ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 19785-4— 2012

Информационные технологии

БИОМЕТРИЯ

Единая структура форматов обмена биометрическими данными

Часть 4

Спецификация формата блока защиты информации

ISO/IEC 19785-4:2010
Information technology — Common Biometric Exchange Formats Framework — Part 4: Security block format specifications
(IDT)

Издание официальное

Москва
Стандартинформ
2013

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0—2004 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

1 ПОДГОТОВЛЕН Ассоциацией автоматической идентификации «ЮНИСКАН/ГС1 РУС» на основе собственного аутентичного перевода на русский язык международного стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 355 «Технологии автоматической идентификации и сбора данных и биометрия»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 24 октября 2012 г. № 554-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 19785-4:2010 «Информационные технологии — Единая структура форматов обмена биометрическими данными — Часть 4: Спецификация формата блока защиты информации» (ISO/IEC 19785-4:2010 «Information technology — Common Biometric Exchange Formats Framework — Part 4: Security block format specifications»).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2004 (подраздел 3.5).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты Российской Федерации, сведения о которых приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

6 Некоторые элементы настоящего стандарта могут быть объектами получения патентных прав. Организации ИСО и МЭК не несут ответственности за установление подлинности каких-либо или всех таких патентных прав

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Национальные стандарты». Соответствующая информация, уведомления и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

Содержание

Введение

Комплекс стандартов ИСО/МЭК 19785 имеет общий заголовок «Информационные технологии. Единая структура форматов обмена биометрическими данными» и включает в себя следующие части:

- часть 1. Спецификация элементов данных;
- часть 2. Процедуры действий регистрационного органа в области биометрии;
- часть 3. Спецификации форматов ведущей организации;
- часть 4. Спецификация блока защиты информации.

Биометрическая верификация и идентификация являются важными технологиями, используемыми для верификации и/или идентификации личности. Биометрические данные для биометрических верификации и идентификации должны быть получены из проверенного источника и быть защищены от возможного повреждения в процессе передачи данных (должна быть обеспечена целостность передаваемых данных). Шифрование может применяться или не применяться в зависимости от требований безопасности. Настоящий стандарт устанавливает требования к обеспечению целостности и шифрованию биометрических данных.

Для обеспечения взаимодействия биометрических систем требования к единой структуре форматов обмена биометрическими данными (ЕСФОБД) установлены в ИСО/МЭК 19785-1 с целью ассоциирования дополнительных данных с одним или несколькими блоками биометрических данных (ББД). Блок защиты информации (БЗИ) обеспечивает защиту биометрических данных в соответствии с требованиями ИСО/МЭК 19785-1, но требования к содержанию и спецификации БЗИ в данном стандарте не установлены.

Если в формате ведущей организации не предусмотрено использование БЗИ, то в элементы данных CBEFF_BDB_encryption_options и CBEFF_BIR_integrity_options должны быть установлены значения NO ENCRYPTION и NO INTEGRITY соответственно.

Если в формате ведущей организации предусмотрено использование БЗИ, то может быть применен БЗИ, спецификация которого соответствует требованиям настоящего стандарта, или любой другой БЗИ. Кроме того, в элементах данных ЕСФОБД CBEFF_SB_format_owner и CBEFF_SB_format_type устанавливают значения, которые обеспечивают идентификацию используемого БЗИ.

Кроме БЗИ, требования к которым установлены в настоящем стандарте, допускается использовать БЗИ, предназначенные для конкретных целей. Например БЗИ, требования к которому установлены в ИСО/МЭК 24713-3 для документа МОТ*, удостоверяющего личность моряка.

В разделе 5 настоящего стандарта установлены требования к БЗИ общего применения, обеспечивающему возможность применения различных способов защиты информации с использованием шифрования и целостности, соответствующих RFC 3852 Cryptographic Message Syntax (CMS)** с некоторыми отличающимися от установленных в данном документе требованиями к EnvelopedData, EncryptedData, SignedData и AuthenticatedData***. Данные изменения введены с целью обеспечения соответствия требованиям к защите биометрической информации ЕСФОБД. В спецификации данного БЗИ предусмотрен также Authentication Context for Biometrics (ACBio)*4, требования к которому установлены в ИСО/МЭК 24761. ACBio также основан на схеме синтаксиса криптографических сообщений, определенной в RFC 3852. Использование ACBio позволяет определить уровни безопасности систем, формирующих аутентифицированные биометрические данные. ACBio также необходим для обеспечения (TAI)*5 [3].

В разделе 6 настоящего стандарта установлены требования к БЗИ, который обеспечивает только простые способы защиты информации и поддерживает только целостность.

Сноски в тексте стандарта, выделенные курсивом, приведены для пояснения текста оригинала.

---

* *МОТ — Международная организация труда.*

** *RFC 3852 Cryptographic Message Syntax (CMS) — регламентирующий документ Специальной комиссии интернет-разработок (Internet Engineering Task Force, IETF), обеспечивающий защиту информации, передаваемой в сети Интернет.*

*** *EnvelopedData, EncryptedData, SignedData и AuthenticatedData — упакованные данные, зашифрованные данные, данные с электронной подписью и данные из аутентифицированного источника соответственно.*

*4 *Authentication Context for Biometrics (ACBio) — аутентификационный статус для биометрии (АСБио).*

*5 *Telebiometric authentication infrastructure (TAI) — аутентификационная телебиометрическая инфраструктура.*

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

БИОМЕТРИЯ

Единая структура форматов обмена биометрическими данными

Часть 4

Спецификация формата блока защиты информации

Information technology. Biometrics. Common Biometric Exchange Formats Framework.
Part 4. Security block format specifications

Дата введения — 2013—01—01

1 Область применения

Настоящий стандарт устанавливает требования к форматам БЗИ (по ИСО/МЭК 19785-1), зарегистрированным в соответствии с ИСО/МЭК 19785-2 в качестве форматов, определенных биометрической организацией ЕСФОБД ИСО/МЭК СТК1/ПК37, а также требования к порядку присвоения зарегистрированного идентификатора формата БЗИ.

Примечание — Идентификатор формата БЗИ записывают в стандартный биометрический заголовок (СБЗ) формата ведущей организации ЕСФОБД или указывают, что использование другого БЗИ неприемлемо.

Формат БЗИ общего применения предусматривает возможность шифрования ББД и/или применения механизмов проверки целостности к СБЗ и ББД, а также использования ACBio (по ИСО/МЭК 24761). Данный БЗИ предусматривает возможность использования всех необходимых способов обеспечения защиты информации, включая использование любых параметров и алгоритмов шифрования и проверки целостности.

При формировании БЗИ для конкретных целей программное обеспечение использует различные алгоритмы и параметры, необходимые для пользователя БЗИ. Комплекс стандартов ИСО/МЭК 19785 не устанавливает требований к алгоритмам и параметрам формирования БЗИ.

Формат БЗИ, установленный в разделе 6 настоящего стандарта, является более ограниченным и простым, не предусматривает использования ACBio и шифрования ББД.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты и другие нормативные документы, которые необходимо учитывать при использовании настоящего стандарта. В случае ссылок на документы, у которых указана дата утверждения, необходимо пользоваться только указанной редакцией. В случае, когда дата утверждения не приведена, следует пользоваться последней редакцией ссылочных документов, включая любые поправки и изменения к ним:

ИСО/МЭК 8824 (все части) Информационные технологии. Абстрактная синтаксическая нотация версии один (АСН 1) (ISO/IEC 8824 (all parts), ITU—T Rec. X.680—683, Information technology — Abstract Syntax Notation One (ASN.1))

ИСО/МЭК 8825 (все части) Информационные технологии. Правила кодирования АСН.1 (ISO/IEC 8825 (all parts), ITU—T Rec. X.690—693, Information technology — ASN.1 encoding rules)

Издание официальное

ИСО/МЭК 9798-6 Информационные технологии. Методы защиты. Аутентификация объектов. Часть 6. Механизмы с применением ручной передачи данных (ISO/IEC 9798-6, Information technology — Security techniques — Entity authentication — Part 6: Mechanisms using manual data transfer)

ИСО/МЭК 19784-1 Информационные технологии. Биометрический программный интерфейс. Часть 1. Спецификация биометрического программного интерфейса (ISO/IEC 19784-1, Information technology — Biometric application programming interface — Part 1: BioAPI specification)

ИСО/МЭК 19785-1 Информационные технологии. Единая структура форматов обмена биометрическими данными. Часть 1. Спецификация элементов данных (ISO/IEC 19785-1, Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification)

ИСО/МЭК 24761 Информационные технологии. Методы защиты информации. Аутентификационный статус для биометрии (ISO/IEC 24761, Information technology — Security techniques — Authentication context for biometrics)

RFC 3852 Криптографический синтаксис сообщений (RFC 3852, Cryptographic Message Syntax (CMS), July 2004)

RFC 5911 Новые модули ACH.1 для криптографического синтаксиса сообщений и криптографической защиты сообщений электронной почты (RFC 5911, New ASN.1 Modules for Cryptographic Message Syntax (CMS) and S-MIME, June 2010)

3 Термины и определения

3.1 Термины, определенные в ИСО/МЭК 19785-1

В настоящем стандарте применены следующие термины, определенные в ИСО/МЭК 19785-1:
биометрический (biometric);
биометрия (biometrics);
блок биометрических данных (ББД) (biometric data block (BDB));
запись биометрической информации (ЗБИ) (biometric information record (BIR));
организация-участник ЕСФОБД (CBEFF biometric organization);
блок защиты информации (БЗИ) (security block (SB));
формат блока защиты информации (security block format);
идентификатор формата блока защиты информации (security block format identifier);
владелец формата блока защиты информации (security block format owner);
стандартный биометрический заголовок (СБЗ) (standard biometric header (SBH)).

3.2 Термины, определенные в ИСО/МЭК 19784-1

В настоящем стандарте применен следующий термин, определенный в ИСО/МЭК 19784-1:
модуль БиоАПИ (BioAPI Unit).

3.3 Термины, определенные в ИСО/МЭК 24761

В настоящем стандарте применены следующие термины, определенные в ИСО/МЭК 24761:
отчет АСБио (ACBio instance);
аутентификационный статус для биометрии (АСБио) (authentication context for biometrics (ACBio));
модуль обработки биометрических данных (МОБД) (biometric processing unit (BPU)).

3.4 Термины, определенные в ИСО/МЭК 9798-6

В настоящем стандарте применен следующий термин, определенный в ИСО/МЭК 9798-6:
аутентификационный код сообщения (message authentication code).

4 Обозначения и сокращения

4.1 Обозначения и сокращения по ИСО/МЭК 19785-1

В настоящем стандарте применены следующие обозначения и сокращения по ИСО/МЭК 19785-1:
ББД (BDB);
ЗБИ (BIR);
ЕСФОБД (CBEFF);
БЗИ (SB);
СБЗ (SBH).

4.2 Обозначения и сокращения по ИСО/МЭК 24761

В настоящем стандарте применены следующие обозначения и сокращения по ИСО/МЭК 24761:
АСБио (ACBio);
МОБД (BPU).

4.3 Обозначения и сокращения по ИСО/МЭК 9798-6

В настоящем стандарте применено следующее обозначение по ИСО/МЭК 9798-6:
АКС (MAC).

4.4 Обозначения и сокращения по RFC 3852

В настоящем стандарте применено следующее обозначение по RFC 3852:
СОС* (CRL).

5 Формат блока защиты информации общего назначения

5.1 Владелец

ИСО/МЭК СТК1/ПК37

5.2 Идентификатор владельца

257 (0101Hex). Данный идентификатор присвоен биометрической организации ИСО/МЭК СТК1/ПК37 по ИСО/МЭК 19785-2.

5.3 Наименование

ISO/IEC JTC 1/SC 37 CBEFF general-purpose security block format

5.4 Идентификатор

1 (0001 Hex). Данный идентификатор зарегистрирован в соответствии с требованиями ИСО/МЭК 19785-2 с использованием DER (см. ИСО/МЭК 8825-1).

2 (0002 Hex). Данный идентификатор зарегистрирован в соответствии с требованиями ИСО/МЭК 19785-2 с использованием PER (см. ИСО/МЭК 8825-2).

3 (0003 Hex). Данный идентификатор зарегистрирован в соответствии с требованиями ИСО/МЭК 19785-2 с использованием XER (см. ИСО/МЭК 8825-3).

5.5 Идентификаторы объектов ACH.1 для данного формата

5.5.1 Запись с использованием DER

{iso registration–authority cbeff(19785) organizations(0) jtc–sc37 (257) sb–formats(3) general–purpose(0) der–encoding(1)}

или значение в нотации XML:

1.1.19785.0.257.3.0.1

5.5.2 Запись с использованием PER

{iso registration–authority cbeff(19785) organizations(0) jtc–sc37 (257) sb–formats(3) general–purpose(0) per–encoding(2)}

или значение в нотации XML:

1.1.19785.0.257.3.0.2

5.5.3 Запись с использованием XER

{iso registration–authority cbeff(19785) organizations(0) jtc–sc37 (257) sb–formats(3) general–purpose(0) xer–encoding(3)}

или значение в нотации XML:

1.1.19785.0.257.3.0.3

5.6 Область применения

БЗИ общего применения используют при необходимости применения целостности и/или шифрования, а также отчетов АСБио.

5.7 Идентификатор версии

Формату БЗИ, установленному в настоящем разделе, присвоен следующий идентификатор версии: основное значение — (0), вспомогательное значение — (0).

---

* *Список отозванных сертификатов (СОС) — certificate revocation list (CRL).*

5.8 Спецификация формата и требования к соответствию

5.8.1 Общие положения

5.8.1.1 В настоящем разделе БЗИ представляет собой тип CBEFFSecurityBlock в нотации АСН.1, состоящий из последовательности типов CBEFFSecurityBlockElement в нотации АСН.1.

```
CBEFFSecurityBlock ::= SEQUENCE OF CBEFFSecurityBlockElement
CBEFFSecurityBlockElement ::= CHOICE {
        elementCBEFFSB ContentInfoCBEFFSB,
        subBlockForACBio SubBlockForACBio,
        accumulatedACBioInstances ACBioInstances
        }
```

5.8.1.2 Для типа CBEFFSecurityBlockElement существует три альтернативы: ContentInfoCBEFFSB, SubBlockForACBio и ACBioInstances. ContentInfoCBEFFSB* содержит информацию о целостности СБЗ и ББД или о шифровании ББД. Два последних типа содержат информацию об АСБио (см. ИСО/МЭК 24761).

5.8.1.3 Тип ContentInfoCBEFFSB представляет собой следующую запись:

```
ContentInfoCBEFFSB ::= SEQUENCE {
        contentType CONTENT–TYPE.&id({ContentTypeCBEFF}),
        content [0] EXPLICIT CONTENT–TYPE.&Type
            ({ContentTypeCBEFF}{@contentType})
        }
```

Примечание — Тип CBEFFSecurityBlockElement должен быть использован в качестве замены типа ContentInfo, требования к которому установлены в RFC 5911. Первый компонент типа CBEFFSecurityBlockElement может содержать только четыре идентификатора объектов: id–envelopeRelatedData, id–encryptionRelatedData, id–signatureRelatedData, или id–authenticationRelatedData, в то время как тип ContentInfo, требования к которому установлены в RFC 5911, может содержать также другие идентификаторы объектов.

Тип ContentInfoCBEFFSB используют дважды при записи CBEFFSecurityBlock: первый раз для поддержки целостности, второй — для поддержки шифрования.

Тип ContentInfoCBEFFSB состоит из двух компонентов: contentType и content, первый из которых представляет собой идентификатор объекта для данных, содержащихся во втором компоненте. Значение contentType представляет собой один из следующих идентификаторов объектов: id-envelopeRelatedData, id-encryptionRelatedData, id-signatureRelatedData или id-authenticationRelatedData, что соответствует текущему определению типа ContentTypeCBEFF, состоящему из четырех CONTENT–TYPEs. В настоящем стандарте для типа CONTENT–TYPE предусмотрен идентификатор объекта с типом, записанным в АСН.1.

```
ContentTypeCBEFF CONTENT–TYPE ::= { envelopeRelatedData | encryptionRelatedData |
                        signatureRelatedData | authenticationRelatedData}
envelopeRelatedData CONTENT–TYPE ::= {
        EnvelopeRelatedData
        IDENTIFIED BY id–envelopeRelatedData
}
encryptionRelatedData CONTENT–TYPE ::= {
        EncryptionRelatedData
        IDENTIFIED BY id–encryptionRelatedData
}
signatureRelatedData CONTENT–TYPE ::= {
        SignatureRelatedData
        IDENTIFIED BY id–signatureRelatedData
}
authenticationRelatedData CONTENT–TYPE ::= {
        AuthenticationRelatedData
        IDENTIFIED BY id–authenticationRelatedData
}
```

---

* *В оригинале ИСО/МЭК 19785-4 допущена ошибка — вместо ContentInfoCBEFFSB указано CBEFFSecurityBlockElement.*

Четырем вышеуказанным наименованиям объектов присвоены следующие идентификаторы объектов:

```
id–envelopeRelatedData OBJECT IDENTIFIER ::= {
        iso(1) standard(0) cbeff(19785) contentType(1) envelopeRelatedData(1)
}
id–encryptionRelatedData OBJECT IDENTIFIER ::= {
        iso(1) standard(0) cbeff(19785) contentType(1) encryptionRelatedData(2)
}
id–signatureRelatedData OBJECT IDENTIFIER ::= {
        iso(1) standard(0) cbeff(19785) contentType(1) signatureRelatedData(3)
}
id–authenticationRelatedData OBJECT IDENTIFIER ::= {
        iso(1) standard(0) cbeff(19785) contentType(1) authenticationRelatedData(4)
}
```

id–envelopeRelatedData или id–encryptionRelatedData используют в составе компонента contentType типа ContentInfoCBEFFSB в случае, если элемент данных CBEFF_BDB_encryption_options (см. ИСО/МЭК 19785-1) имеет значение ENCRYPTION.

id–signatureRelatedData или id–authenticationRelatedData используют в составе компонента contentType типа ContentInfoCBEFFSB в случае, если элемент данных CBEFF_BIR_integrity_options (см.ИСО/МЭК 19785-1) имеет значение INTEGRITY.

5.8.1.4 Данные типа SubBlockForACBio предназначены также для использования в МОБД модуля БиоАПИ, который генерирует отчет АСБио. Эти данные один МОБД модуля БиоАПИ передает другому модулю. Тип SubBlockForACBio представляет собой следующую запись:

```
SubBlockForACBio ::= SEQUENCE {
        bpuIOIndex INTEGER,
        acbioInstance ACBioInstance
}
```

Первый компонент данного типа — bpuIOIndex представляет собой BPU IO index* блока информации при передаче от одного МОБД другому. Второй компонент является отчетом АСБио генерированным первым МОБД (ИСО/МЭК 24761).

5.8.1.5 Данные типа ACBioInstances представляет собой последовательность отчетов АСБио исключая последний, который записывают в тип SubBlockForACBio.Таким образом тип ACBioInstances представляет собой последовательность типов ACBioInstance**.

```
ACBioInstances ::= SEQUENCE OF ACBioInstance
```

5.8.1.6 Таким образом ЗБИ может обеспечивать возможность использования:

1) шифрования, если значение ENCRYPTION установлено в элементе данных CBEFF_DBD_encryption_options или это является обязательным требованием формата ведущей организации;

2) целостности, если значение INTEGRITY установлено в элементе данных CBEFF_BIR_integrity_options или это является обязательным требованием формата ведущей организации;

3) шифрования и целостности или одного из этих компонентов, если это является требованием формата ведущей организации.

5.8.2 Шифрование

Если в элементе данных СБЗ CBEFF_BDB_encryption_options установлено значение ENCRYPTION, ЗБИ должна содержать тип ContentInfoCBEFFSB, первым компонентом которого является id–envelopeRelatedData или id–encryptionRelatedData. В соответствии с требованиями 5.1.8.3, содержание второго компонента устанавливает первый компонент типа ContentInfoCBEFFSB, то есть, если первым компонентом является id–envelopeRelatedData, то вторым должен быть EnvelopeRelatedData, и, если первым компонентом является id–encryptionRelatedData, то вторым должен быть EncryptionRelatedData. ББД в этом случае должен содержать биометрические данные в зашифрованной форме.

Примечание 1 — Различия между компонентами EnvelopeRelatedData и EncryptionRelatedData зависят от системы управления ключами (см.RFC 3852).

---

* *BPU IO index — см. ИСО/МЭК 24761.*

** *В оригинале ИСО/МЭК 19785-4 вместо ACBioInstance ошибочно указано ACBioInstances.*

Примечание 2 — Элементы данных СБЗ содержат значения, описывающие незашифрованный ББД (до проведения шифрования), и не описывают атрибуты зашифрованной ББД.

5.8.2.1 Содержание типа envelopeRelatedData

5.8.2.1.1 Содержание типа envelopeRelatedData устанавливает идентификатор объекта id–envelopeRelatedData в соответствии с типом EnvelopeRelatedData в нотации АСН.1 (см. 5.8.1.3).

a) EnvelopeRelatedData содержит информацию об алгоритме шифрования и зашифрованных ключах шифрования для одного или нескольких получателей. Зашифрованные биометрические данные находятся в ББД. Биометрические данные могут быть зашифрованы для произвольного числа получателей с помощью любой из поддерживаемых технологий управления ключами шифрования для каждого пользователя.

