ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ
ПО СТАНДАРТИЗАЦИИ

**Р 1323565.1.008—2017**

# Информационная технология

# КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

## Использование режимов алгоритма блочного шифрования в защищенном обмене сообщениями между эмитентом и платежным приложением

Издание официальное

Москва
Стандартинформ
2018

gost.e-ecolog.ru

## Предисловие

1 РАЗРАБОТАНЫ Обществом с ограниченной ответственностью «Системы практической безопасности» (ООО «СПБ») совместно с Открытым акционерным обществом «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС») и Обществом с ограниченной ответственностью «КРИПТО-ПРО» (ООО «КРИПТО-ПРО»)

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 19 декабря 2017 г. № 2016-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, 2018

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 . . . . . 2
4 Описание алгоритмов . . . . . 3
4.1 Обеспечение контроля целостности ЗОС между платежным приложением карты и эмитентом . . . . . 3
4.2 Защита конфиденциальности ЗОС между платежным приложением карты и эмитентом . . . . . 3
4.3 Шифрование значений счетчиков при передаче эмитенту . . . . . 4
Приложение А (справочное) Контрольные примеры . . . . . 5

## Введение

В настоящих рекомендациях рассмотрены алгоритмы реализации механизмов скрипт-процессинга для обеспечения защищенного обмена сообщениями. Процедура скрипт-процессинга может быть выполнена в любое время после завершения обработки первой команды GENERATE AC.

Разработка настоящих рекомендаций вызвана необходимостью внедрения процедур для осуществления защищенного обмена сообщениями платежного приложения карты с эмитентом.

Примечание — Настоящие рекомендации дополнены приложением А.

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

**Информационная технология**

**КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ**

# Использование режимов алгоритма блочного шифрования в защищенном обмене сообщениями между эмитентом и платежным приложением

Information technology. Cryptographic data security.
Using block encryption algorithm modes in secure messaging between the issuer and the payment application

**Дата введения — 2018—06—01**

## 1 Область применения

Описанные в настоящих рекомендациях алгоритмы рекомендуется применять при защищенном обмене сообщениями в платежной системе «МИР».

Защищенный обмен сообщениями платежного приложения карты с эмитентом обеспечивается за счет использования механизмов скрипт-процессинга, а также шифрования оффлайновых счетчиков приложения. Реализация скрипт-процессинга подразумевает шифрование конфиденциальных данных команды (*PIN-block*), а также обеспечение целостности данных каждой команды. Инструкции скрипт-процессинга предназначены для изменения внутренних данных приложения, поэтому защищенный обмен сообщениями с эмитентом используется в ограниченном наборе APDU-команд.

## 2 Нормативные ссылки

В настоящих рекомендациях использованы нормативные ссылки на следующие документы:

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

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

Р 1323565.1.010—2017 Информационная технология. Криптографическая защита информации. Использование функции диверсификации для формирования производных ключей платежного приложения

Примечание — При пользовании настоящими рекомендациями целесообразно проверить действие ссылочных документов 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 документ, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого документа с учетом всех внесенных в данную версию изменений. Если заменен ссылочный документ, на который дана датированная ссылка, то рекомендуется использовать версию этого документа с указанным выше годом утверждения (принятия). Если после утверждения настоящих рекомендаций в ссылочный документ, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

**Издание официальное**

## 3 Обозначения

В настоящих рекомендациях использованы следующие обозначения:

$V_n$ — конечномерное векторное пространство размерности $n$;

$A||B$ — конкатенация строк, т. е. если $A \in V_{n1}$, $B \in V_{n2}$, $A = (a_{n1-1}, a_{n1-2}, ..., a_0)$, $B = (b_{n2-1}, b_{n2-2}, ..., b_0)$, то $A||B = (a_{n1-1}, a_{n1-2}, ..., a_0, b_{n2-1}, b_{n2-2}, ..., b_0) \in V_{n1+n2}$;

ЗОС — защищенный обмен сообщениями;

*SMI* — механизм обеспечения целостности передаваемых в команде (сообщении) данных и аутентификации источника данных (Secure Messaging for Integrity and Authentication);

*SMC* — механизм обеспечения конфиденциальности передаваемых данных (Secure Messaging for Confidentiality);

PIN — персональный идентификационный номер (Personal Identification Number). Длина значения равна 4—12 десятичным цифрам;

$SK_{SMI}$ — сессионный ключ, используемый для обеспечения целостности передаваемых в скриптовой команде данных и аутентификации источника данных команды; формируется в соответствии с Р 1323565.1.010—2017. Хранится в оперативной памяти карты только на протяжении одной транзакции, после удаляется. Длина значения равна 32 байтам;

*CLA||INS||P1||P2* — заголовок сообщения. Длина значения равна 4 байтам;

*CLA* — байт класса (Class Byte of the Command Message). Длина значения равна 1 байту;

*INS* — командный байт (Instruction Byte of Command Message). Длина значения равна 1 байту;

*P1* — параметр 1. Указывает элементы управления и опции для обработки команд. Если не используется, то принимает значение '0x00'. Длина значения равна 1 байту;

*P2* — параметр 2. Указывает элементы управления и опции для обработки команд. Если не используется, то принимает значение '0x00'. Длина значения равна 1 байту;

*IM* — значение имитовставки для сообщения. Длина значения равна 4 байтам;

$SK_{SMC}$ — сессионный ключ, используемый для обеспечения конфиденциальности передаваемых данных (*PIN-block*) в скриптовой команде; формируется в соответствии с Р 1323565.1.010—2017. Хранится в оперативной памяти карты только на протяжении одной транзакции, после удаляется. Длина значения равна 32 байтам;

$SK_{AC}$ — сессионный ключ карты, используемый для формирования прикладной криптограммы и формирования ключа шифрования счетчиков $SK_{COUNTER}$; формируется в соответствии с Р 1323565.1.010—2017. Хранится в оперативной памяти карты только на протяжении одной транзакции, после удаляется. Длина значения равна 32 байтам;

$SK_{COUNTER}$ — сессионный ключ, используемый для шифрования счетчиков. Длина значения равна 32 байтам;

AC Session Counter — счетчик количества генераций картой сессионных ключей $SK_{AC}$ с момента последней успешной проверки приложением величины ARPC. Длина значения равна 2 байтам;

SMI Session Key Counter — счетчик общего количества случаев вывода сессионных ключей $SK_{SMI}$, при которых проверка *IM* завершилась неудачно. Длина значения равна 2 байтам;

PIN Decipherment Counter — счетчик количества неверных операций расшифровок приложением *PIN-block* при оффлайновой проверке PIN. Длина значения равна 2 байтам;

Terminal Mutual Authentication Counter — счетчик количества неверных операций взаимной аутентификации приложения с терминалом. Длина значения равна 2 байтам;

*Counters* — блок значений счетчиков, состоящий из значений AC Session Counter, SMI Session Key Counter, PIN Decipherment Counter, Terminal Mutual Authentication Counter. Длина значения равна 8 байтам;

*PIN-block* — данные для вычисления шифрограммы. Длина значения равна 8 байтам.

## 4 Описание алгоритмов

Возможные значения аргументов функций в представленных алгоритмах ограничиваются допустимостью их использования в качестве входных параметров преобразований.

### 4.1 Обеспечение контроля целостности ЗОС между платежным приложением карты и эмитентом

#### 4.1.1 Алгоритм формирования значения имитовставки для сообщения скрипт-процессинга

Значение имитовставки вычисляется на ключе $SK_{SMI}$ в соответствии с ГОСТ 28147—89 с использование узла замены id-tc26-gost-28147-param-Z:

$IM = IM_{ГОСТ}(SK_{SMI})$ [X||Y],

где

X = (*CLA*||*INS*||*P1*||*P2*||'0x80'||'0x00'||'0x00'||'0x00')

Длина значения *X* равна 8 байтам.

Y = (*MSG*||'0x80'||'0x00'||...||'0x00')

Длина значения *Y* равна 264 байтам.

Сообщение *MSG* вычисляется в соответствии с таблицей 1.

