів криптографічних повідомлень»

I. Визначення проблеми

З прийняттям наказу Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 29 березня 2017 року № 1017/5/206 «Про внесення змін до наказу Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 серпня 2012 року № 1236/5/453», зареєстрованого Міністерством юстиції України 29 березня 2017 року за № 422/30290, в інфраструктурі відкритих ключів передбачено можливість застосування нових криптографічних алгоритмів.

У зв'язку з цим виникла необхідність визначення режимів роботи нових криптографічних алгоритмів для формування криптографічних повідомлень.

Крім того, відповідно до практики застосування Вимог до форматів криптографічних повідомлень, затверджених наказом Адміністрації Держспецзв'язку від 18 грудня 2012 року № 739, зареєстрованих в Міністерстві юстиції України 14 січня 2013 року за № 108/22640 (далі – Вимоги), виникла необхідність уточнення положень Вимог з метою їх однозначного тлумачення.

Враховуючи зазначене, можна виділити такі основні групи (підгрупи), на які проблема справляє вплив:

Групи (підгрупи)	Так	Ні
Громадяни	+	
Держава	+	
Суб'єкти господарювання	+	

II. Цілі державного регулювання

Проект наказу спрямовано на забезпечення сумісності засобів криптографічного захисту інформації (далі - КЗІ) та надійних засобів електронного цифрового підпису (далі - ЕЦП) під час організації захищеного електронного документообігу.

III. Визначення та оцінка альтернативних способів досягнення цілей

Вид альтернативи	Опис альтернативи
Альтернатива 1 Прийняття наказу	Надасть можливість застосування цих Вимог у засобах КЗІ та ЕЦП, які підтримують нові криптографічні алгоритми в інфраструктурі відкритих ключів.
Альтернатива 2 Залишення існуючої ситуації без змін	Унеможливить застосування цих Вимог у засобах КЗІ та ЕЦП, які підтримують нові криптографічні алгоритми в інфраструктурі відкритих ключів.

2. Оцінка вибраних альтернативних способів досягнення цілей

Оцінка впливу на сферу інтересів держави

Вид альтернативи	Вигоди	Витрати
1. Прийняття наказу	Можливість удосконалення системи подання електронної звітності. Залучення інвестицій до створення засобів КЗІ та ЕЦП, які можуть використовуватися органами державної влади під час організації захищеного документообігу. Створення конкуренції між розробниками засобів КЗІ. Підвищення конкурентоспроможності вітчизняних засобів КЗІ та ЕЦП на світовому ринку (їх сумісність, відповідність міжнародним стандартам), що підвищить попит на них	Додаткових витрат не потребує.
2. Залишення існуючої ситуації без змін	відсутні	Додаткових витрат не потребує.

Оцінка впливу на сферу інтересів громадян

Вид альтернативи	Вигоди	Витрати
1. Прийняття наказу	Забезпечення прав споживачів на придбання сумісних засобів КЗІ потрібної якості	Додаткових витрат не потребує.
2. Залишення існуючої ситуації без змін	відсутні	Додаткових витрат не потребує.

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, одиниць	14	15	-	-	29
Питома вага групи у загальній кількості, відсотків	45%	55%	-	-	100%

Вид альтернативи	Вигоди	Витрати
1. Прийняття наказу	Створення технічних умов подання суб'єктами господарювання захищеної електронної звітності, що забезпечить їх право на конфіденційність інформації. Підвищення конкурентоспроможності вітчизняних засобів КЗІ та ЕЦП на	Додаткових витрат не потребує.

	світовому ринку (їх сумісність, відповідність міжнародним стандартам), що підвищить попит на них. Можливість інвестування у розроблення засобів КЗІ та ЕЦП, які можуть використовуватися органами державної влади під час організації захищеного документообігу	
2. Залишення існуючої ситуації без змін	Відсутні	Додаткових витрат не потребує.

Вид альтернативи	Сума витрат, гривень
1. Прийняття наказу	Додаткових витрат не потребує.
2. Залишення існуючої ситуації без змін	Додаткових витрат не потребує.