Примечание — Подробная информация о системе управления ключами шифрования приведена в RFC 3852.

b) Пользователь расшифровывает один из зашифрованных ключей шифрования, входящих в состав данных типа EnvelopeRelatedData, а затем с помощью данного ключа расшифровывает биометрические данные, находящиеся в ББД.

5.8.2.1.2 Тип EnvelopeRelatedData представляет собой следующую запись:

```
EnvelopeRelatedData::= SEQUENCE {
        version CBEFFSBVersion DEFAULT v0,
        originatorInfo [0] IMPLICIT OriginatorInfo OPTIONAL,
        recipientInfos RecipientInfos,
    contentEncryptionAlgorithm ContentEncryptionAlgorithmIdentifier
}
```

a) поле version предназначено для указания версии типа CBEFFSBVersion и представляет собой следующую запись:

```
CBEFFSBVersion ::= INTEGER { v0(0) } ( v0, ... )
```

b) поле originatorInfo типа OriginatorInfo предназначено для указания информации об устройстве, сгенерировавшим БЗИ. Данное поле присутствует только в том случае, если этого требует алгоритм управления ключами. Данное поле может содержать сертификаты и СОС. Требования к типу OriginatorInfo установлены в RFC 3852 и RFC 5911;

c) поле recipientInfos типа RecipientInfos предназначено для записи информационных блоков о получателях. Данное поле должно содержать не менее одного информационного блока. Тип RecipientInfos представляет собой последовательность типов RecipientInfo. Требования к типу RecipientInfo установлены в RFC 3852 и RFC 5911;

d) поле contentEncryptionAlgorithm предназначено для указания алгоритма шифрования и вспомогательных параметров, использованных для шифрования биометрических данных. Для всех пользователей указывают единый алгоритм и ключ шифрования.

5.8.2.2 Тип encryptionRelatedData

5.8.2.2.1 Информационное содержимое типа encryptionRelatedData представляет собой идентификатор объекта id–encryptionRelatedData в соответствии с типом EncryptionRelatedData, записанным в нотации АСН.1 (см. 5.8.1.3):

a) в отличие от типа envelopeRelatedData, тип encryptionRelatedData не содержит информации об алгоритме шифрования и зашифрованных ключах шифрования для получателей. Управление ключами шифрования должно осуществляться другими способами.

Примечание — Информационное содержимое типа encryptionRelatedData используют при шифровании биометрических данных для локального хранения, при этом ключи шифрования получают с помощью паролей;

b) тип EncryptionRelatedData представляет собой следующую запись:

```
EncryptionRelatedData ::= SEQUENCE {
    version CBEFFSBVersion DEFAULT v0,
    contentEncryptionAlgorithm ContentEncryptionAlgorithmIdentifier
}
```

5.8.3 Целостность

Если в элементе данных CBEFF_BIR_integrity_options установлено значение INTEGRITY, ЗБИ должен содержать тип ContentInfoCBEFFSB, первым компонентом которого является id–signatureRelatedData или id–authenticationRelatedData. В соответствии с требованиями 5.1.8.3 содер-

жание второго компонента устанавливает первый компонент типа ContentInfoCBEFFSB, то есть, если первым компонентом является id–signatureRelatedData, то вторым должен быть SignatureRelatedData, и, если первым компонентом является id–authenticationRelatedData, то вторым должен быть AuthenticationRelatedData. Таким образом, тип signatureRelatedData используют в том случае, если для обеспечения целостности биометрических данных используют цифровую подпись, и тип authenticationRelatedData должен быть использован, если биометрические данные защищены АКС. Цифровую подпись и АКС записывают в СБЗ или в ББД (в том числе зашифрованном).

5.8.3.1 Содержание типа signatureRelatedData

5.8.3.1.1 Содержание типа signatureRelatedData устанавливает идентификатор объекта id–signatureRelatedData в соответствии с типом SignatureRelatedData, записанным в нотации АСН.1 (см. 5.8.1.3).

a) SignatureRelatedData представляет собой одну или несколько цифровых подписей. Любое количество подписывающих инстанций (далее — подписантов) могут параллельно использовать цифровую подпись для последовательности данных СБЗ и для записи ББД (в том числе зашифрованного). В отличие от типа SignedData (см. RFC 3852 и RFC 5911) тип SignatureRelatedData не содержит данных, к которым была применена цифровая подпись;

b) процесс создания SignatureRelatedData включает в себя следующие этапы, изображенные на рисунке 1 слева:

1) для каждого подписанта дайджест сообщения (или хеш-значение) вычисляют из последовательности данных СБЗ и записи ББД (в том числе зашифрованной) с использованием специфического для данного подписанта алгоритма (САПС*). Результатом является сформированный дайджест сообщения (ДС**);

2) для каждого подписанта, к дайджесту сообщения применяют цифровую подпись с использованием закрытого ключа подписчика (ЗКП***) и специфического алгоритма подписи подписчика (САПП*[4]);

3) для каждого подписанта значение цифровой подписи (ЦП) и другие данные являются значением SignerInfo, требования к которому установлены в RFC 3852 и RFC 5911. Сертификаты и СОС каждого подписанта, а также другие данные, не относящиеся к какому-либо другому подписанту, сохраняются на данном этапе;

4) специфические алгоритмы дайджеста сообщения и соответствующие значения SignerInfo всех подписантов в свою очередь становятся значением SignatureRelatedData;

c) процесс верификации SignatureRelatedData включает в себя несколько этапов (см. справа на рисунке 1). Получатель вычисляет дайджест сообщения (ДС*[5]) из последовательности данных СБЗ и записи ББД (в том числе зашифрованной), используя специфический алгоритм дайджеста сообщения (САДС). Данный дайджест сообщения и открытый ключ подписанта (ОКП*[6]) используют для проверки значения цифровой подписи (ЦП) путем сравнения дайджеста сообщения, вычисленного в процессе верификации (ДС) и дайджеста сообщения подписанта (ДС'). Значение ДС' находящееся в цифровой подписи (ЦП), расшифровывают с помощью открытого ключа подписанта (ОКП) и специфического алгоритма подписи подписанта (САПП*[7]). Открытый ключ подписанта определяют с помощью наименования и оригинального серийного номера организации-разработчика данной системы цифровой подписи или с помощью идентификационного ключа для однозначной идентификации сертификата подписанта, содержащего открытый ключ. Сертификат подписанта может быть включен в содержимое поля certificates типа SignatureRelatedData.

На рисунке 1 пунктирной линией от ЗКП к полю «certificates» указан способ включения в поле «certificates» сертификата открытого ключа, относящегося к закрытому ключу подписанта.

---

* *САДС (специфический алгоритм дайджеста сообщения) — signer–specific message–digest algorithm (DA).*

** *ДС (дайджест сообщение) — message digest (MD).*

*** *ЗКП (закрытый ключ подписчика) — signer's private key (PrK).*

[4] САПП (специфический алгоритм подписи подписанта) — signer-specific signature algorithm (SA).

[5] В оригинале ИСО/МЭК 19785-3 допущена опечатка — вместо сокращения DS указано сокращение DS'.

[6] Открытый ключ подписанта (ОКП) — signer's public key (PbK).

[7] В оригинале ИСО/МЭК 19785-3 допущена опечатка — вместо сокращения SA указано сокращение DS.

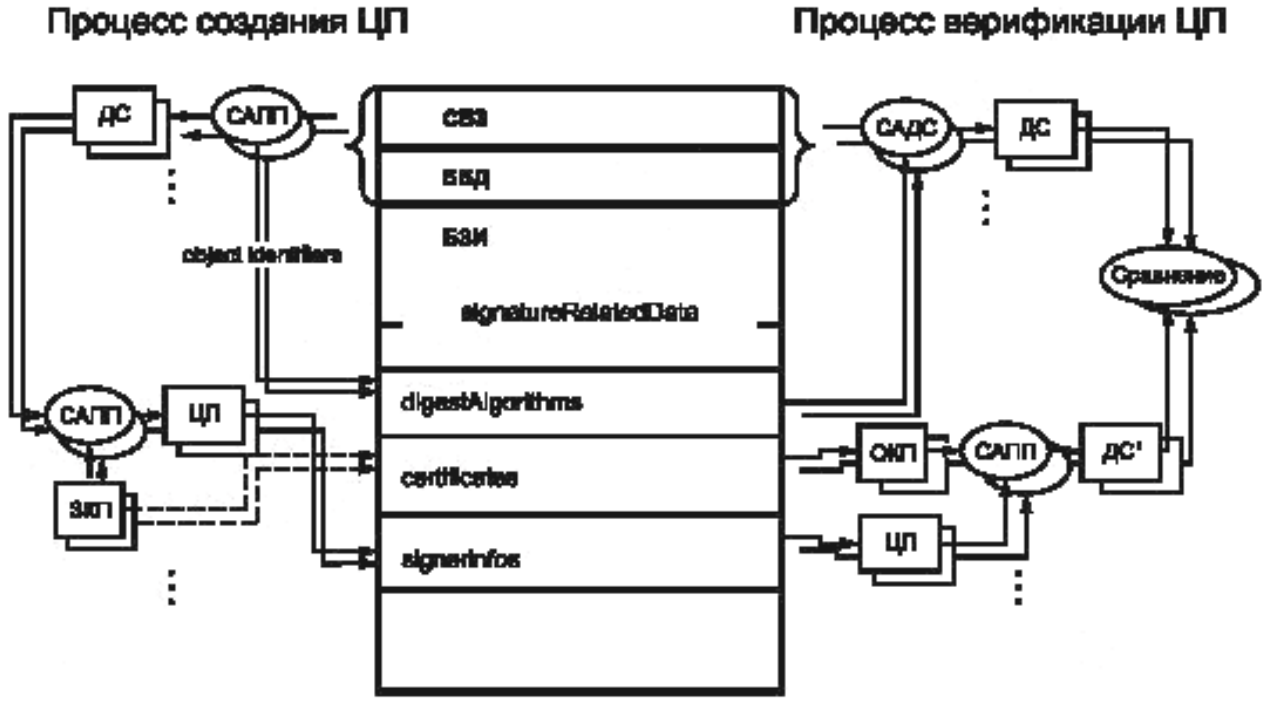

Рисунок 1 — Процессы создания и верификации ЦП

5.8.3.1.2 Тип SignatureRelatedData представляет собой следующую запись:

```
SignatureRelatedData ::= SEQUENCE {
        version CBEFFSBVersion DEFAULT v0,
        digestAlgorithms SET OF DigestAlgorithmIdentifier,
        certificates [0] IMPLICIT CertificateSet OPTIONAL,
        crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,
        signerInfos SignerInfos
}
```

a) version представляет собой номер версии спецификации блока защиты информации типа CBEFFSBVersion по 5.8.2.1.2;

b) digestAlgorithms представляет собой значение типа DigestAlgorithmIdentifiers, содержащего набор идентификаторов специфических алгоритмов дайджеста сообщения. Каждый идентификатор представлен вместе с дополнительными параметрами одного или нескольких подписантов. Данный набор содержит идентификаторы всех САДС всех подписантов в любом порядке. Настоящий стандарт не устанавливает требований к использованию определенного алгоритма криптографического хеширования;

c) certificates представляет собой набор сертификатов. Необходимо, чтобы этот набор содержал необходимую информацию о последовательности от «корневого» сертификата или сертификата от органа, выдающего сертификаты до сертификатов подписантов, записанных в поле signerInfos. Число сертификатов может быть больше, чем необходимо; возможно наличие сертификатов, достаточных для хранения последовательности сертификатов от двух и более независимых органов высшего уровня, выдающих сертификаты. Сертификатов может быть меньше в случае, если предполагается, что у получателей есть альтернативные способы получения необходимых сертификатов (например, из предыдущего набора). Сертификат подписанта также может быть включен в набор сертификатов;

d) crls представляет собой информацию об отозванных сертификатах. Данная информация позволяет определить, действительны ли сертификаты, однако данная информация не является обязательной. Списки отозванных сертификатов (СОС) являются основным источником информации об отозванных (недействительных) сертификатах. Число СОС может быть как больше, так и меньше, чем необходимо;

e) signerInfos представляет собой набор информационных элементов о подписантах. В данном компоненте может быть любое количество элементов. Требования к типу SignerInfo установлены в RFC 3852 и RFC 5911.

5.8.3.2 Содержание типа authenticationRelatedData

5.8.3.2.1 Содержание типа authenticationRelatedData устанавливает идентификатор объекта id–authenticationRelatedData в соответствии с типом AuthenticationRelatedData, записанным в нотации АСН.1 (см. 5.8.1.3):

a) тип AuthenticationRelatedData состоит из аутентификационного кода сообщения (АКС) и зашифрованных аутентификационных ключей, предназначенных для одного или нескольких получателей. Комбинация АКС и одного аутентификационного ключа необходима получателю для проверки целостности последовательности СБЗ и ББД (в том числе зашифрованного). В отличие от содержания типа AuthenticatedData, установленного в RFC 3852, тип AuthenticationRelatedData не содержит данных, которые должны быть аутентифицированы;

b) процесс создания AuthenticationRelatedData включает в себя следующие этапы:

1) генерирование случайным образом аутентификационного ключа сообщения для определенного аутентификационного алгоритма сообщения;

2) шифрование аутентификационного ключа сообщения для каждого получателя. Способ шифрования зависит от используемого алгоритма управления ключами;

3) внесение в RecipientInfo (требование к использованию типа RecipientInfo установлены в RFC 3852 и RFC 5911) зашифрованного аутентификационного ключа сообщения и другой специфической для получателя информации;

4) вычисление отправителем АКС с использованием аутентификационного ключа сообщения на основании последовательности СБЗ и ББД (в том числе зашифрованного). АКС записывают в поле mac.

5.8.3.2.2 Тип AuthenticationRelatedData представляет собой следующую запись:

```
AuthenticationRelatedData ::= SEQUENCE {
    version CBEFFSBVersion DEFAULT v0,
    originatorInfo [0] IMPLICIT OriginatorInfo OPTIONAL,
    recipientInfos RecipientInfos,
    macAlgorithm MessageAuthenticationCodeAlgorithm,
    mac MessageAuthenticationCode
}
```

a) version представляет собой номер версии спецификации БЗИ;

b) originatorInfo предназначен для записи информации о генерирующем устройстве. Данная информация необходима в случае, если этого требует алгоритм управления ключами, и может включать в себя сертификаты, атрибутивные сертификаты и СОС;

c) recipientInfos предназначен для набора информации о получателе. В данном наборе должен быть, как минимум, один элемент;

d) macAlgorithm представляет собой идентификатор алгоритма аутентификационного кода сообщения (АКС), идентифицирующий алгоритм АКС и связанные с ним параметры, используемые генерирующим устройством. Содержание поля macAlgorithm предназначено для облегчения однопроходной обработки данных получателем;

e) mac представляет собой АКС.

5.8.4 Шифрование и проверка целостности

5.8.4.1 Если элементы данных CBEFF_BDB_encryption_options и CBEFF_BIR_integrity_options поддерживаются СБЗ и их значениями являются ENCRYPTION и INTEGRITY соответственно, БЗИ должен содержать элементы шифрования и проверки целостности.

5.8.4.2 Шифрование должно быть проведено до проверки целостности. Последовательность действий должна быть следующей:

1) биометрические данные (ББД) зашифровывают и записывают в поле ББД;

2) генерируют данные типов EnvelopeRelatedData или EncryptionRelatedData и вносят их в БЗИ;

3) из последовательности СБЗ и ББД генерируют одну или несколько цифровых подписей или АКС;

4) генерируют данные типов SignatureRelatedData или AuthenticationRelatedData и включают их в БЗИ.

5.8.4.3 Проверку целостности проводят до процесса расшифровывания. Последовательность действий должна быть следующей:

1) одну или несколько цифровых подписей или АКС получают из данных типов SignatureRelatedData или AuthenticationRelatedData БЗИ;

2) проверку целостности последовательности СБЗ и зашифрованного ББД проводят с помощью цифровой подписи или АКС;

3) информацию о шифровании получают из данных типов EnvelopeRelatedData или EncryptionRelatedData БЗИ;

4) расшифровывают ББД для получения исходного ББД.

Проверка целостности может быть выполнена без расшифровывания.

5.9 Запись абстрактных значений

Запись данных БЗИ проводят следующим образом:

a) побитовую запись СБЗ проводят в соответствии с требованиями используемого формата ведущей организации;

b) побитовую запись ББД проводят в соответствии с требованиями спецификации формата ББД;

c) запись CBEFFSecurityBlock проводят в соответствии с подразделом 5.5 и приложением А настоящего стандарта.

6 Формат блока защиты информации, использующий только цифровую подпись

6.1 Владелец

ИСО/МЭК СТК1/ПК37

6.2 Идентификатор владельца

257 (0101 Hex). Данный идентификатор присвоен биометрической организации ИСО/МЭК СТК1/ПК37 в соответствии с требованиями ИСО/МЭК 19785-2.

6.3 Наименование

ISO/IEC JTC1/SC 37 signature–only security block format

6.4 Идентификатор

4 (0004 Hex). Данный идентификатор зарегистрирован в соответствии с требованиями ИСО/МЭК 19785-2 для кодирования с использованием DER (см. ИСО/МЭК 8825-1).

5 (0005 Hex). Данный идентификатор зарегистрирован в соответствии с требованиями ИСО/МЭК 19785-2 для кодирования с использованием PER (см. ИСО/МЭК 8825-2).

6 (0006 Hex). Данный идентификатор зарегистрирован в соответствии с требованиями ИСО/МЭК 19785-2 для кодирования с использованием XER (см. ИСО/МЭК 8825-3).

6.5 Идентификаторы объектов АСН.1 для данного формата

6.5.1 Запись с использованием DER

{iso registration–authority cbeff(19785) biometric–organization(0) jtc1–sc37(257) sbformats(3) signature–only(2) der–encoding(1)}

или значение в нотации XML:

1.1.19785.0.257.3.2.1

6.5.2 Запись с использованием PER

{iso registration–authority cbeff(19785) biometric–organization(0) jtc1–sc37(257) sbformats(3) signature–only(2) per–encoding(2)}

или значение в нотации XML:

1.1.19785.0.257.3.2.2

6.5.3 Запись с использованием XER

{iso registration–authority cbeff(19785) biometric–organization(0) jtc1–sc37(257) sbformats(3) signature–only(2) xer–encoding(3)}

или значение в нотации XML:

1.1.19785.0.257.3.2.3

6.6 Область применения

Блок защиты информации, использующий только цифровую подпись, применяют в случаях, когда требуется только цифровая подпись и не требуется шифрование. Данный формат предоставляет возможность использования форматированных с помощью синтаксиса криптографических сообщений данных, подписанных с использованием личной информации без применения дополнительных механизмов защиты информации. Блок защиты информации, использующий только цифровую подпись, не поддерживает использование отчетов АСБио, а также множественных цифровых подписей.

Примечание — Данный формат соответствует требованиям [4].

6.7 Идентификатор версии

Формату ЗБИ, установленному в настоящем разделе, присвоен следующий идентификатор версии: основное значение — (0), вспомогательное значение — (0).

6.8 Спецификация формата и требования к соответствию

Блок защиты информации, использующий только цифровую подпись, должен представлять собой запись, соответствующую требованиям RFC 3852, или данные типа SignedData в нотации АСН.1, соответствующие требованиям вышеуказанного документа.

Примечание — В RFC 3852 установлено требование к использованию отличительных (DER) правил кодирования (ИСО/МЭК 8825-1*) для записи SignedData.

Цифровую подпись применяют к записи, соответствующей требованиям ЕСФОБД (СБЗ и ББД) за исключением БЗИ, использующего только цифровую подпись.

Данный формат БЗИ должен соответствовать следующим требованиям, установленным в RFC 3852:

- значением CMSVersion должно быть v3;
- encapcontentInfo не должно содержать поля eContent field;
- поле certificates должно иметь нулевое значение или содержать один certificate (если такое требование установлено конкретным применением), который используют для проверки signature записанного в поле SignerInfo;
- поле crls не используют;
- поле signerInfos должно содержать один SignerInfo;
- SignerInfo должен содержать:
    - значение issuerAndSerialNumber для элемента SignerIdentifier;
    - атрибут MessageDigest для хеш-значения последовательности СБЗ и ББД.

---

* *В оригинале ИСО/МЭК 19785-4 вместо ISO/IEC 8825-1 ошибочно указано ISO 8825-1.*

Приложение А
(обязательное)

Модуль ACH.1 для формата блока защиты информации

Данный модуль ACH.1 был проверен на наличие ошибок с помощью специального инструмента ACH.1, предназначенного для синтаксической проверки.

```
CBEFF-GENERAL-PURPOSE-SECURITY-BLOCK
        {iso(1) standard(0) cbeff(19785) module(0) sb(16) rev(0)}
DEFINITIONS AUTOMATIC TAGS ::= BEGIN
IMPORTS
-- RFC 5911 ASN.1 Module for RFC 3852 Cryptographic Message Syntax
        ContentEncryptionAlgorithmIdentifier,
        SignerInfos, MessageAuthenticationCodeAlgorithm,
        DigestAlgorithmIdentifier, AuthAttributes, MessageAuthenticationCode,
        OriginatorInfo, RecipientInfos
        FROM CryptographicMessageSyntax2004 {
            iso(1) member-body(2) us(840) rsadsi(113549)
            pkcs(1) pkcs-9(9) smime(16) modules(0) cms-2004(24)}
-- ISO/IEC 24761 Authentication context for biometrics
        ACBioInstance, CertificateSet, RevocationInfoChoices
        FROM AuthenticationContextForBiometrics {
            iso(1) standard(0) acbio(24761) module(1) acbio(2) rev(0)} ;
CONTENT-TYPE ::= TYPE-IDENTIFIER
CBEFFSecurityBlock ::= SEQUENCE OF CBEFFSecurityBlockElement
CBEFFSecurityBlockElement ::= CHOICE {
          elementCBEFFSB ContentInfoCBEFFSB,
          subBlockForACBio SubBlockForACBio,
          accumulatedACBioInstances ACBioInstances
}
ContentInfoCBEFFSB ::= SEQUENCE {
        contentType CONTENT-TYPE.&id({ContentTypeCBEFF}),
        content [0] EXPLICIT CONTENT-TYPE.&Type
            ({ContentTypeCBEFF}{@contentType})
}
ContentTypeCBEFF CONTENT-TYPE ::= { envelopeRelatedData | encryptionRelatedData |
                    signatureRelatedData | authenticationRelatedData}
EnvelopeRelatedData::= SEQUENCE {
        version CBEFFSBVersion DEFAULT v0,
        originatorInfo [0] IMPLICIT OriginatorInfo OPTIONAL,
        recipientInfos RecipientInfos,
        contentEncryptionAlgorithm ContentEncryptionAlgorithmIdentifier
}
CBEFFSBVersion ::= INTEGER { v0(0) } ( v0, ... )
EncryptionRelatedData ::= SEQUENCE {
        version CBEFFSBVersion DEFAULT v0,
        contentEncryptionAlgorithm ContentEncryptionAlgorithmIdentifier
}
SignatureRelatedData ::= SEQUENCE {
        version CBEFFSBVersion DEFAULT v0,
        digestAlgorithms SET OF DigestAlgorithmIdentifier,
        certificates [0] IMPLICIT CertificateSet OPTIONAL,
        crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,
        signerInfos SignerInfos
}
AuthenticationRelatedData ::= SEQUENCE {
        version CBEFFSBVersion DEFAULT v0,
        originatorInfo [0] IMPLICIT OriginatorInfo OPTIONAL,
```

```
            recipientInfos RecipientInfos,
            macAlgorithm MessageAuthenticationCodeAlgorithm,
            mac MessageAuthenticationCode
}
SubBlockForACBio ::= SEQUENCE {
            bpuIOIndex INTEGER,
            acbioInstance ACBioInstance
}
ACBioInstances ::= SEQUENCE OF ACBioInstance
- - contentType object identifiers
id-envelopeRelatedData OBJECT IDENTIFIER ::= {
        iso(1) standard(0) cbeff(19785) contentType(1) envelopeRelatedData(1)
}
id-encryptionRelatedData OBJECT IDENTIFIER ::= {
        iso(1) standard(0) cbeff(19785) contentType(1) encryptionRelatedData(2)
}
id-signatureRelatedData OBJECT IDENTIFIER ::= {
        iso(1) standard(0) cbeff(19785) contentType(1) signatureRelatedData(3)
}
id-authenticationRelatedData OBJECT IDENTIFIER ::= {
        iso(1) standard(0) cbeff(19785) contentType(1) authenticationRelatedData(4)
}
- - ContentType objects
envelopeRelatedData CONTENT-TYPE ::= {
            EnvelopeRelatedData
            IDENTIFIED BY id-envelopeRelatedData
}
encryptionRelatedData CONTENT-TYPE ::= {
            EncryptionRelatedData
            IDENTIFIED BY id-encryptionRelatedData
}
signatureRelatedData CONTENT-TYPE ::= {
            SignatureRelatedData
            IDENTIFIED BY id-signatureRelatedData
}
authenticationRelatedData CONTENT-TYPE ::= {
            AuthenticationRelatedData
            IDENTIFIED BY id-authenticationRelatedData
}
END - - CBEFF-SECURITY-BLOCK
```

Приложение В
(справочное)

Отличия типов, установленных в RFC 5911

Большинство типов, входящих в нотацию АСН.1, используемых в настоящем стандарте, установлены в RFC 3852, однако некоторые типы заменены на аналогичные. В данном приложении указаны отличия между этими типами.

В.1 Отличие EnvelopeRelatedData от EnvelopedData

EnvelopeRelatedData по настоящему стандарту отличается от EnvelopedData, требования к которому установлены в RFC 5911.

EnvelopedData представляет собой:

```
EnvelopedData ::= SEQUENCE {
        version CMSVersion,
        originatorInfo [0] OriginatorInfo OPTIONAL,
        recipientInfos RecipientInfos,
        encryptedContentInfo EncryptedContentInfo,
        unprotectedAttrs [1] UnprotectedAttributes OPTIONAL
}
```

EnvelopeRelatedData представляет собой:

```
EnvelopeRelatedData::= SEQUENCE {
        version CBEFFSBVersion DEFAULT v0,
        originatorInfo [0] IMPLICIT OriginatorInfo OPTIONAL,
        recipientInfos RecipientInfos,
        contentEncryptionAlgorithm ContentEncryptionAlgorithmIdentifier
}
```

Отличие EnvelopeRelatedData от EnvelopedData заключается в том, что первый не включает в себя поля encryptedContentInfo* и поля unproctectedAttrs. Согласно требованиям RFC 5911 зашифрованные данные помещают в поле encryptedContent типа EncryptedContent, в котором EnvelopedData может быть представлена в виде вложенной структуры. В случае использования ЕСФОБД зашифровывают только биометрические данные и сохраняют их в ББД, поэтому нет необходимости их представления в виде вложенной структуры. При расшифровывании ББД необходимо наличие поля contentEncryptionAlgorithm типа ContentEncryptionAlgorithmIdentifier, которое является последним в записи типа EnvelopeRelatedData.

В.2 Отличие EnvelopeRelatedData от EncryptedData

Определение EncryptionRelatedData, представленное в настоящем стандарте, основано на EncryptedData,требования к которому установлены в RFC 5911.

EncryptedData представляет собой:

```
EncryptedData ::= SEQUENCE {
        version CMSVersion,
        encryptedContentInfo EncryptedContentInfo,
        unprotectedAttrs [1] UnprotectedAttributes OPTIONAL
}
```

EncryptionRelatedData представляет собой:

```
EncryptionRelatedData ::= SEQUENCE {
        version CBEFFSBVersion DEFAULT v0,
        contentEncryptionAlgorithm ContentEncryptionAlgorithmIdentifier
}
```

Отличие EncryptionRelatedData от EncryptedData аналогично указанному в В.1.

В.3 Отличие SignatureRelatedData от SignedData

Определение SignatureRelatedData, представленное в настоящем стандарте, основано на SignedData, требования к которому установлены в RFC 5911.

---

* *В оригинале ИСО/МЭК 19785-4 вместо encryptedContentInfo ошибочно указано encryptionContentInfo.*

SignedData представляет собой:

```
SignedData ::= SEQUENCE {
        version CMSVersion,
        digestAlgorithms SET OF DigestAlgorithmIdentifier,
        encapContentInfoEncapsulatedContentInfo,
        certificates [0] CertificateSet OPTIONAL,
        crls [1] RevocationInfoChoices OPTIONAL,
        signerInfos SignerInfos
}
```

SignatureRelatedData представляет собой:

```
SignatureRelatedData ::= SEQUENCE {
        version CBEFFSBVersion DEFAULT v0,
        digestAlgorithms SET OF DigestAlgorithmIdentifier,
        certificates [0] IMPLICIT CertificateSet OPTIONAL,
        crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,
        signerInfos SignerInfos
}
```

Отличие между SignatureRelatedData и SignedData заключается в том, что SignatureRelatedData не включает в себя поля encapContentInfo. В соответствии с требованием RFC 5911, данные с цифровой подписью помещают в поле encapContentInfo типа EncapsulatedContentInfo, в котором SignedData может быть представлена в виде вложенной структуры. Однако в случае использования ЕСФОБД цифровую подпись применяют только к СБЗ и ББД (возможно, зашифрованного), которые сохраняются соответственно в каждом блоке, поэтому не требуется их представление в виде вложенной структуры.

B.4 Отличие AuthenticationRelatedData от AuthenticatedData

AuthenticationRelatedData, представленное в настоящем стандарте, основано на AuthenticatedData, требования к которому установлены в RFC 5911.

AuthenticatedData представляет собой:

```
AuthenticatedData ::= SEQUENCE {
        version CMSVersion,
        originatorInfo [0] IMPLICIT OriginatorInfo OPTIONAL,
        recipientInfos RecipientInfos,
        macAlgorithm MessageAuthenticationCodeAlgorithm,
        digestAlgorithm [1] DigestAlgorithmIdentifier OPTIONAL,
        encapContentInfo EncapsulatedContentInfo,
        authAttrs [2] AuthAttributes OPTIONAL,
        mac MessageAuthenticationCode,
        unauthAttrs [3] UnauthAttributes OPTIONAL
}
```

AuthenticationRelatedData представляет собой:

```
AuthenticationRelatedData ::= SEQUENCE {
        version CBEFFSBVersion DEFAULT v0,
        originatorInfo [0] IMPLICIT OriginatorInfo OPTIONAL,
        recipientInfos RecipientInfos,
        macAlgorithm MessageAuthenticationCodeAlgorithm,
        mac MessageAuthenticationCode
}
```

Отличие между AuthenticationRelatedData и AuthenticatedData заключается в том, что AuthenticationRelatedData не включает в себя поля encapContentInfo. В соответствии с требованием RFC 5911, сгенерированный АКС помещают в поле encapContentInfo типа EncapsulatedContentInfo, в котором AuthenticatedData может быть представлена в виде вложенной структуры. В случае использования ЕСФОБД цифровую подпись применяют только к СБЗ и ББД (возможно, зашифрованного), которые сохраняются соответственно в каждом блоке, и поэтому не требуется их представление в виде вложенной структуры. Для представления биометрической информации в соответствии с требованиями ЕСФОБД не требуется использование полей authAttrs и unauthAttrs, поэтому они не входят в состав AuthenticationRelatedData. Кроме того, AuthenticationRelatedData не содержит поля digestAlgorithm, так как оно используется только при наличии поля authAttrs (см. RFC 5911).

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО/МЭК 8824-1:2008	IDT	ГОСТ Р ИСО/МЭК 8824-1—2001 «Информационная технология. Абстрактная синтаксическая нотация версии один (АСН.1). Часть 1. Спецификация основной нотации»
ИСО/МЭК 8824-2:2008	IDT	ГОСТ Р ИСО/МЭК 8824-2—2001 «Информационная технология. Абстрактная синтаксическая нотация версии один (АСН.1). Часть 2. Спецификация информационного объекта»
ИСО/МЭК 8824-3:2008	IDT	ГОСТ Р ИСО/МЭК 8824-3—2002 «Информационная технология. Абстрактная синтаксическая нотация версии один (АСН.1). Часть 3. Спецификация ограничения»
ИСО/МЭК 8824-4:2008	IDT	ГОСТ Р ИСО/МЭК 8824-4—2003 «Информационная технология. Абстрактная синтаксическая нотация версии один (АСН.1). Часть 4. Параметризация спецификации АСН.1»
ИСО/МЭК 8825-1:2008	IDT	ГОСТ Р ИСО/МЭК 8825-1—2003 «Информационная технология. Правила кодирования АСН.1. Часть 1. Спецификация базовых (BER), канонических (CER) и отличительных (DER) правил кодирования»
ИСО/МЭК 8825-2:2008	IDT	ГОСТ Р ИСО/МЭК 8825-2—2003 «Информационная технология. Правила кодирования АСН.1. Часть 2. Спецификация правил уплотненного кодирования (PER)»
ИСО/МЭК 8825-3:2008	—	*
ИСО/МЭК 8825-4:2008	IDT	ГОСТ Р ИСО/МЭК 8825-4—2009 «Информационная технология. Правила кодирования АСН.1. Часть 4. Правила XML кодирования (XER)»
ИСО/МЭК 8825-5:2008	—	*
ИСО/МЭК 8825-6:2008	—	*
ИСО/МЭК 9798-6	—	*
ИСО/МЭК 19784-1	IDT	ГОСТ Р ИСО/МЭК 19784-1—2007 «Автоматическая идентификация. Идентификация биометрическая. Биометрический программный интерфейс. Часть 1. Спецификация биометрического программного интерфейса»
ИСО/МЭК 19785-1	IDT	ГОСТ Р ИСО/МЭК 19785-1—2007 «Автоматическая идентификация. Идентификация биометрическая. Единая структура форматов обмена биометрическими данными. Часть 1. Спецификация элементов данных»
ИСО/МЭК 24761	—	*

* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:
- IDT — идентичные стандарты.

Библиография

[1] ISO/IEC 19785-2 (Information technology — Common Biometric Exchange Formats Framework — Part 2: Procedures for the operation of the Biometric Registration Authority)

[2] ISO/IEC 24713-3 Information technology — Biometric profiles for interoperability and data interchange — Part 3: Biometrics—based verification and identification of seafarers

[3] ITU–T Rec. X.1089 Telebiometrics authentication infrastructure

[4] FIPS PUB 201–1 (Change Notice 1) Federal Information Processing Standards Publication, Personal Identity Verification (PIV) of Federal Employees and Contractors

УДК 004.93'1:006.89:006.354 ОКС 35.040 П 85

Ключевые слова: информационные технологии, единая структура, форматы обмена биометрическими данными, спецификация формата, блок защиты информации

Редактор *Т.А. Леонова*
Технический редактор *В.Н. Прусакова*
Корректор *М.С. Кабашова*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 14.03.2013. Подписано в печать 09.04.2013. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 2,79. Уч.-изд. л. 2,40. Тираж 84 экз. Зак. 372.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ.
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.