Таблица 1

| Тэг 1 | Длина 1 | Значение 1 | Тэг 2 | Длина 2 |
|---|---|---|---|---|
| '87', если данные команды зашифрованы<br>'81', если данные команды передаются в открытом виде | Длина данных команды *L* | Данные (*L* байт) | '8E' | '04' |

Итоговый формат сообщения скрипт-процессинга после формирования имитовставки представляется в виде *MSG*||*IM*.

#### 4.1.2 Алгоритм проверки значения имитовставки для сообщения скрипт-процессинга

Для проверки значения имитовставки для сообщения необходимо выполнить расчет имитовставки аналогично 5.1.1 и сравнить полученное значение со значением таблицы 2.

Таблица 2

| Тэг 1 | Длина 1 | Значение 1 | Тэг 2 | Длина 2 | Значение 2 |
|---|---|---|---|---|---|
| '87', если данные команды зашифрованы<br>'81', если данные команды передаются в открытом виде | Длина данных команды *L* | Данные (*L* байт) | '8E' | '04' | Значение имитовставки |

Если значения совпадают, то значение счетчика SMI Session Key Counter уменьшается на 1.

Если значения не совпадают, то приложение должно отклонить команду скрипт-процессинга.

### 4.2 Защита конфиденциальности ЗОС между платежным приложением карты и эмитентом

#### 4.2.1 Алгоритм шифрования конфиденциальных данных PIN сообщения скрипт-процессинга

Для шифрования конфиденциальных данных PIN формируется *PIN-block* в следующем виде:

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| C | N | P | P | P | P | P/F | P/F | P/F | P/F | P/F | P/F | P/F | P/F | F | F |

Значение в каждом столбце имеет длину 4 бита.

Значение знаков *PIN-block* определены в таблице 3.

Таблица 3

| Знак в *PIN-block* | Имя | Значение |
|---|---|---|
| C | Контрольное поле | '2' ('0010'b) |
| N | Длина PIN | 4-битовый двоичный номер с допустимыми значениями в двоичном представлении от '0100'b до '1100'b (от 4 до 12 в десятичном представлении) |
| P | Цифра PIN | 4-битовое представление десятичной цифры PIN с допустимыми значениями от '0000'b до '1001'b (от 0 до 9 в десятичном представлении) |
| P/F | Цифра PIN/заполнитель | Определяется длиной PIN |
| F | Заполнитель | 4-битовое двоичное число '1111'b |

Шифрование *PIN-block* осуществляется на ключе $SK_{SMC}$ в соответствии с ГОСТ 28147—89 в режиме простой замены с узлом замены id-tc26-gost-28147-param-Z:

$Block1 = E_{ГОСТ}(SK_{SMC})$ [*PIN-block*]

**4.2.2 Алгоритм расшифрования конфиденциальных данных PIN сообщения скрипт-процессинга**

Расшифрование *PIN-block* осуществляется на ключе $SK_{SMC}$ в соответствии с ГОСТ 28147—89 в режиме простой замены с узлом замены id-tc26-gost-28147-param-Z:

$PIN\text{-}block = D_{ГОСТ}(SK_{SMC})$ [*Block*1]

Формат расшифрованного *PIN-block* должен соответствовать приведенному в 5.2.1. В противном случае приложение должно отклонить команду.

**4.3 Шифрование значений счетчиков при передаче эмитенту**

**4.3.1 Алгоритм шифрования счетчиков при передаче эмитенту**

Блок значений счетчиков шифруется на ключе $SK_{COUNTER}$ в соответствии с ГОСТ 28147—89 в режиме простой замены с узлом замены id-tc26-gost-28147-param-Z:

$Block2 = E_{ГОСТ}(SK_{COUNTER})$ [*Counters*]

Ключ $SK_{COUNTER}$ формируется из ключа $SK_{AC}$ по следующей схеме:

$SK_{COUNTER} = H(SK_{AC})$,

где $H$ — это хэш-функция ГОСТ Р 34.11—2012 с длиной выхода, равной 256 битам.