IV. Вибір найбільш оптимального альтернативного способу досягнення цілей

Прийняття наказу надасть можливість застосувати ці Вимоги у засобах КЗІ та ЕЦП, які підтримують нові криптографічні алгоритми в інфраструктурі відкритих ключів під час організації захищеного електронного документообігу та подання суб'єктами господарювання захищеної електронної звітності, що забезпечить їх право на конфіденційність інформації.

Здійснити вибір оптимального альтернативного способу з урахуванням системи бальної оцінки ступеня досягнення визначених цілей.

Вартість балів визначається за чотирибальною системою оцінки ступеня досягнення визначених цілей, де:

4 - цілі прийняття регуляторного акта, які можуть бути досягнуті повною мірою (проблема більше існувати не буде);

3 - цілі прийняття регуляторного акта, які можуть бути досягнуті майже повною мірою (усі важливі аспекти проблеми існувати не будуть);

2 - цілі прийняття регуляторного акта, які можуть бути досягнуті частково (проблема значно зменшиться, деякі важливі та критичні аспекти проблеми залишаться невирішеними);

1 - цілі прийняття регуляторного акта, які не можуть бути досягнуті (проблема продовжує існувати).

Рейтинг результативності (досягнення цілей під час вирішення проблеми)	Бал результативності (за чотирибальною системою оцінки)	Коментарі щодо присвоєння відповідного бала
1. Прийняття наказу	4	Цілі прийняття регуляторного акта можуть бути досягнуті повною мірою (проблема більше існувати не буде)
2. Залишення існуючої ситуації без змін	1	Цілі прийняття регуляторного акта не можуть бути досягнуті (проблема продовжить існувати)

Рейтинг результативності	Вигоди (підсумок)	Витрати (підсумок)	Обґрунтування відповідного місця альтернативи у рейтингу
1. Прийняття наказу	Прийняття наказу надасть можливість застосувати ці Вимоги у засобах КЗІ та ЕЦП, які підтримують нові криптографічні алгоритми в інфраструктурі відкритих ключів під час організації захищеного електронного документообігу та подання суб'єктами господарювання захищеної електронної звітності, що забезпечить їх право на конфіденційність інформації.	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

Проект наказу визначає синтаксис (формат представлення) криптографічних повідомлень (зашифрованих даних) в електронній формі, а також протоколи узгодження ключів для засобів КЗІ та ЕЦП. Встановлення єдиних форматів криптографічних повідомлень має на меті визначення технічних умов щодо забезпечення сумісності засобів КЗІ та ЕЦП різних розробників.

Прийняття проекту наказу надасть можливість застосувати ці Вимоги у засобах КЗІ та ЕЦП, які підтримують нові криптографічні алгоритми в інфраструктурі відкритих ключів під час організації захищеного електронного документообігу та подання суб'єктами господарювання захищеної електронної звітності, що забезпечить їх право на конфіденційність інформації.

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

Вимоги наказу стосуються розробників та користувачів засобів криптографічного захисту інформації.

Можливість впровадження державними органами та суб'єктами господарювання вимог наказу на цей час не обмежується.

Правильне виконання користувачами засобів КЗІ та ЕЦП вимог наказу залежить від рівня ознайомленості користувачів з експлуатаційною документацією на відповідний засіб КЗІ та ЕЦП та практичних навичок.

VII. Обґрунтування запропонованого строку дії регуляторного акта

Строк дії цього регуляторного акта не обмежується.

VIII. Визначення показників результативності дії регуляторного акта

Прогнозними значеннями показників результативності дії проекту наказу є:

- кількість суб'єктів господарювання, на яких поширюватиметься дія наказу;
- кількість звернень суб'єктів господарювання щодо трактування вимог цього наказу;
- кількість засобів КЗІ та ЕЦП в яких реалізовані формати криптографічних повідомлень із застосуванням нових криптографічних алгоритмів відповідно до цього наказу;

Рівень поінформованості суб'єктів господарювання з основних положень проекту наказу є високим, оскільки вказаний проект розміщується на офіційному веб-сайті Державної служби спеціального зв'язку та захисту інформації України.

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

Базове відстеження результативності регуляторного акта буде здійснено до набрання чинності цим актом шляхом аналізу та підрахунку статистичних даних, але не пізніше дня, з якого починається проведення повторного відстеження результативності цього акта.

Повторне відстеження результативності регуляторного акта здійснюватиметься через рік з дня набрання чинності цим регуляторним актом, але не пізніше двох років після набрання ним чинності. За результатами даного відстеження відбудеться порівняння показників базового та повторного відстеження.

Періодичне відстеження результативності цього регуляторного акта здійснюватиметься раз на три роки, починаючи з дня виконання заходів з повторного відстеження результативності.

Цільові групи, які залучатимуться для проведення відстеження – суб'єкти господарювання, які здійснюють свою діяльність у даній сфері.

Відстеження результативності цього регуляторного акта буде здійснюватися за допомогою статистичного методу, виконавцем якого є Держспецзв'язку.

ВИТРАТИ
на одного суб'єкта господарювання великого і середнього підприємництва, які виникають внаслідок дії регуляторного акта

Порядковий номер	Витрати	За перший рік	За п'ять років
1	2	3	4
1	Витрати на придбання основних фондів, обладнання та приладів, сервісне обслуговування, навчання/підвищення кваліфікації персоналу тощо, гривень	0 грн.	0 грн.

1	2	3	4
2	Податки та збори (зміна розміру податків/зборів, виникнення необхідності у сплаті податків/зборів), гривень	0 грн.	0 грн.
3	Витрати, пов'язані із веденням обліку, підготовкою та поданням звітності державним органам, гривень	0 грн.	0 грн.
4	Витрати, пов'язані з адмініструванням заходів державного нагляду (контролю) (перевірок, штрафних санкцій, виконання рішень/ приписів тощо), гривень	0 грн.	0 грн.
5	Витрати на отримання адміністративних послуг (дозволів, ліцензій, сертифікатів, атестатів, погоджень, висновків, проведення незалежних/обов'язкових експертиз, сертифікації, атестації тощо) та інших послуг (проведення наукових, інших експертиз, страхування тощо), гривень	0 грн.	0 грн.
6	Витрати на оборотні активи (матеріали, канцелярські товари тощо), гривень	0 грн.	0 грн.
7	Витрати, пов'язані із наймом додаткового персоналу, гривень	0 грн.	0 грн.
8	Інше (уточнити), гривень	0 грн.	0 грн.
9	РАЗОМ (сума рядків: 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8), гривень	0 грн.	0 грн.
10	Кількість суб'єктів господарювання великого та середнього підприємництва, на яких буде поширено регулювання, одиниць*	29	
11	Сумарні витрати суб'єктів господарювання великого та середнього підприємництва, на виконання регулювання (вартість регулювання) (рядок 9 х рядок 10), гривень	0 грн.	0 грн.
* статистика стосовно розподілу на суб'єктів господарювання малого, середнього чи великого підприємництва не ведеться та не вимагається			

Розрахунок відповідних витрат на одного суб'єкта господарювання

Вид витрат	У перший рік	Періодичні (за рік)	Витрати за п'ять років
Витрати на придбання основних фондів, обладнання та приладів, сервісне обслуговування, навчання/підвищення кваліфікації персоналу тощо	0 грн.	0 грн.	0 грн.

Вид витрат	Витрати на сплату податків та зборів (змінених/нововведених) (за рік)	Витрати за п'ять років
Податки та збори (зміна розміру податків/зборів, виникнення необхідності у сплаті податків/зборів)	0 грн.	0 грн.

Вид витрат	Витрати* на ведення обліку, підготовку та	Витрати на оплату штрафних	Разом за рік	Витрати за п'ять років

	подання звітності (за рік)	санкцій за рік		
Витрати, пов'язані із веденням обліку, підготовкою та поданням звітності державним органам (витрати часу персоналу)	0 грн.	0 грн.	0 грн.	0 грн.

* Вартість витрат, пов'язаних із підготовкою та поданням звітності державним органам, визначається шляхом множення фактичних витрат часу персоналу на заробітну плату спеціаліста відповідної кваліфікації).

Вид витрат	Витрати* на адміністрування заходів державного нагляду (контролю) (за рік)	Витрати на оплату штрафних санкцій та усунення виявлених порушень (за рік)	Разом за рік	Витрати за п'ять років
Витрати, пов'язані з адмініструванням заходів державного нагляду (контролю) (перевірок, штрафних санкцій, виконання рішень/ приписів тощо)	0 грн.	0 грн.	0 грн.	0 грн.

* Вартість витрат, пов'язаних з адмініструванням заходів державного нагляду (контролю), визначається шляхом множення фактичних витрат часу персоналу на заробітну плату спеціаліста відповідної кваліфікації.

Вид витрат	Витрати на проходження відповідних процедур (витрати часу, витрати на експертизи, тощо)	Витрати безпосередньо на дозволи, ліцензії, сертифікати, страхові поліси (за рік - стартовий)	Разом за рік (стартовий)	Витрати за п'ять років
Витрати на отримання адміністративних послуг (дозволів, ліцензій, сертифікатів, атестатів, погоджень, висновків, проведення незалежних/обов'язкових експертиз, сертифікації, атестації тощо) та інших послуг (проведення наукових, інших експертиз, страхування тощо)	0 грн.	0 грн.	0 грн.	0 грн.

Вид витрат	За рік (стартовий)	Періодичні (за наступний рік)	Витрати за п'ять років
Витрати на оборотні активи (матеріали, канцелярські товари тощо)	0 грн.	0 грн.	0 грн.

Вид витрат	Витрати на оплату праці додатково найманого персоналу (за рік)	Витрати за п'ять років
Витрати, пов'язані із наймом додаткового персоналу	0 грн.	0 грн.

Голова Державної служби спеціального зв'язку та захисту інформації України Леонід Євдоченко

«___»_____ 2017 року

04/02/03 - 2958

17.11.17

прим. №

Повідомлення про оприлюднення проекту наказу Адміністрації Держспецзв'язку «Про затвердження Змін до Вимог до форматів криптографічних повідомлень»

1. Стислий виклад змісту проекту акта

З прийняттям наказу Мін'юсту, Адміністрації Держспецзв'язку від 29 березня 2017 року № 1017/5/206 «Про внесення змін до наказу Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 серпня 2012 року № 1236/5/453», зареєстрованого в Мін'юсті 29 березня 2017 року за № 422/30290, в інфраструктурі відкритих ключів передбачено можливість застосування нових криптографічних алгоритмів.

У зв'язку з цим виникла необхідність визначення режимів роботи нових криптографічних алгоритмів для формування криптографічних повідомлень.

Також відповідно до практики застосування Вимог до форматів криптографічних повідомлень, затверджених наказом Адміністрації Держспецзв'язку від 18 грудня 2012 року № 739, зареєстрованих в Мін'юсті 14 січня 2013 року за № 108/22640 (далі – Вимоги), виникла необхідність уточнення положень Вимог з метою їх однозначного тлумачення.

Адміністрацією Держспецзв'язку розроблено проект наказу «Про затвердження Змін до Вимог до форматів криптографічних повідомлень».

2. Адреси для зауважень та пропозицій до проекту акта

Пропозиції та зауваження до проекту наказу просимо надсилати протягом місяця з дати його оприлюднення на адреси:

- Адміністрації Державної служби спеціального зв'язку та захистуінформації України:

поштова: вул. Солом'янська, 13, м. Київ, 03680; тел. (044) 281-90-10, (044) 281-94-83, факс (044) 226-26-83;

електронна: info@dsszzi.gov.ua;

- Державної регуляторної служби України:

поштова: вул. Арсенальна, 9/11, м. Київ, 01011; тел. (044) 254-56-73, факс (044) 254-43-93;

електронна: inform@dkrp.gov.ua

3. Обраний спосіб оприлюднення проекту акта

Проект акта оприлюднюється в мережі Інтернет: проект наказу та аналіз регуляторного впливу.

4. Строк, протягом якого приймаються зауваження та пропозиції

Зауваження та пропозиції до проекту акта приймаються у період – «15»листопада 2017 року – «15» грудня 2017 року.

Зауваження та пропозиції до проекту акта необхідно надавати письмово на адреси, зазначені у пункті 2.

Голова Державної служби спеціального зв'язку та захисту інформації України Леонід Євдоченко

«___» листопада 2017 р.

04/02/03-2859
12.11.17