

ЗАТВЕРДЖЕНО

Наказ Міністерства юстиції України,
Адміністрації Державної служби
спеціального зв'язку та захисту
інформації України

27 грудня 2013 року № 2782/5/689

ВИМОГИ

**до алгоритмів формування ключів шифрування ключів та захисту
особистих ключів електронного цифрового підпису та особистих ключів
шифрування**

I. Загальні положення

1. Ці Вимоги визначають алгоритми формування ключів шифрування ключів на основі парольної інформації та захисту особистих ключів електронного цифрового підпису та особистих ключів шифрування з використанням алгоритмів ДСТУ ГОСТ 28147:2009 «Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования», затвердженого наказом Державного комітету України з пи-

тань технічного регулювання та споживчої політики від 22 грудня 2008 року № 495 (із змінами) (далі – ГОСТ 28147:2009), та ГОСТ 34.311-95 «Информационная технология. Криптографическая защита информации. Функция хэширования», затвердженого наказом Державного комітету України з питань технічного регулювання та споживчої політики від 21 жовтня 1997 року № 640 (далі – ГОСТ 34.311-95).

2. Формати даних представлено у нотації ASN.1, визначеній у міжнародному стандарті ISO/IEC 8824 «Information technology – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1)» / ДСТУ ISO/IEC 8824-3:2008 «Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 3. Специфікація обмежень», затвердженому наказом Державного комітету України з питань технічного регулювання та споживчої політики від 26 грудня 2008 року № 508 (із змінами).

3. Усі структури даних кодують за правилами DER згідно з міжнародним стандартом ISO/IEC 8825-1:2002 «Information technology – ASN.1 encoding Rules – Part 1: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)» & AMD1:2004 «Support for EXTENDED-XER».

4. Ці Вимоги засновані на національному стандарті України ГОСТ 28147:2009, міждержавному стандарті ГОСТ 34.311-95 та міжнародних рекомендаціях RFC 2898 «Password-Based Cryptography Specification (PKCS#5)», September 2000 (далі – RFC 2898), RFC 2104 «HMAC: Keyed-Hashing for Message Authentication», February 1997 (далі – RFC 2104).

5. Ці Вимоги не дублюють стандарти ГОСТ 28147:2009, ГОСТ 34.311-95 та міжнародні рекомендації RFC 2898, а описують положення цих стандартів і рекомендацій та алгоритми формування ключів шифрування ключів на основі паролльної інформації та захисту особистих ключів електронного цифрового підпису та особистих ключів шифрування з використанням алгоритмів, визначених ГОСТ 28147:2009 та ГОСТ 34.311-95. У разі виникнення розбіжностей між положеннями зазначених стандартів і рекомендацій та положеннями цих Вимог застосовуються положення цих Вимог.

6. Правильність реалізації алгоритмів формування ключів шифрування ключів на основі паролльної інформації та захисту особистих ключів електронного цифрового підпису та особистих ключів шифрування з використанням алгоритмів ГОСТ 28147:2009 та ГОСТ 34.311-95 у надійних засобах електронного цифрового підпису та у засобах шифрування підтверджується позитивним експертним висновком за результатами державної експертизи у сфері криптографічного захисту інформації.

II. Алгоритм формування ключа шифрування ключа на основі парольної інформації (PBKDF-функція)

1. Алгоритм формування ключа шифрування ключа на основі парольної інформації (PBKDF-функція) призначений для формування симетричного ключа (DK) на основі парольної інформації, випадкових даних та числа ітерацій.

2. Процес реалізації PBKDF-функції передбачає здійснення таких дій: формування ключового матеріалу (KM) з використанням парольної інформації, випадкових даних та числа ітерацій;

створення симетричного ключа для заданого алгоритму шифрування або контролю цілісності даних на основі ключового матеріалу.

3. Ці Вимоги визначають функцію формування ключа на основі функції PBKDF2 з використанням псевдовипадкової функції (PRF-функції), що базується на міжнародних рекомендаціях RFC 2104, алгоритмі гешування за ГОСТ 34.311-95 (далі – HMAC_GOST34311):

$DK = PBKDF(P, S, c, dkLen)$,
де P – пароль, символьний рядок у кодуванні Unicode UTF-8,
 S – випадкові дані,
 c – число ітерацій алгоритму,
 $dkLen$ – необхідна довжина вихідної послідовності в байтах.

4. Під час формування симетричного ключа на основі парольної інформації вчиняються такі дії:

виконується перевірка умови $dkLen > (2^{32} - 1) * hLen$,
де $hLen$ – довжина вихідного значення функції HMAC_GOST34311.

У разі виконання умови подальші дії не виконуються у зв'язку з недопустимим значенням довжини ключа;

обчислюються значення:

$n = V(dkLen/hLen)$,

де V – функція округлення аргументу функції до найменшого натурального числа, більшого за аргумент функції,

$T_1 = F(P, S, c, 1)$,

$T_2 = F(P, S, c, 2)$,

...,

$T_n = F(P, S, c, n)$,

де $F(P, S, c, i) = U_1 \oplus U_2 \oplus \dots \oplus U_c$,

$U_1 = HMAC_GOST34311(P, S \parallel INT(i))$,

$U_2 = HMAC_GOST34311(P, U_1)$,

...,

$U_c = HMAC_GOST34311(P, U_{c-1})$,

\oplus – порозрядне додавання за модулем 2,

INT (i) – представлення цілого числа «i» чотирма байтами зі старшим байтом зліва;

в результаті конкатенації $\{T_i\}$ з урізанням T_n до необхідної довжини $dkLen$ формується ключ «DK»:

$$DK = T_1 \parallel T_2 \parallel \dots \parallel T_n.$$

5. Формування ключа шифрування ключа на основі парольної інформації здійснюється згідно з додатком до цих Вимог.

III. Алгоритми захисту особистих ключів електронного цифрового підпису та особистих ключів шифрування на основі парольної інформації

1. Алгоритм шифрування алгоритмів захисту особистих ключів електронного цифрового підпису та особистих ключів шифрування на основі парольної інформації (PBES-функція)

1. Алгоритм шифрування алгоритмів захисту особистих ключів електронного цифрового підпису та особистих ключів шифрування (далі – дані) на основі парольної інформації (PBES-функція) призначений для шифрування даних на основі парольної інформації.

2. Ці Вимоги визначають функцію шифрування даних на основі функції PBES2 відповідно до RFC 2898 з використанням алгоритму ГОСТ 28147:2009 у режимі гамування зі зворотним зв'язком.

3. Під час здійснення процесу зашифрування даних на основі парольної інформації вчиняються такі дії:

встановлюється довгостроковий ключовий елемент «dke», що відповідає вимогам 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);

генерується випадкове значення «S» розміром від 8 до 32 байтів. Рекомендований розмір значення «S» – 32 байти;

встановлюється число ітерацій «с» залежно від умов застосування. Мінімально допустиме значення параметра – 1000 ітерацій, рекомендоване – 10000 ітерацій;

встановлюється значення параметра «dkLen» = 32;

обчислюється значення ключа «DK» = PBKDF (P, S, c, 32);

генеруються випадкові 8 байтів як вектор ініціалізації «IV» (синхропосилка);

шифруються дані за алгоритмом ГОСТ 28147:2009 у режимі гамування зі зворотним зв'язком, використовуючи отримані «dke», ключ «DK» та вектор ініціалізації «IV».

Параметри «S», «с», «dke» та «IV» повинні бути збережені разом із зашифрованими даними для їх розшифрування.

4. Під час здійснення процесу розшифрування даних на основі парольної інформації вчиняються такі дії:

встановлюється довгостроковий ключовий елемент «dke», що відповідає вимогам Інструкції;

отримуються випадкове значення «S» та число ітерацій «с»;

встановлюється значення параметра «dkLen» = 32;

обчислюється значення ключа «DK» = PBKDF (P, S, с, 32);

отримується вектор ініціалізації «IV»;

розшифровуються дані за алгоритмом ГОСТ 28147:2009 у режимі гамування зі зворотним зв'язком, використовуючи «dke», ключ «DK» та вектор ініціалізації «IV».

2. Алгоритм контролю цілісності даних на основі парольної інформації (РВМАС-функція)

1. Алгоритм контролю цілісності даних на основі парольної інформації (РВМАС-функція) призначений для контролю цілісності даних на основі парольної інформації.

2. Ці Вимоги визначають функцію контролю цілісності даних на основі функції РВМАС1 відповідно до RFC 2898 з використанням алгоритму ГОСТ 28147:2009 у режимі вироблення імітовставки.

3. Під час здійснення процесу вироблення імітовставки на основі парольної інформації вчиняються такі дії:

встановлюється довгостроковий ключовий елемент «dke», що відповідає вимогам Інструкції;

генерується випадкове значення «S» розміром від 8 до 32 байтів. Рекомендований розмір значення «S» = 32 байти;

встановлюється число ітерацій «с» залежно від умов застосування. Мінімально допустиме значення параметра – 1000 ітерацій, рекомендоване – 10000 ітерацій;

встановлюється значення параметра «dkLen» = 32;

обчислюється значення ключа «DK» = PBKDF (P, S, с, 32);

обчислюється імітовставка згідно з розділом 5 ГОСТ 28147:2009, використовуючи «dke» та ключ «DK».

Параметри «S», «с» та «dke» повинні бути збережені разом з обчисленою імітовставкою для її перевірки.

4. Під час здійснення процесу перевірки імітовставки на основі пароліної інформації вчиняються такі дії:

встановлюється довгостроковий ключовий елемент «dke», що відповідає вимогам Інструкції;

отримуються випадкове значення «S» та число ітерацій «с»;

встановлюється значення параметра «dkLen» = 32;

обчислюється значення ключа «DK» = PBKDF (P, S, с, 32);

обчислюється імітовставка згідно з ГОСТ 28147:2009, використовуючи «dke» та ключ «DK»;

порівнюється значення імітовставки, отриманої за результатами виконання цих обчислень, із значенням імітовставки, яка перевіряється.

У разі нерівності значень імітовставок подальше оброблення даних припиняється у зв'язку з їх пошкодженням.

IV. Параметри алгоритмів захисту даних на основі пароліної інформації

1. Параметри алгоритму формування ключа шифрування ключа на основі пароліної інформації

1. Об'єктний ідентифікатор функції PBKDF2 позначається як:

id-PBKDF2 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-5(5) 12 }.

2. Параметри алгоритму PBKDF2 визначаються як:

```
PBKDF2-params ::= SEQUENCE {
    salt CHOICE {
        specified OCTET STRING,
        otherSource AlgorithmIdentifier {{PBKDF2-
SaltSources}}
    },
    iterationCount INTEGER (1..MAX),
    keyLength INTEGER (1..MAX) OPTIONAL,
    prf AlgorithmIdentifier {{PBKDF2-PRFs}}},
```

де salt – випадкове значення розміром від 8 до 32 байтів, що подається у вигляді OCTET STRING;

iterationCount – кількість ітерацій, яка визначається умовами застосування;

keyLength – розмір ключа у байтах. Поле «keyLength» у випадку застосування PBES-функції повинно бути відсутнім;

prf – ідентифікатор алгоритму HMAC_GOST34311:

id-hmacGost34311 OBJECT IDENTIFIER ::= { iso(1) member-body(2) Ukraine(804) root(2) security(1) cryptography(1) ua-pki (1) alg (1) sym (1) 2 };

параметри алгоритму повинні бути NULL (ASN.1 NULL).

2. Параметри алгоритму шифрування даних на основі паролльної інформації

1. Об'єктний ідентифікатор функції PBES2 позначається як:

id-PBES2 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-5(5) 13 }.

2. Параметри алгоритму PBES2 визначаються як:

PBES2-params ::= SEQUENCE {
keyDerivationFunc AlgorithmIdentifier {{PBES2-KDFs}},
encryptionScheme AlgorithmIdentifier {{PBES2-Encs}}},

де keyDerivationFunc – ідентифікатор та параметри PBKDF-функції відповідно до пункту 1 цієї глави;

encryptionScheme – алгоритм ГОСТ 28147:2009 у режимі гамування зі зворотним зв'язком;

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) }.

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

де iv – вектор ініціалізації, що обирається випадково;

dke – довгостроковий ключовий елемент для ГОСТ 28147:2009, що відповідає вимогам Інструкції.

**Начальник Управління
функціонування центрального
засвідчувального органу
Міністерства юстиції України**

Д.В. Журавльов

**Директор Департаменту криптографічного
захисту інформації Адміністрації
Державної служби спеціального зв'язку
та захисту інформації України**

А.І. Пушкарьов