**4.3.2 Алгоритм расшифрования счетчиков при передаче эмитенту**

Блок значений счетчиков расшифровывается на ключе $SK_{COUNTER}$ в соответствии с ГОСТ 28147—89 в режиме простой замены с узлом замены id-tc26-gost-28147-param-Z:

$Counters = E_{ГОСТ}(SK_{COUNTER})$ [*Block2*]

Ключ $SK_{COUNTER}$ формируется из ключа $SK_{AC}$ по следующей схеме:

$SK_{COUNTER} = H(SK_{AC})$,

где $H$ — это хэш-функция ГОСТ Р 34.11—2012 с длиной выхода, равной 256 битам.

## Приложение А
## (справочное)

## Контрольные примеры

Приводимые ниже значения параметров PIN, *CLA*, *INS*, *P1*, *P2*, а также значения счетчиков AC Session Counter, SMI Session Key Counter, PIN Decipherment Counter, Terminal Mutual Authentication, значение сообщения *MSG* и значения ключей $SK_{SMI}$, $SK_{SMC}$, $SK_{AC}$ рекомендуется использовать только для проверки корректной работы конкретной реализации алгоритмов, описанных в настоящих рекомендациях.

Все числовые значения приведены в десятичной или шестнадцатеричной записи. Нижний индекс в записи числа обозначает основание системы счисления.

В данном приложении двоичные строки из $V^*$, длина которых кратна 4, записываются в шестнадцатеричном виде, а символ конкатенации («||») опускается. То есть строка $a \in V_{4r}$ будет представлена в виде $a_{r-1}\, a_{r-2} \ldots a_0$, где $a_i \in \{0, 1, \ldots, 9, a, b, c, d, e, f\}$, $i = 0, 1, \ldots, r-1$. Соответствие между двоичными строками длины 4 и шестнадцатеричными строками длины 1 задается естественным образом (таблица А.1).

Преобразование, ставящее в соответствие двоичной строке длины $4r$ шестнадцатеричную строку длины $r$, и соответствующее обратное преобразование для простоты записи опускаются.

Таблица А.1 — Соответствие между двоичными и шестнадцатеричными строками

| | |
|---|---|
| 0000 | 0 |
| 0001 | 1 |
| 0010 | 2 |
| 0011 | 3 |
| 0100 | 4 |
| 0101 | 5 |
| 0110 | 6 |
| 0111 | 7 |
| 1000 | 8 |
| 1001 | 9 |
| 1010 | a |
| 1011 | b |
| 1100 | c |
| 1101 | d |
| 1110 | e |
| 1111 | f |

### А.1 Исходные данные

Для вычисления имитовставки, шифрования конфиденциальных данных (PIN) и шифрования значения счетчиков используют следующие исходные данные:

PIN = $1234567_{10}$
Заголовок сообщения: $CLA||INS||P1||P2 = 211faa43_{16}$
Значение сообщения *MSG*: $MSG = 870445153fbb8e04_{16}$

Значения счетчиков:
AC Session Counter = $0001_{16}$
SMI Session Key Counter = $0001_{16}$
PIN Decipherment Counter = $0001_{16}$
Terminal Mutual Authentication = $0001_{16}$

Значения ключей:

$SK_{SMI}$ = 4*b*6*af*8*f*777*c*5001*d*6*ae*570*d*29*b*9*d*1*b*60\\
43777887*c*1*cc*4*db*64*feaa*8*ba*0*a*226788$_{16}$

$SK_{SMC}$ = 6*a*0*cd*3673*c*2*ce*5*e*8*f*32*c*5*c*6698829917\\
665*ff*5*b*8920750*fcec*465*c*2*ddc*271*c*14$_{16}$

$SK_{AC}$ = 5361ad354b17186e09deb20d37586d46\\
*a*64*f*8*cddd*699238*f*0210*db*7*d*9*e*6090*ed*$_{16}$

Символ «\\» обозначает перенос числа на новую строку.

**А.1.1 Имитовставка для сообщения**

Используя исходные данные, получают следующее значение имитовставки:

*IM* = 1*f*14115*e*$_{16}$

**А.1.2 Шифрование конфиденциальных данных (PIN)**

*PIN-block* = 271234567*ffffffff*$_{16}$

В результате применения алгоритма шифрования PIN получится следующее значение шифрограммы:

$E_{SK_{SMC}}$ (*PIN-block*) = 9073*bb*4*f*8*f*08*f*916$_{16}$

**А.1.3 Расшифрование PIN**

С использованием приведенных значений $SK_{SMC}$ и значения шифрограммы с помощью операции расшифрования воспроизводится исходное значение PIN.

**А.1.4 Ключ шифрования счетчиков**

На основе ключа $SK_{AC}$ формируется значение ключа $SK_{Counters}$

$SK_{Counters}$ = 93*a*20*f*29*d*3*e*4*c*445*e*47358003302*b*90*e*\\
223*ba*98*e*1*b*2*a*55*a*7*c*18*c*086634236*e*68$_{16}$

**А.1.5 Шифрование значения счетчиков**

*Counters* = 0001000100010001$_{16}$

В результате применения алгоритма шифрования счетчиков получится следующее значение шифрограммы:

$ESK_{Counters}$ (*Counters*) = *bdbdfd*20657*f*13*d*4$_{16}$

**А.1.6 Расшифрование значения счетчиков**

С использованием приведенных значений $SK_{Counters}$ и значения шифрограммы с помощью операции расшифрования воспроизводятся исходные значения счетчиков.

**А.2 Исходные данные**

Для вычисления имитовставки, шифрования конфиденциальных данных (PIN) и шифрования значения счетчиков используют следующие исходные данные:

PIN = $1234_{10}$

Заголовок сообщения: *CLA*||*INS*||*P*1||*P*2 = 0001*a*2*ac*$_{16}$

Значение сообщения *MSG*: *MSG* = 810545343*f*45*df*8*e*04$_{16}$

Значения счетчиков:

AC Session Counter = $0002_{16}$

SMI Session Key Counter = $0002_{16}$

PIN Decipherment Counter = $0002_{16}$

Terminal Mutual Authentication = $0002_{16}$

Значения ключей:

$SK_{SMI}$ = 88*f*8163*b*91*e*53*ccd*1*d*42*e*5*aed*806*b*2*f*2\\
*aa*022*e*3*b*558051642*ead*998*c*5*e*1*af*330$_{16}$

$SK_{SMC}$ = *c*7*d*8*fc*5*f*9*cb*04*f*9*b*86*f*30*f*0*f*6*e*40188*a*\\
*f*9513*abe*0*ffd*684261*d*89424*f*6*c*4680*a*$_{16}$

$SK_{AC}$ = 04*f*9*b*88*df*553*d*190*a*2*aeb*2*f*4*d*9*f*2*b*6*a*2\\
*f*4*ce*8*eac*89*eab*879*a*807866*c*0*ec*0*e*6*f*8$_{16}$

**А.2.1 Имитовставка для сообщения**

Используя исходные данные, получают следующее значение имитовставки:

*IM* = 48*b*0*d*8*a*6$_{16}$

**А.2.2 Шифрование конфиденциальных данных (PIN)**

*PIN-block* = 241234*fffffffff*$_{16}$

В результате применения алгоритма шифрования PIN получится следующее значение шифрограммы:

$E_{SK_{SMC}}$ (*PIN-block*) = *b*4*d*781574*ded*10*b*7$_{16}$

**А.2.3 Расшифрование PIN**

С использованием приведенных значений $SK_{SMC}$ и значения шифрограммы с помощью операции расшифрования воспроизводится исходное значение PIN.

**А.2.4 Ключ шифрования счетчиков**

На основе ключа $SK_{AC}$ формируется значение ключа $SK_{Counters}$

$SK_{Counters}$ = 1*dc*1c864*c*50*a*8*a*95*aba*515962*cad*0b42\\
13*cafcbb*75*c*3684*d*1*f*04151*ca*2*cb*75*ed*$_{16}$

**А.2.5 Шифрование значения счетчиков**

*Counters* = 0002000200020002$_{16}$

В результате применения алгоритма шифрования счетчиков получится следующее значение шифрограммы:

$E_{SK_{Counters}}$ (*Counters*) = 3ecefdcbf1c9d440$_{16}$

**А.2.6 Расшифрование значения счетчиков**

С использованием приведенных значений $SK_{Counters}$ и значения шифрограммы с помощью операции расшифрования воспроизводятся исходные значения счетчиков.

**А.3 Исходные данные**

Для вычисления имитовставки, шифрования конфиденциальных данных (PIN) и шифрования значения счетчиков используются следующие исходные данные:

PIN = 3247839010$_{10}$

Заголовок сообщения: *CLA*||*INS*||*P*1||*P*2 = 29cb34ac$_{16}$

Значение сообщения *MSG*: *MSG* = 8101658*e*04$_{16}$

Значения счетчиков:

AC Session Counter = 0003$_{16}$

SMI Session Key Counter = 0003$_{16}$

PIN Decipherment Counter = 0003$_{16}$

Terminal Mutual Authentication = 0003$_{16}$

Значения ключей:

$SK_{SMI}$ = *dca*82274*bd*029*bbe*9*e*4265*af*9651*de*4*a*\\
*c*61*b*55*c*3*bc*4*f*862*f*057*d*3*ed*549*ce*15*b*3$_{16}$

$SK_{SMC}$ = 3*aee*3354*c*808*edd*7*f*3*bca*1*f*77186*f*86*b*\\
550748*cebe*0882*e*072*e*7294*f*6*a*9660*e*5$_{16}$

$SK_{AC}$ = ed7e91da7485ca6324ae0e982d699e1e\\
3*bf*74*df*8*a*4691*c*231*ab*5*d*378*c*02*f*4367$_{16}$

**А.3.1 Имитовставка для сообщения**

Используя исходные данные, получают следующее значение имитовставки:

*IM* = 8114*cd*64$_{16}$

**А.3.2 Шифрование конфиденциальных данных (PIN)**

*PIN-block* = 2*a*3247839010*ffff*$_{16}$

В результате применения алгоритма шифрования PIN получится следующее значение шифрограммы:

$E_{SK_{SMC}}$ (*PIN-block*) = *fea*7*fedcc*32687*d*3$_{16}$

**А.3.3 Расшифрование PIN**

С использованием приведенных значений $SK_{SMC}$ и значения шифрограммы с помощью операции расшифрования воспроизводится исходное значение PIN.

**А.3.4 Ключ шифрования счетчиков**

На основе ключа $SK_{AC}$ формируется значение ключа $SK_{Counters}$

$SK_{Counters}$ = 2*ee*67*d*8*b*3*ccf*9*aadadd*03814*e*7*e*25439\\
8*ad*2*c*3*c*341*ee*30354*d*0*c*4025*eb*06*aec*1$_{16}$

**А.3.5 Шифрование значения счетчиков**

*Counters* = 0003000300030003$_{16}$

В результате применения алгоритма шифрования счетчиков получится следующее значение шифрограммы:

$E_{SK_{Counters}}$ (*Counters*) = 7*b*342*f*35259*e*9689$_{16}$

**А.3.6 Расшифрование значения счетчиков**

С использованием приведенных значений $SK_{Counters}$ и значения шифрограммы с помощью операции расшифрования воспроизводятся исходные значения счетчиков.

УДК 681.3.06:006.354 ОКС 35.040

Ключевые слова: информационная технология, криптографическая защита информации, аутентификация, ключ, защищенный обмен сообщениями, платежная карта, платежное приложение

БЗ 1—2018/93

Редактор *Л.С. Зимилова*
Технический редактор *И.Е. Черепкова*
Корректор *Е.Р. Ароян*
Компьютерная верстка *Ю.В. Поповой*

Сдано в набор 05.12.2017. Подписано в печать 14.02.2018. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,40. Уч.-изд. л. 1,26. Тираж 19 экз. Зак. 100.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ИД «Юриспруденция», 115419, Москва, ул. Орджоникидзе, 11.
gost.e-ecolog.ru gost.e-ecolog.ru

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123001, Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru