ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ
ПО СТАНДАРТИЗАЦИИ

Р 50.1.111—2016

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Парольная защита ключевой информации

Издание официальное

Москва
Стандартинформ
2016

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАНЫ подкомитетом 1 Технического комитета по стандартизации ТК 26 «Криптографическая защита информации»

2 ВНЕСЕНЫ Техническим комитетом по стандартизации ТК 26 «Криптографическая защита информации»

3 УТВЕРЖДЕНЫ И ВВЕДЕНЫ В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 23 ноября 2016 г. № 1752-ст

4 ВВЕДЕНЫ ВПЕРВЫЕ

*Правила применения настоящих рекомендаций установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящим рекомендациям публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящих рекомендаций соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, 2016

Настоящие рекомендации не могут быть полностью или частично воспроизведены, тиражированы и распространены в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Обозначения 1
4 Алгоритм выработки ключа из пароля 2
5 Шифрование данных 2
6 Контроль целостности 3
7 Идентификаторы и параметры 3
7.1 PBKDF2 3
7.2 PBES2 3
7.3 PBMAC1 4
8 Рекомендуемые криптографические параметры 4
Приложение А (справочное) Контрольные примеры 5
Библиография 7

Введение

Настоящие рекомендации содержат описание расширения документа PKCS#5 «Password-Based Cryptography Standard» версии 2.1 [1]. Он относится к группе Public Key Cryptography Standarts (стандарты криптографии с открытым ключом) и содержит рекомендации по реализации криптографических механизмов при использовании низкоэнтропийных данных (пароля пользователя).

Данное расширение [1] позволяет, не нарушая исходных принципов работы схем выработки общей ключевой информации из парольной информации, использовать в нем криптографические механизмы из национальных стандартов Российской Федерации.

Разработка настоящих рекомендаций вызвана необходимостью создания решения, корректно использующего национальные криптографические стандарты для процедур взаимодействия сторон, обеспечивающих безопасную выработку общей ключевой информации при наличии общих исходных данных с низкой энтропией.

Примечание — Основная часть рекомендаций дополнена приложением А.

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Парольная защита ключевой информации

Information technology. Cryptographic data security.
Password-based protection of key information

Дата введения — 2017—06—01

1 Область применения

Настоящие рекомендации предназначены для применения в информационных системах, использующих механизмы шифрования и обеспечения аутентичности данных, с реализацией алгоритмов шифрования по ГОСТ 28147—89 и функции хэширования по ГОСТ Р 34.11 в общедоступных и корпоративных сетях для защиты информации, не содержащей сведений, составляющих государственную тайну. Описанные в данных рекомендациях методы предназначены для выработки ключевой информации с использованием пароля пользователя и защиты такой информации.

2 Нормативные ссылки

В настоящих рекомендациях использованы нормативные ссылки на следующие стандарты:

ГОСТ 28147—89 Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования

ГОСТ Р 34.11—2012 Информационная технология. Криптографическая защита информации. Функция хэширования

Р 50.1.113—2016 Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования

Примечание — При пользовании настоящими рекомендациями целесообразно проверить действие ссылочных стандартов (рекомендаций) в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт (рекомендации), на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта (рекомендаций) с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт (рекомендации), на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта (рекомендаций) с указанным выше годом утверждения (принятия). Если после утверждения настоящих рекомендаций в ссылочный стандарт (рекомендации), на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт (рекомендации) отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Обозначения

В настоящих рекомендациях использованы следующие обозначения:

HMAC_GOSTR3411(*K, T*) — значение кода аутентификации сообщения, вычисленное для сообщения *T* на ключе *K* по алгоритму HMAC_GOSTR3411_2012_512, определенному в Р 50.1.113—2016 длина значения равна 512 битам;

Издание официальное

P	—	пароль, представляющий собой символьную строку в кодировке Unicode UTF-8;
S	—	случайное значение в соответствии с [1];
c	—	число итераций алгоритма;
$dkLen$	—	требуемая длина выходной последовательности (в байтах);
DK	—	производный ключ длины $dkLen$;
$\oplus$	—	операция покомпонентного сложения по модулю 2 двух двоичных строк одинаковой длины;
B_n	—	множество байтовых строк длины n, $n \geq 0$. Строка $b=(b_n,..,b_1)$ принадлежит множеству B_n, если $b_1,..,b_n \in \{0,...,255\}$. При $n = 0$ множество B_n состоит из единственной пустой строки длины 0;
$\alpha \| \beta$	—	конкатенация двух байтовых строк $\alpha=(\alpha_{n_1},...,\alpha_1) \in B_{n_1}$ и $\beta=(\beta_{n_2},..., \beta_1) \in B_{n_2}$, т.е. строка $\gamma=(\alpha_{n_1},..., \alpha_1, \beta_{n_2},..., \beta_1) \in B_{n_1+n_2}$;
$R_r^n: B_n \rightarrow B_r$	—	усечение байтовой строки до размера r путем удаления младших $n-r$ байт, то есть: $R_r^n(\alpha_n,..., \alpha_{n-r+1}, \alpha_{n-r},..., \alpha_1) = (\alpha_n,..., \alpha_{n-r+1})$;
Int(i)	—	представление целого неотрицательного числа $i < 2^{32}$ в виде байтовой строки длины 4 $(i_4,i_3,i_2,i_1) \in B_4$, такой, что $i = i_1 + i_2 \cdot 2^8 + i_3 \cdot 2^{16} + i_4 \cdot 2^{24}$.

4 Алгоритм выработки ключа из пароля

Ключ *DK* вычисляют как функцию диверсификации PBKDF2 (*P, S, c, dkLen*) с использованием в качестве псевдослучайной функции PRF функции HMAC_GOSTR3411:

$$DK = \text{PBKDF2}(P, S, c, dkLen). \quad (1)$$

Функцию диверсификации вычисляют по следующему алгоритму:

1) Если $dkLen > (2^{32} - 1) \cdot 64$, то алгоритм завершает работу с ошибкой (неверные параметры).

2) Вычисляют $n = [dkLen/64]$.

3) Для каждого i от 1 до n вычисляют набор значений:

$$U_1(i) = \text{HMAC_GOSTR3411}(P, S \| \text{Int}(i))$$
$$U_2(i) = \text{HMAC_GOSTR3411}(P, U_1)$$
$$\ldots$$
$$U_c(i) = \text{HMAC_GOSTR3411}(P, U_{c-1}). \quad (2)$$

$$T(i) = U_1(i) \oplus U_2(i) \oplus \ldots \oplus U_c(i). \quad (3)$$

4) Ключ *DK* вычисляют как конкатенацию байтовых строк $\{T(i)\}$ с последующим усечением полученной последовательности до длины выходной последовательности:

$$DK = R_{dkLen}^{n \cdot 64}(T(1) \| T(2) \| \ldots \| T(n)). \quad (4)$$

5 Шифрование данных

Шифрование данных при использовании ключа *DK* осуществляют в соответствии со схемой PBES2, см. 6.2 [1], с использованием ГОСТ 28147—89 в режиме гаммирования с обратной связью.

Процесс шифрования в данной схеме выглядит следующим образом:

1) Выбирают случайное значение *S* размерности от 8 до 32 байт. Рекомендуемая размерность — 32 байта.

2) Число итераций *c* выбирают в зависимости от условий применения. Минимально допустимое значение параметра 1000, рекомендуемое 2000.

3) Устанавливают *dkLen* = 32.

4) Производят выработку последовательности *DK* = PBKDF2 (*P*, *S*, *c*, 32).

5) Ключ шифрования данных *K* получают усечением выходной последовательности *T*(1) до размерности 32, то есть $K = R_{32}^{64}(T(1))$.

6) Выбирают случайное значение синхропосылки *S'* размерности 8 байт.

7) Осуществляют шифрование данных по алгоритму ГОСТ 28147—89 (раздел 4) на ключе *K* с синхропосылкой *S'* в режиме гаммирования с обратной связью.

8) Параметры *S*, *c*, *S'* сохраняют в качестве параметров алгоритмов в соответствии с разделом 7.

Расшифрование данных осуществляют аналогичным образом с использованием параметров *S*, *c* и *S'*, применявшихся при зашифровании.

6 Контроль целостности

Для вычисления контрольной суммы передаваемых данных следует использовать схему PBMAC1, см. 7.1 [1], на основе функции HMAC_GOSTR3411 с ключом

$$DK = \text{PBKDF2}(P, S, c, 32). \quad (5)$$

7 Идентификаторы и параметры

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

7.1 PBKDF2

Объектный идентификатор для схемы PBKDF2:

```
id-PBKDF2 OBJECT IDENTIFIER ::= {pkcs-5 12}
```

Параметры алгоритма:

```
id-tc26-hmac-gost-3411-12-512 OBJECT IDENTIFIER ::= {iso(1) member-body(2) ru(643) reg7(7) tk26(1) algorithms(1) hmac(4) 512(2) }
 PBKDF2-params ::= SEQUENCE {
      salt CHOICE {
           specified OCTET STRING,
           otherSource AlgorithmIdentifier {{PBKDF2- SaltSources}}
      },
      iterationCount INTEGER (1000..MAX),
      keyLength INTEGER (32..MAX) OPTIONAL,
      prf AlgorithmIdentifier {{PBKDF2-PRFs}}
},
```

(6)

где

1) `salt` — значение случайной синхропосылки *S*, представленное в виде `OCTET STRING`;

2) `iterationCount` — число итераций алгоритма *c*;

3) `keyLength` — размер ключа в байтах; размер ключа в рамках схемы PBES2 может отсутствовать, так как всегда равен 32; в рамках схемы PBMAC1 он должен быть равен 32 и должен всегда присутствовать, так как функция HMAC_GOSTR3411 имеет переменный размер ключа;

4) `prf` — описание алгоритма псевдослучайной функции, где

```
prf.algorithm = id-tc26-hmac-gost-3411-12-512
prf.parameters = NULL.
```

7.2 PBES2

Объектный идентификатор для схемы PBES2:

```
id-PBES2 OBJECT IDENTIFIER ::= {pkcs-5 13}
```

Параметры алгоритма:

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

(7)

где

1) `keyDerivationFunc` — идентификатор и параметры алгоритма выработки парольного ключа PBKDF2 с параметрами в соответствии с 7.1;

2) `encryptionScheme` — идентификатор и параметры алгоритма шифрования ГОСТ 28147—89 в соответствии с [2]:

```
encryptionScheme.algorithm = id-Gost28147-89
encryptionScheme.parameters = Gost28147-89-Parameters
```

Параметры:

```
Gost28147-89-Parameters ::= SEQUENCE {
     iv         Gost28147-89-IV,
     encryptionParamSet   OBJECT IDENTIFIER
}
```

Gost28147-89-IV ::= OCTET STRING (SIZE (8)) должно содержать значение синхропосылки шифрования *S'*.

7.3 PBMAC1

Объектный идентификатор для схемы PBMAC1:

```
id-PBMAC1 OBJECT IDENTIFIER ::= {pkcs-5 14}.
```

Параметры алгоритма:

```
 PBMAC1-params ::= SEQUENCE {
      keyDerivationFunc AlgorithmIdentifier {{PBMAC1-KDFs}},
      messageAuthScheme AlgorithmIdentifier {{PBMAC1-MACs}},
```

(8)

где

1) keyDerivationFunc — идентификатор и параметры алгоритма выработки парольного ключа в соответствии с разделом PBKDF2;

2) messageAuthScheme — идентификатор алгоритма HMAC_GOSTR3411_2012_512.

8 Рекомендуемые криптографические параметры

При шифровании данных согласно схеме PBES2 рекомендуется использовать набор подстановок, описанный в [3].

Объектный идентификатор набора :

```
id-tc26-gost-28147-paramSetISO = OBJECT IDENTIFIER ::= { iso(1) member-
body(2) ru(643) rosstandart(7) tk26(1) algorithms(1) cipher(5) params(1)
tk26iso(1) }.
```

Приложение А
(справочное)

Контрольные примеры

Данные тестовые вектора сформированы по аналогии с тестовыми векторами из [4].

```
    Input:
      P = "password" (8 octets)
      S = "salt" (4 octets)
      c = 1
      dkLen = 64
DK = 64 77 0a f7 f7 48 c3 b1 c9 ac 83 1d bc fd 85 c2
61 11 b3 0a 8a 65 7d dc 30 56 b8 0c a7 3e 04 0d
28 54 fd 36 81 1f 6d 82 5c c4 ab 66 ec 0a 68 a4
90 a9 e5 cf 51 56 b3 a2 b7 ee cd db f9 a1 6b 47
```

```
    Input:
      P = "password" (8 octets)
      S = "salt" (4 octets)
      c = 2
      dkLen = 64
DK = 5a 58 5b af df bb 6e 88 30 d6 d6 8a a3 b4 3a c0
0d 2e 4a eb ce 01 c9 b3 1c 2c ae d5 6f 02 36 d4
d3 4b 2b 8f bd 2c 4e 89 d5 4d 46 f5 0e 47 d4 5b
ba c3 01 57 17 43 11 9e 8d 3c 42 ba 66 d3 48 de
```

```
    Input:
      P = "password" (8 octets)
      S = "salt" (4 octets)
      c = 4096
      dkLen = 64
DK = e5 2d eb 9a 2d 2a af f4 e2 ac 9d 47 a4 1f 34 c2
03 76 59 1c 67 80 7f 04 77 e3 25 49 dc 34 1b c7
86 7c 09 84 1b 6d 58 e2 9d 03 47 c9 96 30 1d 55
df 0d 34 e4 7c f6 8f 4e 3c 2c da f1 d9 ab 86 c3
```

```
    Input:
      P = "password" (8 octets)
      S = "salt" (4 octets)
      c = 16777216
      dkLen = 64
DK = 49 e4 84 3b ba 76 e3 00 af e2 4c 4d 23 dc 73 92
de f1 2f 2c 0e 24 41 72 36 7c d7 0a 89 82 ac 36
1a db 60 1c 7e 2a 31 4e 8c b7 b1 e9 df 84 0e 36
ab 56 15 be 5d 74 2b 6c f2 03 fb 55 fd c4 80 71
```

```
    Input:
      P = "passwordPASSWORDpassword" (24 octets)
      S = "saltSALTsaltSALTsaltSALTsaltSALTsalt" (36 octets)
      c = 4096
      dkLen = 100
DK = b2 d8 f1 24 5f c4 d2 92 74 80 20 57 e4 b5 4e 0a
07 53 aa 22 fc 53 76 0b 30 1c f0 08 67 9e 58 fe
4b ee 9a dd ca e9 9b a2 b0 b2 0f 43 1a 9c 5e 50
f3 95 c8 93 87 d0 94 5a ed ec a6 eb 40 15 df c2
bd 24 21 ee 9b b7 11 83 ba 88 2c ee bf ef 25 9f
33 f9 e2 7d c6 17 8c b8 9d c3 74 28 cf 9c c5 2a
2b aa 2d 3a
```

```
    Input:
      P = "pass\0word" (9 octets)
      S = "sa\0lt" (5 octets)
      c = 4096
      dkLen = 64
DK = 50 df 06 28 85 b6 98 01 a3 c1 02 48 eb 0a 27 ab
6e 52 2f fe b2 0c 99 1c 66 0f 00 14 75 d7 3a 4e
16 7f 78 2c 18 e9 7e 92 97 6d 9c 1d 97 08 31 ea
78 cc b8 79 f6 70 68 cd ac 19 10 74 08 44 e8 30
```

Библиография

[1]	PKCS#5	PKCS#5 (версия 2.1) Криптографический стандарт на основе пароля [Password-Based Cryptography Standard, RSA Laboratories, 2006]
[2]	RFC4490	С. Леонтьев, Г. Чудов. Использование алгоритмов ГОСТ 28147—89, ГОСТ Р 34.11—94, ГОСТ Р 34.10—94 и ГОСТ Р 34.10—2001 в синтаксисе криптографических сообщений (CMS) [S. Leontiev, G. Chudov. Using the GOST 28147—89, GOST R 34.11—94, GOST R 34.10—94, and GOST R 34.10—2001 Algorithms with Cryptographic Message Syntax (CMS), IETF RFC 4490, May 2006]
[3]	Методические рекомендации ТК 26	Информационная технология. Криптографическая защита информации. Задание узлов замены блока подстановки алгоритма шифрования ГОСТ 28147—89 (ТК26УЗ)
[4]	RFC6070	С. Йозефссон. PKCS#5 Основанная на пароле функция выработки ключа (PBKDF2). Тестовый набор [S. Josefsson. PKCS#5 Password-Based Key Derivation Function 2 (PBKDF2). Test Vectors, IETF RFC 6070, January 2011]

УДК 681.3.06:006.354 ОКС 35. 040 ОКСТУ 5002 П85

Ключевые слова: криптографические протоколы, пароль, ключ, шифрование, хэш-функция, аутентификация

Редактор *И.А. Сериков*
Технический редактор *В.Н. Прусакова*
Корректор *И.А. Королева*
Компьютерная верстка *А.А. Ворониной*

Сдано в набор 28.11.2016. Подписано в печать 08.12.2016. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,40. Уч.-изд. л. 1,26. Тираж 33 экз. Зак. 3074.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru