ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ГОСТ Р ИСО/МЭК 24713-2— 2011**

# ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

# БИОМЕТРИЯ

## Биометрические профили для взаимодействия и обмена данными

### Часть 2

## Контроль физического доступа сотрудников аэропортов

**ISO/IEC 24713-2:2008**
**Information technology — Biometric profiles for interoperability and data interchange — Part 2: Physical access control for employees at airports (IDT)**

**Издание официальное**

Москва
Стандартинформ
2012

gost.e-ecolog.ru

## 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 Научно-исследовательским и испытательным центром биометрической техники Московского государственного технического университета имени Н.Э. Баумана (НИИЦ БТ МГТУ им. Н.Э. Баумана) на основе собственного аутентичного перевода на русский язык стандарта, указанного в пункте 4, при консультативной поддержке Ассоциации автоматической идентификации «ЮНИСКАН/ГС1 РУС»

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 13 декабря 2011 г. № 1200-ст.

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 24713-2–2008 «Информационные технологии. Биометрические профили для взаимодействия и обмена данными. Часть 2. Контроль физического доступа сотрудников аэропортов» (ISO/IEC 24713-2:2008 «Information technology — Biometric profiles for interoperability and data interchange — Part 2: Physical access control for employees at airports»).

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

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

5 ВВЕДЕН ВПЕРВЫЕ

*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, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет*

© Стандартинформ, 2012

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

## Содержание

1 Область применения . . . . . 1
2 Соответствие . . . . . 1
3 Нормативные ссылки . . . . . 2
4 Термины и определения . . . . . 3
5 Условия . . . . . 4
5.1 Специальные условия . . . . . 4
5.2 Архитектура . . . . . 5
5.3 Токен . . . . . 5
5.4 Система управления токеном . . . . . 5
5.5 Система управления и контроля . . . . . 6
5.6 Административная система управления и контроля . . . . . 6
5.7 Инфраструктура . . . . . 6
6 Процесс . . . . . 6
6.1 Общие положения . . . . . 6
6.2 Подтверждение достоверности . . . . . 7
6.3 Регистрация . . . . . 7
6.4 Выдача . . . . . 7
6.5 Активация в локальной системе контроля доступа . . . . . 7
6.6 Использование . . . . . 8
7 Меры по обеспечению безопасности . . . . . 9
Приложение А (обязательное) Список требований . . . . . 10
Приложение В (справочное) Дополнительная информация . . . . . 37
Приложение С (справочное) Меры по обеспечению безопасности . . . . . 39
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации . . . . . 41
Библиография . . . . . 42

## Введение

Настоящий стандарт входит в серию международных стандартов, разрабатываемых ИСО/МЭК СТК 1/ПК 37. Они обеспечивают возможность взаимодействия и обмена данными между биометрическими приложениями и системами*. В стандартах данной серии определены требования к применению биометрии в различных приложениях по распознаванию личности вне зависимости от того, функционируют ли данные приложения в среде открытых систем или состоят из единственной замкнутой системы.

Биометрические стандарты ИСО/МЭК СТК 1/ПК 37 представляют собой многоуровневый набор стандартов, включающий в себя форматы обмена биометрическими данными и биометрические интерфейсы наравне с биометрическими профилями, в которых определяются способы использования данных стандартов в конкретных областях приложений.

Стандарты форматов обмена биометрическими данными определяют записи обмена биометрическими данными для разных биометрических модальностей. Стороны, заранее договорившиеся обмениваться записями обмена биометрическими данными, как определено в стандартах форматов обмена биометрическими данными ИСО/МЭК СТК 1/ПК 37, должны быть способны осуществлять биометрическое распознавание при использовании данных друг друга. Стороны должны быть способны осуществлять биометрическое распознавание даже в том случае, если конкретные стандарты форматов обмена биометрическими данными, которые должны быть применены, заранее не были оговорены, но их системы базируются на биометрических стандартах ИСО/МЭК СТК 1/ПК 37.

Стандарты биометрических интерфейсов включают в себя ИСО/МЭК 19785, описывающий единую структуру форматов обмена биометрическими данными (ЕСФОБД), и ИСО/МЭК 19784, описывающий биометрический программный интерфейс (БиоАПИ). Данные стандарты обеспечивают обмен биометрическими данными в рамках одной системы или между системами. В ИСО/МЭК 19785 определена базовая структура стандартизированной записи биометрической информации (ЗБИ), включающая в себя запись обмена биометрическими данными с добавленными метаданными, представляющими собой дату захвата, дату истечения срока использования, информацию о том, зашифрованы данные или нет, и т. д. В ИСО/МЭК 19784 определена открытая система программных пользовательских интерфейсов (АПИ), обеспечивающая связь между приложениями и основополагающими услугами биометрических технологий. Также БиоАПИ устанавливает формат ЗБИ согласно ЕСФОБД для хранения и передачи полученных им данных.

Стандарты биометрических профилей способствуют реализациям базовых стандартов (например, ИСО/МЭК СТК 1/ПК 37 стандартов форматов обмена биометрическими данными и биометрического программного интерфейса и, возможно, небиометрических стандартов) для определенных приложений. Стандарты биометрических профилей определяют функции приложения (например, контроль физического доступа сотрудников аэропортов) и устанавливают порядок применения вариантов, описанных в базовых стандартах, для обеспечения возможности биометрического взаимодействия.

---

* *Открытые системы основаны на соответствующих стандартам форматах данных, интерфейсах и протоколах для обеспечения обмена данными и способности к взаимодействию с другими системами, которые могут включать в себя компоненты, отличающиеся с точки зрения устройства и производства. Замкнутая система также может соответствовать стандартам и включать в себя компоненты, отличающиеся с точки зрения устройства и производства, но, по сути, к ней могут не предъявляться требования к обмену данными и взаимодействию с другими системами.*

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

# ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

# БИОМЕТРИЯ

## Биометрические профили для взаимодействия и обмена данными

## Часть 2

## Контроль физического доступа сотрудников аэропортов

Information technologies. Biometrics. Biometric profiles for interoperability and data interchange. Part 2. Physical access control for employees at airports

**Дата введения — 2013—01—01**

## 1 Область применения

Настоящий стандарт определяет биометрический профиль, включающий в себя необходимые параметры и интерфейсы для взаимодействия функциональных модулей (то есть основанных на БиоАПИ модулей и внешнего интерфейса), для поддержания биометрической идентификации и верификации сотрудников, осуществляемых при помощи токенов в локальных точках доступа (двери или иные контролируемые входы) и вдоль локальных границ в рамках определенной контролируемой области в аэропорту. Токен должен содержать один или более биометрических эталонов.

В настоящем стандарте не рассматривается полная система контроля доступа, предназначенная для использования в точках доступа в рамках обеспечения безопасности в аэропорту. Предполагается, что подобные системы существуют и биометрическая составляющая, рассматриваемая в настоящем стандарте, будет внедрена в существующую систему. Вследствие этого исключаются из рассмотрения такие понятия, как параметры устройства, оповещение об исключительных ситуациях и ошибках и их обработка. Данная информация содержится в справочном приложении С.

Настоящий стандарт содержит руководящие указания по регистрации, проверке списка отслеживания, предотвращению повторной выдачи и верификации личности сотрудников аэропортов. В нем также описаны архитектуры и бизнес-процессы, необходимые для поддержки управления идентичностью, основанного на применении токенов в среде обеспечения безопасности аэропорта.

Настоятельно рекомендуется, чтобы конфиденциальность, целостность и доступность биометрических данных были защищены в соответствии с местными, региональными или национальными законами.

Настоящий стандарт не исключает возможности того, что созданные пользователями приложения, основанные на настоящем стандарте, могут также отвечать требованиям к конфиденциальности/защите данных. Определение требований к конфиденциальности/защите данных выходит за рамки области применения настоящего стандарта.

## 2 Соответствие

Система контроля доступа соответствует требованиям настоящего стандарта в том случае, если она корректно осуществляет все функции и обладает всеми необходимыми техническими характеристиками, определенными в списке требований, и предоставляет декларацию соответствия реализации (ДСР) для определенных профилей в соответствии с приложением А. Стоит также отметить, что системе могут быть предъявлены дополнительные требования к ее возможностям, помимо указанных в базовых стандартах.

**Издание официальное**

## 3 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты, 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 19784-1:2006 Информационные технологии. Биометрический программный интерфейс. Часть 1. Спецификация биометрического программного интерфейса (ISO/IEC 19784-1:2006, Information technology — Biometric application programming interface — Part 1: BioAPI specification)

ИСО/МЭК 19785-1:2006 Информационные технологии. Единая структура форматов обмена биометрическими данными. Часть 1. Спецификация элементов данных (ISO/IEC 19785-1:2006, Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification)

ИСО/МЭК 19785-3:2007 Информационные технологии. Единая структура форматов обмена биометрическими данными. Часть 3. Спецификация формата организации патрона (ISO/IEC 19785-3:2007, Information technology — Common Biometric Exchange Formats Framework — Part 3: Patron format specifications)

ИСО/МЭК 19794-2:2005 Информационные технологии. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца — контрольные точки (ISO/IEC 19794-2:2005, Information technology — Biometric data interchange formats — Part 2: Finger minutiae data)

ИСО/МЭК 19794-3:2006 Информационные технологии. Форматы обмена биометрическими данными. Часть 3. Спектральные данные изображения отпечатка пальца (ISO/IEC 19794-3:2006, Information technology — Biometric data interchange formats — Part 3: Finger pattern spectral data)

ИСО/МЭК 19794-4:2005 Информационные технологии. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца (ISO/IEC 19794-4:2005, Information technology — Biometric data interchange formats — Part 4: Finger image data)

ИСО/МЭК 19794-5:2005 Информационные технологии. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица (ISO/IEC 19794-5:2005, Information technology — Biometric data interchange formats — Part 5: Face image data)

ИСО/МЭК 19794-6:2005 Информационные технологии. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза (ISO/IEC 19794-6:2005, Information technology — Biometric data interchange formats — Part 6. Iris image data)

ИСО/МЭК 19794-7:2007 Информационные технологии. Форматы обмена биометрическими данными. Часть 7. Данные динамики подписи (ISO/IEC 19794-7:2007, Information technology — Biometric data interchange formats — Part 7: Signature/sign time series data)

ИСО/МЭК 19794-8:2006 Информационные технологии. Форматы обмена биометрическими данными. Часть 8. Данные структуры остова отпечатка пальца (ISO/IEC 19794-8:2006, Information technology — Biometric data interchange formats — Part 8: Finger pattern skeletal data)

ИСО/МЭК 19794-9:2007 Информационные технологии. Форматы обмена биометрическими данными. Часть 9. Данные изображения сосудистого русла (ISO/IEC 19794-9:2007, Information technology — Biometric data interchange formats — Part 9: Vascular image data)

ИСО/МЭК 19794-10:2007 Информационные технологии. Форматы обмена биометрическими данными. Часть 10. Данные геометрии контура кисти руки (ISO/IEC 19794-10:2007, Information technology — Biometric data interchange formats — Part 10: Hand geometry silhouette data)

ИСО/МЭК 19795-1:2006 Информационные технологии. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура (ISO/IEC 19795-1:2006, Information technology — Biometric performance testing and reporting — Part 1: Principles and framework)

ИСО/МЭК 19795-2:2007 Информационные технологии. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 2. Методы проведения технологического и сценарного испытаний (ISO/IEC 19795-2:2007, Information technology — Biometric performance testing and reporting — Part 2: Testing methodologies for technology and scenario evaluation)

ИСО/МЭК 24713-1:2008 Информационные технологии. Биометрические профили для взаимодействия и обмена данными. Часть 1. Общая архитектура биометрической системы и биометрические профили (ISO/IEC 24713-1:2008, Information technology — Biometric profiles for interoperability and data interchange — Part 1: Overview of biometric systems and biometric profiles)

## 4 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

4.1 **приложение** (application): Программа или элемент программного обеспечения, разработанный для осуществления практических задач.

4.2 **базовый стандарт** (base standard): Стандарт, относящийся к данной серии стандартов, в котором определяются и регламентируются понятия, не определенные в настоящем стандарте.

4.3 **биометрический** (biometric): Относящийся к биометрии.

4.4 **биометрия** (biometrics): Автоматическое распознавание субъектов, основанное на поведенческих и биологических характеристиках.

4.5 **биометрическая характеристика** (biometric characteristic): Измеряемая физическая характеристика или индивидуальный поведенческий признак, при помощи которого можно идентифицировать или верифицировать предъявляемую идентификационную информацию зарегистрированного пользователя.

4.6 **биометрический признак** (biometric feature): Компактное представление данных, извлеченных из полученного или находящегося на промежуточном этапе образца при помощи математического преобразования.

4.7 **биометрический профиль** (biometric profile): Соответствующие наборы или комбинации базовых стандартов, используемые для выполнения определенных биометрических функций.

Примечание — Биометрические профили устанавливают метод использования определенных вариантов, которые доступны в базовом стандарте, и обеспечивают основу для обмена данными между приложениями и возможность взаимодействия систем.

4.8 **биометрический эталон** (biometric reference): Один или более биометрических образцов, биометрических шаблонов или биометрических моделей, связанных с субъектом и применяемых для сопоставления.

4.9 **биометрический образец** (biometric sample): Необработанные данные, представляющие собой биометрическую характеристику конечного пользователя, полученную биометрической системой (например, изображение отпечатка пальца).

4.10 **биометрическая система** (biometric system): Автоматизированная система, которая предоставляет возможность:

1) получать биометрический образец от конечного пользователя;
2) извлекать биометрические данные из биометрического образца;
3) сопоставлять биометрические данные с данными, содержащимися в одном или более эталонах;
4) определять степень схожести;
5) отображать результаты идентификации или верификации.

4.11 **биометрический шаблон** (biometric template): Данные, представляющие собой биометрические характеристики зарегистрированной личности.

Примечание — Биометрический шаблон используется биометрической системой для сопоставления с предоставленными биометрическими образцами.

4.12 **захват данных** (capture): Процесс получения биометрического образца от конечного пользователя.

4.13 **сравнение** (comparison): Процесс сличения биометрического образца с ранее полученным эталоном или шаблонами.

4.14 **предъявитель** (claimant): Человек, предоставляющий биометрический образец для верификации или идентификации, являющийся законным пользователем или «самозванцем».

4.15 **база данных** (database): Структурированный набор данных, хранящийся в компьютере.

4.16 **конечный пользователь** (end-user): Человек (сотрудник), взаимодействующий с биометрической системой с целью регистрации или идентификации его личности.

4.17 **зарегистрированная личность** (enrolee): Человек, биометрический эталон которого хранится в системе.

4.18 **регистрация** (enrolment): Процесс сбора биометрических образцов человека для получения биометрических эталонов, представляющих личность человека, с целью их сохранения в биометрической системе.

4.19 **извлечение** (extraction): Процесс преобразования захваченного биометрического образца в биометрические данные.

4.20 **ложный допуск** (false acceptance): (В биометрической системе) ошибочная идентификация субъекта или ошибочная верификация «самозванца» при предъявлении идентификационной информации.

4.21 **вероятность ложного допуска ВЛД** (false acceptance rate): Доля транзакций верификации «самозванца», которые будут ошибочно приняты.

Примечание — Вероятность ложного допуска представляет собой долю записанных пассивных транзакций «самозванца», которые были ошибочно приняты (или взвешенную долю в том случае, если количество записанных пассивных транзакций «самозванца» отличается для различных представителей испытуемой группы).

4.22 **ложный недопуск** (false rejection): Отказ в идентификации зарегистрированной личности или в верификации предъявленной идентификационной информации зарегистрированной личности.

4.23 **вероятность ложного недопуска ВЛНД** (false rejection rate): Доля транзакций верификации подлинного лица, которые будут ошибочно отвергнуты.

Примечание — Вероятность ложного недопуска представляет собой долю записанных истинных транзакций, которые были ошибочно отвергнуты (или взвешенную долю в том случае, если количество записанных истинных транзакций отличается для различных представителей испытуемой группы).

4.24 **идентификатор** (identifier): Уникальная строка данных, используемая в биометрической системе в качестве ключа для сопоставления биометрических данных личности с приписанной личности идентификационной информацией.

4.25 **идентификация/идентифицировать** (identification/identify): Функция биометрической системы, осуществляющая поиск предъявленного образца по части регистрационной базы данных или по всей базе данных и выводящая список кандидатов, состоящий из нуля, одного или нескольких идентификаторов сохраненных эталонов, которые оказались схожи с предъявленным образцом.

4.26 **сопоставлять/сопоставление** (match/matching): Процесс сопоставления биометрического образца (образцов) с ранее сохраненным шаблоном (шаблонами) и определение степени схожести.

4.27 **мультибиометрическая система** (multiple biometric): Биометрическая система, включающая в себя более одной модальности.

4.28 **популяция** (population): Совокупность конечных пользователей приложения.

4.29 **запись** (record): Шаблон и другая информация о конечном пользователе.

***Пример — Разрешение на доступ.***

4.30 **регистрация** (registration): Процесс предоставления личной идентификационной информации биометрической системе, сопоставления уникального идентификатора с данной идентификационной информацией, сбор и запись соответствующей личной информации в систему.

4.31 **токен** (token): Физическое устройство, содержащее информацию о его обладателе (конечном пользователе) или авторе (пользователе).

4.32 **транзакция** (transaction): Попытка конечного пользователя проверить идентичность биометрической информации посредством последовательного предоставления одного или более образцов в зависимости от политики принятия решений системы.

4.33 **верификация/верифицировать** (verification/verify): Функция биометрической системы, осуществляющая сопоставление предоставляемого образца с определенным сохраненным эталоном один к одному и возвращающая степень схожести или решение о схожести.

## 5 Условия

### 5.1 Специальные условия

Для ввода в действие физического контроля доступа необходимо, чтобы группы сотрудников были идентифицированы. Сотрудниками называются группы людей, принимающие то или иное участие в работе аэропорта, обладающие общими характеристиками.

Характеристики сотрудников:

- субъекты, имеющие доступ в разные зоны ограниченного доступа, предусмотренные администрацией аэропорта;
- субъекты, имеющие доступ в зоны ограниченного доступа только по профессиональным нуждам;
- субъекты трудового права.

К сотрудникам относятся, например, персонал стойки регистрации, персонал по топливозаправке, сотрудники технического обслуживания, носильщики багажа, временные дорожные рабочие.

**Работодателей и сотрудников** связывают договорные отношения. Договорные отношения заключаются на основе трудового или торгового договора. Работодатели должны обратиться с просьбой к администрации аэропорта об осуществлении физического контроля доступа сотрудников. Работодатели несут ответственность за сбор любых данных по запросу администрации аэропорта, кроме биометрических данных. Работодателем является, например, компания-оператор аэропорта, любая подрядная организация или администрация аэропорта.

Только **администрация аэропорта** имеет возможность предоставлять права доступа в зоны ограниченного доступа. Предоставление права доступа сопровождается регистрацией. Только администрация аэропорта ответственна за подтверждение достоверности данных (см. ИСО/МЭК 24713-1, 6.2.1). Регистрация и выдача свидетельства (см. ИСО/МЭК 24713-1, 6.2) производятся либо непосредственно администрацией аэропорта, либо под контролем администрации аэропорта.

**Уполномоченный орган по обеспечению конфиденциальности данных** полностью независим от администрации аэропорта, работодателей и любых сотрудников, лоббирующих сотрудничество. Уполномоченный орган по обеспечению конфиденциальности данных осуществляет надзор за защитой биометрических данных в соответствии с действующими законами и правилами. Стоит отметить, что в некоторых случаях ответственные за защиту данных являются наемными сотрудниками, наделенными уполномоченным органом по обеспечению конфиденциальности данных определенными полномочиями.

Примечание — Требования к конфиденциальности/защите данных, которые могут быть предъявлены, выходят за рамки области применения настоящего стандарта. В ряде законодательств, в зависимости от местных законов и правил, может быть задействован уполномоченный орган по обеспечению конфиденциальности данных.

### 5.2 Архитектура

Архитектура профиля сотрудника может быть разделена на четыре подсистемы. Первая подсистема: токен — физический компонент, используемый отдельным сотрудником для получения доступа в охраняемую зону на месте работы. Спецификация токена выходит за рамки области применения настоящего стандарта. Вторая подсистема: система управления токеном, применяемая для инвентаризации, распределения и аннулирования токенов. Третья подсистема: система управления и контроля, являющаяся центральной базой данных и «зонтиком безопасности» сотрудников. Четвертая подсистема: административная система командного управления, используемая для управления процессами. Инфраструктура поддержки приложения объединяет четыре указанные подсистемы.

Примечание — Возможна архитектура с другой структурой подсистем, например такая, в которой токен содержит данные биометрического эталона и/или осуществляет верификацию (см. ИСО/МЭК 7816-11).

### 5.3 Токен

Токеном называется физический компонент, который, будучи собственностью сотрудника, должен обеспечивать санкционированный физический доступ в пределах охраняемой зоны аэропорта. Кроме того, токен может поддерживать множество технологий памяти, включая память чипа инетральной схемы, магнитную полосу, оптическую полосу и штрих-код, а также осуществлять обработку данных (как это предусмотрено в микропроцессоре чипа интегральной схемы). Токен должен иметь уникальный идентификационный номер. Биометрический эталон, как правило, хранится в токене.

В зависимости от конфигурации системы командного управления токен является компонентом системы безопасности, содержащим биометрические данные. Необходимо принимать во внимание соответствующую оценку безопасности токена. Требования к безопасности токена выходят за рамки области применения настоящего стандарта.

### 5.4 Система управления токеном

Система управления токеном представляет собой систему, осуществляющую передачу, хранение, распечатку, персонализацию, загрузку, обработку и аннулирование токена. Обработка в рамках системы управления токенами может включать в себя следующие функции:

- загрузку приложения;
- управление запросами;
- осуществление большого объема печати;
- отслеживание инвентаря;
- проверку токенов;
- качество биометрических данных;
- обработку исключений;
- обработку возвращений;

- производство изображений;
- обработку зашифрованных данных;
- получение фотографии, производимое совместно с получением цифрового видео;
- совместимость цифровой камеры;
- хранение базы данных, включая хранение фотографий;
- кодирование магнитной полосы;
- печать штрих-кода;
- поддержку встроенного токена;
- кодирование инфраструктуры открытых ключей (ИОК);
- кодирование и хранение биометрических данных;
- открытый программный интерфейс для разработки приложений;
- кодирование смарт-чипа.

Примечание — Список является неполным, и некоторые элементы данного списка выходят за рамки области применения настоящего стандарта.

### 5.5 Система управления и контроля

Система управления и контроля является центральной базой данных и «зонтиком безопасности» сотрудников. Центральная база данных должна включать в свой состав по крайней мере список действительных и аннулированных идентификационных номеров токенов. Также в нее может входить несколько элементов, включая сервисы, центр коммуникации, данные о токене и иные данные, которые считаются необходимыми в рамках требований безопасности (как установлено приложением). Биометрические данные могут храниться в центральной базе данных и быть связанны с идентификационным номером токена. Система управления и контроля также должна иметь возможность осуществлять проверки предъявленной идентификационной информации и фактов, имевших место в биографии. Система управления и контроля должна иметь функцию «список отслеживания» для токенов и субъектов. Последней составляющей системы управления и контроля должна быть активно-пассивная система безопасного обмена сообщениями.

### 5.6 Административная система управления и контроля

Функцией административной системы управления и контроля является отслеживание целостности данных, контроль попыток атак на систему, включение или отключение административного контроля системы и управление политикой, то есть контроль политики подтверждения права на доступ, основанный на уровне тревоги. Данная подсистема включает в свой состав централизованную систему управления для случаев террористических или иных атак.

### 5.7 Инфраструктура

В инфраструктуру внедрены биометрические терминалы обработки токенов, проводные средства соединения, управление дверями, датчики состояния проводов, продукты и сервисы контроля доступа. Компоненты системы, параметры которых могут быть изменены при эксплуатации с помощью программного обеспечения, должны включать в себя технологию цифровой защиты для предотвращения попыток взлома системы.

## 6 Процесс

### 6.1 Общие положения

В ИСО/МЭК 24713-1 в разделе 6 подробно описывается связь между биометрической системой и приложением. В настоящем стандарте приложением является контроль доступа для сотрудников аэропортов. Процесс, описанный ниже, позволяет конкретизировать понятие архитектуры. Дополнительная информация приведена в приложении С. В данном подразделе описывается бизнес-процесс для обеспечения управления идентификационной информацией, содержащейся на токенах.

В аэропортах имеются зоны общественного пользования, служебные помещения и зоны ограниченного доступа. Доступ в зоны ограниченного доступа разрешен только сотрудникам аэропорта. Входу в зону ограниченного доступа препятствуют такие защитные механизмы, как стены, ворота, турникеты и т. п. Ворота на входе в зону должны быть оснащены механизмом контроля доступа, включающим биометрическое оборудование для сотрудников. Каждой зоне должен быть присвоен уровень привилегий. Например, в том случае, если зона ограниченного доступа А находится в пределах зоны ограниченного доступа В, то уровень привилегий зоны А должен быть выше, чем уровень привилегий

зоны В. В том случае, если зоны А и В никак не «связаны», то привилегии данных зон являются независимыми с точки зрения доступа.

### 6.2 Подтверждение достоверности

Сотрудник (первый раз или повторно) получает токен в пункте проверки и выдачи. Здесь он предоставляет заявку на получение токена от своего работодателя в порядке, установленном работодателем. Верификация предоставленной идентификационной информации производится по документам, представленным сотрудником (удостоверение личности с фотографией, свидетельство о рождении, подтверждение от работодателя и т. п.).

Данный этап является первым этапом жизненного цикла идентификатора (см. ИСО/МЭК 24713-1), который касается только сотрудников (см. 5.1). Физическая идентичность может быть проверена по документам, которые предоставляются либо сотрудником, либо работодателем. Только администрация аэропорта вправе осуществлять верификацию идентификационной информации. В этот процесс должен быть вовлечен уполномоченный орган по обеспечению конфиденциальности данных. В соответствии со стандартом ИСО/МЭК 24713-1 биометрия может быть использована для проверки фактов, имевших место в биографии.

Примечание — У сотрудника может иметься в наличии токен, который был выдан ранее. Это является следствием управления идентификационной информацией в течение жизненного цикла идентификатора.

### 6.3 Регистрация

После того как предъявленная идентификационная информация подтверждена, производится сбор биометрического эталона (эталонов) и личных данных для запуска процесса проверки фактов, имевших место в биографии. Как указано в ИСО/МЭК 24713-1, биометрия может быть использована для проверки фактов, имевших место в биографии. Иные меры по предварительной проверке, если это требуется локальным помещением, осуществляются в это же время.

Данные, необходимые системе токена, далее вводятся в регистрационную запись вместе с фотографией и биометрическим эталоном. Биометрический эталон (эталоны) отбирается из списка базовых технологий, которые необходимы для идентификации (один ко многим) и верификации (один к одному), в соответствии с приложением А. Действия при утере токена описаны в 6.5. Специалисты, осуществляющие регистрацию, должны обладать высокой квалификацией для эффективного управления биометрической системой при получении биометрических образцов сотрудников. Зона, где проводится регистрация и хранятся токены, должна быть зоной (зонами) безопасности, контроль доступа к которой (которым) вправе осуществлять только администрация аэропорта.

Биометрический образец может быть зашифрован и подписан (обозначен) приложением (см. А.7.2). Управление ключами, применяемыми для шифрования биометрического образца, должно происходить в рамках системы управления подходящими ключами, а системы управления подходящими сертификатами и персональными ключами должны применяться для эффективной биометрической аутентификации.

В дополнение к проверке фактов, имевших место в биографии, система может осуществить дублирующую проверку для сопоставления биометрических шаблонов с ранее зарегистрированными биометрическими шаблонами посредством биометрической идентификации (1:N) для снижения уровня опасности появления в системе повторяющейся идентификационной информации.

### 6.4 Выдача

Этап выдачи, описанный в ИСО/МЭК 24713-1, представляет собой предоставление привилегий и пароля. Данный этап является следующим после регистрации. В том случае, если предыдущие этапы были успешно завершены, регистрационная информация и запрос передаются в центр распечатки и персонализации, в котором токен блокируется электронным способом и передается в соответствующий центр регистрации и выдачи. Далее центральной администрации и сотруднику, которому предназначается токен, сообщается о том, что токен готов к выдаче.

После этого сотрудник, которому предназначается токен, возвращается в администрацию аэропорта, где происходит электронная разблокировка токена; биометрический эталон (эталоны) верифицируются (проверка 1:1) для гарантии того, что токен выдан именно тому сотруднику, который подавал заявку; происходит подтверждение данных, выдается токен, о чем сообщается в центральную администрацию. Срок действия токена устанавливается администрацией аэропорта.

### 6.5 Активация в локальной системе контроля доступа

Активация токена производится в каждом помещении, куда сотруднику требуется доступ. Любая передача биометрических данных должна быть защищена посредством зашифрованных и подписан-

ных шаблонов. Когда сотрудник приходит в помещение или на соответствующий пункт регистрации и выдачи, он предъявляет токен и называет причину, по которой ему требуется доступ.

При помощи биометрического эталона производится верификация идентификационной информации сотрудника и в случае необходимости подтверждается чистота биографических данных. Этот процесс представляет собой как проверку соответствия, так и проверку безопасности. Далее происходит принятие решения по привилегии на доступ и предоставляется соответствующий допуск в помещение. Привилегия на доступ, предоставленная сотруднику, определяется на основании установленного локального плана по обеспечению безопасности и данных, верифицированных токеном. Если локальная система контроля доступа совместима с токеном, то он может быть использован во всем помещении (по всему предприятию). В том случае, если системы несовместимы, сотрудник должен начать процедуру, начиная с этапа проверки, для получения совместимого токена. По предъявлении доступа сотруднику служащие помещения сообщают в центральную администрацию о выданной привилегии на доступ, и запись сотрудника обновляется.

### 6.6 Использование

Сотрудник использует выданный токен для получения доступа в одну или более зон ограниченного доступа в рамках местного аэропорта. Токен должен быть активирован для использования в местном аэропорту, а авторизованный сотрудник должен иметь доступ в зону ограниченного доступа. Последовательность событий при использовании токена зависит от реализации системы. Образец сценария использования представлен далее (этот сценарий является одним из нескольких способов реализации системы).

При входе в зону ограниченного доступа сотрудник предъявляет токен биометрическому терминалу обработки токенов для авторизации. Идентификатор сотрудника или идентификатор токена считывается с токена. Эталонные биометрические данные считываются с токена или из центральной базы данных. Система должна удостовериться в достоверности и целостности данных, считываемых с токена посредством таких техник обеспечения безопасности, как цифровая подпись, сертификаты или иные криптографические техники и/или шифрование. Сотруднику необходимо предъявить устройству захвата биометрических данных один или более биометрических образцов. Посредством этих действий сотрудник заявляет, что он является действительным авторизированным пользователем зоны ограниченного доступа в конкретный момент времени.

Биометрический эталон (эталоны) сопоставляется с биометрическими данными, предоставленными предъявителем, производится проверка полномочий для подтверждения того, что сотрудник действительно имеет доступ в зону ограниченного доступа в текущих условиях (например, время дня, рабочее расписание конкретного сотрудника, уровень опасности, история передвижений). Биометрическая верификация и проверка полномочий сотрудника могут осуществляться, частично или полностью основываясь на токене, в биометрическом терминале обработки токенов, в устройстве контроля доступа или в любом другом устройстве обработки, или в системе управления и контроля, или других объединенных в сеть центральных пунктах. Места осуществления данных операций зависят от реализации системы.

В случае, если система принимает решение о том, что биометрические данные успешно совпали и сотрудник действительно авторизован в данной зоне, то ему предоставляется доступ. Данный процесс может сопровождаться открытием дверей, ворот или иным способом предоставления входа.

Существует несколько причин, по которым токен может быть объявлен более недействительным. Данный перечень включает в себя следующие систуации, но не ограничивается ими:

- сотрудник объявляет администрации аэропорта или работодателю, что токен утерян;

- сотрудник объявляет администрации аэропорта или работодателю, что токен украден;

- сотрудник объявляет администрации аэропорта, что трудовой договор с работодателем расторгнут;

- администрация аэропорта решает аннулировать токен.

Любое из вышеперечисленных событий влечет за собой принятие решения об аннулировании токена. Данное решение принимается на основании уникального идентификационного номера токена и осуществляется автоматически по истечении срока действия токена, истечении срока действия или при расторжении существующих отношений между администрацией аэропорта и работодателем. При фактической процедуре аннулирования токена независимо от причины аннулирования необходимо принять все меры по обеспечению конфиденциальности данных обо всех, кто имеет отношение к этому процессу. Конкретные процедуры аннулирования и меры по обеспечению конфиденциальности, связанные с данными действиями, выходят за рамки области применения настоящего стандарта.

После того как произведено аннулирование токена, привилегии, связанные с наличием данного токена, блокируются. Также уникальный идентификационный номер токена должен быть заблокирован и не должен в дальнейшем снова использоваться. Отклоненные попытки доступа в зону ограниченного доступа по аннулированному токену должны отслеживаться администрацией аэропорта. Уникальный идентификационный номер токена должен применяться для ведения статистики отклоненных попыток доступа. Биометрический образец, полученный во время отклоненной попытки доступа, может быть передан и сохранен для дальнейшего расследования.

Сотрудник, который объявляет о потере или краже своего токена, делает заявку и получает новый токен в соответствии с процедурами, производимыми в этом случае администрацией аэропорта.

Администрация аэропорта имеет возможность заменить действительный токен на новый действительный токен в любое время и по любой причине. По запросу сотрудника или администрации аэропорта срок действия токена может быть продлен. В данном случае уникальный идентификационный номер токена сохраняется. После продления срока действия токена биометрический эталон может быть заменен. Управление биометрическими данными осуществляется в соответствии с описаниями стадии регистрации (см. 6.3). Процедура продления срока действия токена выходит за рамки области применения настоящего стандарта. Администрация аэропорта должна регламентировать порядок действий для случаев, когда истинный сотрудник, предоставив свой действительный токен для получения привилегий, не получает их вследствие какой-либо ошибки (например, ложный недопуск). Содержание подобных действий выходит за рамки области применения настоящего стандарта.

Управление ключами, предоставленными на считывающем устройстве, должно происходить в рамках контекста системы управления подходящими ключами, а системы управления подходящими сертификатами и персональными ключами должны применяться для эффективной биометрической аутентификации.

## 7 Меры по обеспечению безопасности

В данном разделе описываются общие понятия применяемого способа обеспечения безопасности в системе биометрической аутентификации, включая подходы и профили.

В том случае, если система контроля доступа сотрудников в аэропорту вводится в действие, датчики и сопутствующее оборудование должны быть сертифицированы в соответствии с правилами аэропорта и с учетом результатов испытаний на воздействие окружающей среды в случае эксплуатации вне помещения.

В приложении С описывается общая концепция обеспечения безопасности, которая может применяться в системе биометрической аутентификации, включая подходы и профили. Приложение С хотя и не включает в себя все данные, но может использоваться в качестве отправной точки для принятия мер по обеспечению безопасности.

Обнаружение жизненности в биометрической системе* гарантирует, что создание действительного биометрического образца может осуществляться только при помощи отпечатков пальца, изображений лица, радужной оболочки глаза и иных биометрических характеристик, полученных непосредственно от человека, подающего запрос на верификацию подобной характеристики. Дополнительная информация об обнаружении жизненности приведена в приложении С.

Характеристики системы контроля физического доступа для сотрудников аэропортов обусловлены требованиями к безопасности. Оценка эксплуатационных характеристик системы должна быть осуществлена в соответствии с ИСО/МЭК 19795-1 и ИСО/МЭК 19795-2.

Как правило, данные эксплуатационные характеристики включают в себя:

- ВЛД;
- ВЛНД;
- вероятность отказа регистрации (ВОР);
- вероятность отказа сбора данных (ВОСД).

Диапазон значений каждого параметра контролируется юридически уполномоченными органами гражданской авиации страны и местных аэропортов.

---

* *Подтверждение того, что поступающий в биометрическую систему биометрический образец принят от живого человека.*

**Приложение А**
**(обязательное)**

## Список требований

### А.1 Общие положения

В настоящем стандарте определены требования к реализации биометрической системы, которые выходят за рамки требований базовых стандартов, упомянутых в настоящем стандарте, и приводят к их изменениям. В настоящем приложении определены изменения (далее список требований — СТ), которым подвергается статус пунктов в каждой проформе ДСР, включая последующие изменения требований к ответам, которые необходимо дать.

Обозначение статуса, используемое в настоящем приложении, утверждено в ИСО/МЭК 9646-7. Ниже приведены используемые обозначения, для которых в базовом стандарте определено содержание или характеристика реализации.

M: обязательный — необходима поддержка возможности. Для значений в базовых стандартах определяется содержание требуемого элемента. Для функций в базовом стандарте определяется требуемая характеристика реализации.

N/A. неприменимый — в данном контексте невозможность использования.

O: необязательный — возможность может поддерживаться или не поддерживаться. Если поддерживается: в случае значений в базовых стандартах определяется содержание дополнительного элемента; в случае функций в базовых стандартах определяется требуемая характеристика реализации.

O.i: уточненный необязательный — для взаимоисключающих или выборочных параметров из набора, «i» — целое число, идентифицирующее уникальную группу связанных дополнительных пунктов и логику их отбора, определенное под таблицей.

X: применение данной функции контролируется приложением и может регулироваться местным соглашением.

СТ, представленный в настоящем приложении, должен применяться с целью ограничения допустимых служебных ответов в соответствующей ДСР.

### А.2 Связь между СТ и соответствующими проформами ДСР

В контексте спецификации профайла, представленной в настоящем стандарте, проформы ДСР базовых стандартов содержат таблицы трех категорий:

- таблицы проформы, в которых данный профиль не ограничивает допустимые служебные ответы;
- таблицы проформы, в которых данный профиль ограничивает допустимые служебные ответы;
- таблицы проформы, которые не относятся к данному профилю.

СТ состоит из таблиц, относящихся ко второй категории, с указанием на измененные пункты в данных таблицах.

### А.3 Декларация соответствия реализации для определенных профилей

Поставщику реализации профиля, которая должна соответствовать требованиям настоящего стандарта, необходимо оформить проформу ДСР для определенных профилей, содержащуюся в настоящем приложении, для тех пунктов, для которых запрошены реализация и соответствие. Все остальные пункты не должны учитываться.

Оформленная проформа ДСР для определенных профилей представляет собой ДСР для данной реализации. В ДСР содержатся те возможности и параметры профиля, которые были реализованы. ДСР может использоваться:

- реализатором профиля в качестве списка проверки для снижения риска ошибки соответствия стандарту по причине недосмотра;
- поставщиком и получателем (или потенциальным получателем) реализации в качестве подробного отчета о возможностях реализации, представленной в стандартной проформе ДСР;
- пользователем (или потенциальным пользователем) реализации в качестве основы для предварительной оценки возможности взаимодействия с другой реализацией (так как возможность взаимодействия не может быть гарантирована, ошибка возможности взаимодействия часто может быть предсказана при помощи несовместимой ДСР);
- испытателем в качестве основы для выбора подходящих наборов тестов, при помощи которых можно оценить требование соответствия реализации.

### А.4 Руководство по оформлению проформы ДСР

#### А.4.1 Общая структура проформы ДСР

Проформа ДСР представляет собой анкету определенного вида, разделенную на формы, каждая из которых содержит набор отдельных пунктов. Каждый пункт имеет собственный номер, наименование (вопрос, на кото-

рый требуется ответ) и ссылку (ссылки) либо на базовый стандарт, либо на определенный пункт в базовом стандарте, либо на пункт, определенный в основной части настоящего стандарта (в том случае, если в списке ссылок ни одного базового стандарта не значится).

Ответы на вопросы анкеты должны быть представлены в разделе «Поддержка» в виде ограниченного набора вариантов, из которых можно выбрать и отметить подходящие ответы.

В процессе заполнения данной формы необходимо обращаться к таблицам, представленным ниже, для того чтобы определить, является ли пункт обязательным или необязательным для поставки данного типа реализации.

**А.4.2 Дополнительная информация**

Пункты раздела «Дополнительная информация» позволяют поставщику предоставлять информацию, облегчающую интерпретацию ДСР. Не предполагается большого количества подобной информации; допускается оформление ДСР без подобной информации. Примером такой информации могут являться общие сведения о способах реализации при разных условиях и конфигурациях.

Ссылки на пункты раздела «Дополнительная информация» могут быть помещены после любого ответа в анкете и могут быть включены в позиции раздела «Исключения».

**А.4.3 Исключения**

Может произойти так, что поставщик захочет ответить на пункт со статусом «обязательный» или «запрещенный» (после того, как все условия были соблюдены) таким образом, что ответ будет противоречить указанным требованиям. Для такого случая в разделе «Поддержка» не найдется предварительно указанного ответа. Вместо этого поставщик должен указать в разделе «Поддержка» ссылку вида «х.<i>» на пункт раздела «Исключения» и предоставить соответствующее объяснение в данном пункте.

Примеры реализаций, для которых требуется раздел «Исключения», не представлены в настоящем стандарте. Необходимость в данном разделе может возникнуть при наличии сообщения о недоработках стандарта, исправление которых может повлечь изменение требования, которому должна соответствовать реализация.

**А.5 Проформа ДСР**

| | |
|---|---|
| Поставщик | |
| Контактные данные для запросов о ДСР | |
| Название и версия реализации (см. Примечание) | |
| Иная информация, необходимая для полноценной идентификации; например, название и версия устройств и/или операционных систем, название системы | |
| Потребовался ли раздел «Исключения»? | Нет [ ] Да [ ]<br>(Ответ «Да» означает, что реализация не определена в настоящем стандарте) |
| Дата утверждения | |
| Примечание — Определения «название» и «версия» должны быть интерпретированы в соответствии с терминологией поставщика (например, тип, серия, модель). | |

**А.6 Форматы обмена**

**А.6.1 Данные изображения отпечатка пальца (ИСО/МЭК 19794-4:2005)**

Таблица А.6.1

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | Статус профиля идентификации | Поддержка ДСР | Статус профиля верификации | Поддержка ДСР |
| 1 | Последовательность битов и байтов | 6.1 | M | M | [да] | M | [да] | M | [да] |
| 2 | Порядок сканирования | 6.2 | M | M | [да] | M | [да] | M | [да] |

*Окончание таблицы А.6.1*

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | Статус профиля идентификации | Поддержка ДСР | Статус профиля верификации | Поддержка ДСР |
| 3 | Требования к регистрации изображения (см. примечание 1) | 7 | O | M Уровень настройки ≥ 30 | [да, N/A] | M Уровень настройки ≥ 20 | [да, N/A] | M Уровень настройки ≥ 20 | [да, N/A] |
| 4 | Отношение размеров точки | 7.2 | M | M | [да] | M | [да] | M | [да] |
| 5 | Разрядность шкалы градаций серого | 7.3 | M | M | [да] | M | [да] | M | [да] |
| 6 | Данные градации серого | 7.4 | M | M | [да] | M | [да] | M | [да] |
| 7 | Динамический диапазон изображения | 7.5 | M | M | [да] | M | [да] | M | [да] |
| 8 | Разрешение сканирования | 7.6 | M | M | [да] | M | [да] | M | [да] |
| 9 | Разрешение изображения | 7.7 | M | M | [да] | M | [да] | M | [да] |
| 10 | Расположение отпечатка пальца | 7.8 | M | M | [да] | M | [да] | M | [да] |
| 11 | Формат записи изображения отпечатка пальца | 8 | M | M | [да] | M | [да] | M | [да] |
| 12 | Общий заголовок записи | 8.2 | M | M | [да] | M | [да] | M | [да] |
| 13 | Алгоритм сжатия изображения (см. примечание 2) | 8.2.14 | O | M Алгоритм (2)* | [да, N/A] | M Другой алгоритм | [да, N/A] | M Другой алгоритм | [да, N/A] |
| 14 | Заголовок записи изображения отпечатка пальца | 8.3 | M | M | [да] | M [да] | M [да] | M [да] | M [да] |

Примечание 1 — Требования к регистрации изображения (уровень настройки не менее 30) необходимы для получения изображения размером не менее 500 пикселей. Для идентификации и верификации могут использоваться меньшие значения уровня настройки (уровень настройки не менее 20), которые являются приемлемыми. Однако рекомендуется, чтобы для данных функций использовались большие значения уровня настройки.

Примечание 2 — Алгоритм сжатия изображения (2) используется при уровне настройки не менее 30; при уровне настройки менее 30 используются другие алгоритмы сжатия изображения.

** В п. 8.2.14 ИСО/МЭК 19794-4:2005 установлены коды алгоритмов сжатия. Код (2) соответствует алгоритму изображения WSQ.*

### А.6.2 Данные изображения отпечатка пальца — контрольные точки (ИСО/МЭК 19794-2:2005)

Таблица А.6.2

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | Статус профиля идентификации | Поддержка ДСР | Статус профиля верификации | Поддержка ДСР |
| 1* | Расположение контрольных точек | 6.3 | M | M | [да] | M | [да] | M | [да] |
| 2 | Система координат | 6.3.1 | M | M | [да] | M | [да] | M | [да] |
| 3 | Расположение контрольной точки окончания гребня | 6.3.2 | M | M | [да] | M | [да] | M | [да] |
| 4 | Расположение контрольной точки бифуркации гребня | 6.3.3 | M | M | [да] | M | [да] | M | [да] |
| 5 | Расположение контрольной точки окончания основы гребней | 6.3.4 | M | M | [да] | M | [да] | M | [да] |
| 6 | Расположение других контрольных точек | 6.3.5 | M | M | [да] | M | [да] | M | [да] |
| 7 | Используемые допущения | 6.4.1 | M | M | [да] | M | [да] | M | [да] |
| 8 | Ориентация контрольной точки окончания гребня | 6.4.2 | M | M | [да] | M | [да] | M | [да] |
| 9 | Ориентация контрольной точки бифуркации гребня | 6.4.3 | M | M | [да] | M | [да] | M | [да] |
| 10 | Ориентация контрольной точки окончания основы гребней | 6.4.4 | M | M | [да] | M | [да] | M | [да] |
| 11 | Расположение и направление ядра и дельты | 6.5 | M | M | [да] | M | [да] | M | [да] |
| 12 | Соответствие типов контрольных точек | 6.6 | M | M | [да] | M | [да] | M | [да] |
| 13 | Кодирование многобайтовых значений | 6.7 | M | M | [да] | M | [да] | M | [да] |
| 14 | Организация записи | 7.2 | M | M | [да] | M | [да] | M | [да] |
| 15 | Заголовок записи | 7.3 | M | M | [да] | M | [да] | M | [да] |
| 16 | Идентификатор формата | 7.3.1 | M | M | [да] | M | [да] | M | [да] |
| 17 | Номер версии стандарта | 7.3.2 | M | M | [да] | M | [да] | M | [да] |

* *В оригинале ИСО/МЭК 24713-2 в нумерации пунктов таблицы А.6.2. допущена ошибка.*

*Продолжение таблицы А.6.2*

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | | Статус профиля идентификации | Поддержка ДСР | | Статус профиля верификации | Поддержка ДСР |
| 18 | Длина записи | 7.3.3 | M | M | [да] | | M | [да] | | M | [да] |
| 19 | Сертификаты сканеров | 7.3.4 | M | M | [да] | | M | [да] | | M | [да] |
| 20 | Идентификационный номер типа сканеров | 7.3.5 | M | M | [да] | | M | [да] | | M | [да] |
| 21 | Размер изображения по горизонтали | 7.3.6 | M | M | [да] | | M | [да] | | M | [да] |
| 22 | Размер изображения по вертикали | 7.3.7 | M | M | [да] | | M | [да] | | M | [да] |
| 23 | Разрешение изображений по горизонтали | 7.3.8 | M | M | [да] | | M | [да] | | M | [да] |
| 24 | Разрешение изображений по вертикали | 7.3.9 | M | M | [да] | | M | [да] | | M | [да] |
| 25 | Число представлений пальцев | 7.3.10 | M | M | [да] | | M | [да] | | M | [да] |
| 26 | Зарезервированное поле | 7.3.11 | M | M | [да] | | M | [да] | | M | [да] |
| 27 | Формат записи отдельного представления пальца | 7.4 | M | M | [да] | | M | [да] | | M | [да] |
| 28 | Заголовок записи отдельного представления пальца | 7.4.1 | M | M | [да] | | M | [да] | | M | [да] |
| 29 | Данные контрольных точек отпечатка пальца | 7.4.2 | M | M | [да] | | M | [да] | | M | [да] |
| 30 | Дополнительные данные | 7.5 | O | O | [да, нет] | | O | [да, нет] | | O | [да, нет] |
| 31 | Общие поля дополнительных данных | 7.5.1 | O | O | [да, нет] | | O | [да, нет] | | O | [да, нет] |
| 32 | Формат данных гребневого счета | 7.5.2 | O | O.1 | [да, нет] | | O.1 | [да, нет] | | O.1 | [да, нет] |
| 33 | Формат данных ядра и дельты | 7.5.3 | O | O.2 | [да, нет] | | O.2 | [да, нет] | | O.2 | [да, нет] |
| 34 | Формат данных локального качества | 7.5.4 | O | O.2 | [да, нет] | | O.2 | [да, нет] | | O.2 | [да, нет] |
| 35 | Структура формата записи контрольных точек | 7.6 | M | M | [да] | | M | [да] | | M | [да] |

*Окончание таблицы А.6.2*

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | Статус профиля идентификации | Поддержка ДСР | Статус профиля верификации | Поддержка ДСР |
| 36 | Формат контрольных точек для использования в идентификационных картах | 8 | O | M | [да] | M | [да] | M | [да] |
| 37 | Владелец и тип формата ЕСФОБД | 9 | M | M | [да] | M | [да] | M | [да] |
| Примечание 1 — Параметры, обозначенные «O.1», связаны с дополнительной информацией о количестве гребней и должны появляться или использоваться совместно.<br>Примечание 2 — Параметры, обозначенные «O.2», связаны с дополнительной информацией о количестве других контрольных точек и должны появляться или использоваться совместно. | | | | | | | | | |

Дополнительные требования к применению данного формата указаны ниже и относятся к тем реализациям, которые должны быть определены в настоящем стандарте.

1. Расширенные данные не должны применяться для установки собственного формата контрольных точек в обход обязательных функций настоящего стандарта.

2. Контрольные точки, представляющие собой окончания папиллярных гребней, должны быть зашифрованы как «окончание гребней», а контрольные точки, представляющие собой места разделения папиллярных гребней на два гребня, как «бифуркация». Тип контрольных точек «иной» применяется для контрольных точек типа «окончание гребней» или «бифуркация», где затруднено однозначное определение типа.

3. При использовании гребневого счета он должен быть рассчитан следующим образом. если используется гребневой счет по 4 секторам, то секторы должны быть ограничены углами в 45, 135, 225 и 315 градусов, если используется гребневой счет по 8 секторам, то каждый сектор должен иметь угол 45 градусов, формируя тем самым гипотетическую окружность с центром в месте контрольной точки.

**А.6.3 Спектральные данные изображения отпечатка пальца (ИСО/МЭК 19794-3:2006)**

Таблица А.6.3

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | Статус профиля идентификации | Поддержка ДСР | Статус профиля верификации | Поддержка ДСР |
| 1 | Идентификатор формата | 8.1.1 | M | M | [да] | M | [да] | M | [да] |
| 2 | Номер версии стандарта | 8.1.2 | M | M | [да] | M | [да] | M | [да] |
| 3 | Длина записи | 8.1.3 | M | M | [да] | M | [да] | M | [да] |
| 4* | Число представлений пальцев | 8.1.4 | M | M | [да] | M | [да] | M | [да] |
| 5 | Разрешение изображения по горизонтали | 8.1.5 | M | M | [да] | M | [да] | M | [да] |

* *В оригинале ИСО/МЭК 24713-2 в таблице А.6.3 пропущен пункт 4.*

*Продолжение таблицы А.6.3*

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | | Статус профиля идентификации | Поддержка ДСР | | Статус профиля верификации | Поддержка ДСР |
| 6 | Разрешение изображения по вертикали | 8.1.6 | М | М | [да] | | М | [да] | | М | [да] |
| 7 | Число ячеек по горизонтали | 8.1.7 | М | М | [да] | | М | [да] | | М | [да] |
| 8 | Число ячеек по вертикали | 8.1.8 | М | М | [да] | | М | [да] | | М | [да] |
| 9 | Число пикселей в ячейках по горизонтали | 8.1.9 | М | М | [да] | | М | [да] | | М | [да] |
| 10 | Число пикселей в ячейках по вертикали | 8.1.10 | М | М | [да] | | М | [да] | | М | [да] |
| 11 | Число пикселей между центрами ячеек по горизонтали | 8.1.11 | М | М | [да] | | М | [да] | | М | [да] |
| 12 | Число пикселей между центрами ячеек по вертикали | 8.1.12 | М | М | [да] | | М | [да] | | М | [да] |
| 13 | Метод выбора спектральных составляющих | 8.1.13 | М | М | [да] | | М | [да] | | М | [да] |
| 14 | Тип окна | 8.1.14 | М | М | [да] | | М | [да] | | М | [да] |
| 15 | Стандартное отклонение | 8.1.15 | М | М | [да] | | М | [да] | | М | [да] |
| 16 | Число частот | 8.1.16 | М | М | [да] | | М | [да] | | М | [да] |
| 17 | Частоты | 8.1.17 | М | М | [да] | | М | [да] | | М | [да] |
| 18 | Число направлений | 8.1.18 | М | М | [да] | | М | [да] | | М | [да] |
| 19 | Число сохраняемых спектральных составляющих для каждой ячейки | 8.1.19 | М | М | [да] | | М | [да] | | М | [да] |
| 20 | Число битов, кодирующих угол распространения | 8.1.20 | М | М | [да] | | М | [да] | | М | [да] |
| 21 | Число битов, кодирующих длину волны | 8.1.21 | М | М | [да] | | М | [да] | | М | [да] |
| 22 | Число битов, кодирующих фазовый сдвиг | 8.1.22 | М | М | [да] | | М | [да] | | М | [да] |
| 23 | Число битов, кодирующих модуль | 8.1.23 | М | М | [да] | | М | [да] | | М | [да] |
| 24 | Число битов, кодирующих показатель качества | 8.1.24 | М | М | [да] | | М | [да] | | М | [да] |

*Окончание таблицы А.6.3*

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | Статус профиля идентификации | Поддержка ДСР | Статус профиля верификации | Поддержка ДСР |
| 25 | Параметр зернистости группы ячеек | 8.1.25 | M | M | [да] | M | [да] | M | [да] |
| 26 | Зарезервированные байты | 8.1.26 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 27 | Запись данных одного пальца | 8.2 | M | M | [да] | M | [да] | M | [да] |
| 28 | Заголовок | 8.2.1 | M | M | [да] | M | [да] | M | [да] |
| 29 | Блок спектральных данных изображения отпечатка пальца | 8.2.2 | M | M | [да] | M | [да] | M | [да] |
| 30 | Блок дополнительных данных | 8.2.3 | M | M | [да] | M | [да] | M | [да] |
| 31 | Формат карты спектральных данных изображения отпечатка пальца | 9 | M | M | [да] | M | [да] | M | [да] |

### А.6.4 Данные изображения лица (ИСО/МЭК 19794-5:2005)

Таблица А.6.4

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | Статус профиля идентификации | Поддержка ДСР | Статус профиля верификации | Поддержка ДСР |
| 1 | Последовательность байтов | 5.2.1 | M | M | [да] | M | [да] | M | [да] |
| 2 | Блок заголовка ЕСФОБД | 5.3 | M | M | [да] | M | [да] | M | [да] |
| 3 | Идентификатор формата | 5.4.1 | M | M | [да] | M | [да] | M | [да] |
| 4 | Номер версии стандарта | 5.4.2 | M | M | [да] | M | [да] | M | [да] |
| 5 | Длина записи | 5.4.3 | M | M | [да] | M | [да] | M | [да] |
| 6 | Число изображений лица | 5.4.4 | M | M | [да] | M | [да] | M | [да] |
| 7 | Длина данных записи изображения лица | 5.5.1 | M | M | [да] | M | [да] | M | [да] |
| 8 | Число контрольных точек | 5.5.2 | M | M | [да] | M | [да] | M | [да] |
| 9 | Пол | 5.5.3 | M | M | [да] | M | [да] | M | [да] |

*Продолжение таблицы А.6.4*

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | | Статус профиля идентификации | Поддержка ДСР | | Статус профиля верификации | Поддержка ДСР |
| 10 | Цвет глаз | 5.5.4 | M | M | [да] | | M | [да] | | M | [да] |
| 11 | Цвет волос | 5.5.5 | M | M | [да] | | M | [да] | | M | [да] |
| 12 | Маска свойств | 5.5.6 | M | M | [да] | | M | [да] | | M | [да] |
| 13 | Выражение лица | 5.5.7 | M | M | [да] | | M | [да] | | M | [да] |
| 14 | Угловая координата — поворот | 5.5.8.1 | M | M | [да] | | M | [да] | | M | [да] |
| 15 | Угловая координата — наклон | 5.5.8.2 | M | M | [да] | | M | [да] | | M | [да] |
| 16 | Угловая координата — отклонение | 5.5.8.3 | M | M | [да] | | M | [да] | | M | [да] |
| 17 | Погрешность угловых координат | 5.5.9 | M | M | [да] | | M | [да] | | M | [да] |
| 18 | Тип контрольной точки | 5.6.1 | M | M | [да] | | M | [да] | | M | [да] |
| 19 | Код контрольной точки | 5.6.2 | M | M | [да] | | M | [да] | | M | [да] |
| 20 | Контрольные точки MPEG4 | 5.6.3 | M | M | [да] | | M | [да] | | M | [да] |
| 21 | Контрольные точки центров глаз и ноздрей | 5.6.4 | M | M | [да] | | M | [да] | | M | [да] |
| 22 | Тип изображения лица | 5.7.1 | M | M | [да] | | M | [да] | | M | [да] |
| 23 | Тип данных изображения | 5.7.2 | M | M | [да] | | M | [да] | | M | [да] |
| 24 | Горизонтальный размер изображения | 5.7.3 | M | M | [да] | | M | [да] | | M | [да] |
| 25 | Вертикальный размер изображения | 5.7.4 | M | M | [да] | | M | [да] | | M | [да] |
| 26 | Цветовое пространство изображения | 5.7.5 | M | M | [да] | | M | [да] | | M | [да] |
| 27 | Тип источника | 5.7.6 | M | M | [да] | | M | [да] | | M | [да] |
| 28 | Тип устройства | 5.7.7 | M | M | [да] | | M | [да] | | M | [да] |
| 29 | Качество | 5.7.8 | M | M | [да] | | M | [да] | | M | [да] |
| 30 | Структура данных | 5.8.1 | M | M | [да] | | M | [да] | | M | [да] |
| 31 | Требования наследования для основного типа изображения лица | 6.1 | M | M | [да] | | M | [да] | | M | [да] |

*Продолжение таблицы А.6.4*

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | Статус профиля идентификации | Поддержка ДСР | Статус профиля верификации | Поддержка ДСР |
| 32 | Требования к кодированию данных изображения для основного типа изображения лица | 6.2 | M | M | [да] | M | [да] | M | [да] |
| 33 | Требования к сжатию данных изображения для основного типа изображения лица | 6.3 | M | M | [да] | M | [да] | M | [да] |
| 34 | Требования к формату записи данных для основного типа изображения лица | 6.4 | M | M | [да] | M | [да] | M | [да] |
| 35 | Требования к блоку заголовка записи изображения лица | 6.4.1 | M | M | [да] | M | [да] | M | [да] |
| 36 | Требования к блоку информации о лице | 6.4.2 | M | M | [да] | M | [да] | M | [да] |
| 37 | Требования к блоку информации об изображении | 6.4.3 | M | M | [да] | M | [да] | M | [да] |
| 38 | Требования к положению лица | 7.2.2 | M.1, M.2 | M.1, M.2 | [да] | N/A | [n/a] | N/A | [n/a] |
| 39 | Требования к выражению лица | 7.2.3 | O.1, O.2 | M.1, M.2 | [да] | N/A | [n/a] | N/A | [n/a] |
| 40 | Требования к помощи в позиционировании лица | 7.2.4 | M.1, M.2 | M | [да] | N/A | [n/a] | N/A | [n/a] |
| 41 | Требования к положению плеч | 7.2.5 | M.1, M.2 | M.1, M.2 | [да] | N/A | [n/a] | N/A | [n/a] |
| 42 | Требования к фону | 7.2.6 | O.1, O.2 | M.1, M.2 | [да] | M.1, M.2 | [да] | M.1, M.2 | [да] |
| 43 | Требования к освещению | 7.2.7 | M.1, M.2 | M.1, M.2 | [да] | M.1, M.2 | [да] | M.1, M.2 | [да] |
| 44 | Требования к теням на лице | 7.2.8 | M.1, M.2 | M.1, M.2 | [да] | M.1, M.2 | [да] | M.1, M.2 | [да] |
| 45 | Требования к теням в глазных впадинах | 7.2.9 | M.1, M.2 | M.1, M.2 | [да] | M.1, M.2 | [да] | M.1, M.2 | [да] |
| 46 | Требования к бликам изображения | 7.2.10 | O.1, O.2 | M.1, M.2 | [да] | M.1, M.2 | [да] | M.1, M.2 | [да] |
| 47 | Требования к фотографированию в очках | 7.2.11 | O.1, O.2 | M.1, M.2 | [да] | N/A | [n/a] | N/A | [n/a] |
| 48 | Требования к повязке на глазах | 7.2.12 | O.1, O.2 | M.1, M.2 | [да] | N/A | [n/a] | N/A | [n/a] |

*Продолжение таблицы А.6.4*

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | | Статус профиля идентификации | Поддержка ДСР | | Статус профиля верификации | Поддержка ДСР |
| 49 | Требования к экспозиции | 7.3.2 | M.1, M.2 | M.1, M.2 | [да] | | M.1, M.2 | [да] | | M.1, M.2 | [да] |
| 50 | Требования к фокусировке и глубине резкости | 7.3.3 | M.1, M.2 | M.1, M.2 | [да] | | M.1, M.2 | [да] | | M.1, M.2 | [да] |
| 51 | Требования к воспроизведению исходных цветов объекта на изображении | 7.3.4 | M.1, M.2 | M.1, M.2 | [да] | | M.1,M.2 | [да] | | M.1, M.2 | [да] |
| 52 | Требования к редактированию цветного или черно-белого изображения | 7.3.5 | M.1, M.2 | M.1, M.2 | [да] | | M.1, M.2 | [да] | | M.1, M.2 | [да] |
| 53 | Требования к бочкообразной дисторсии | 7.3.6 | M.1, M.2 | M.1, M.2 | [да] | | M.1, M.2 | [да] | | M.1, M.2 | [да] |
| 54 | Отношение размеров пикселя | 7.4.1.1 | M.1, M.2 | M.1, M.2 | [да] | | M.1, M.2 | [да] | | M.1, M.2 | [да] |
| 55 | Начало отсчета | 7.4.1.2 | M.1, M.2 | M.1, M.2 | [да] | | M.1, M.2 | [да] | | M.1, M.2 | [да] |
| 56 | Разрядность шкалы градаций серого | 7.4.2.1 | O.1, O.2 | M.1, M.2 | [да] | | M.1, M.2 | [да] | | M.1, M.2 | [да] |
| 57 | Цветовая насыщенность | 7.4.2.2 | O.1, O.2 | M.1, M.2 | [да] | | M.1, M.2 | [да] | | M.1, M.2 | [да] |
| 58 | Цветовое пространство | 7.4.2.3 | M.1, M.2 | M.1, M.2 | [да] | | M.1, M.2 | [да] | | M.1, M.2 | [да] |
| 59 | Требования к чересстрочной развертке | 7.4.3 | M.1, M.2 | M.1, M.2 | [да] | | M.1, M.2 | [да] | | M.1, M.2 | [да] |
| 60 | Требования к положению лица по горизонтали | 8.3.2 | M.1 | M.1 | [да] | | N/A | [n/a] | | N/A | [n/a] |
| 61 | Требования к положению лица по вертикали | 8.3.3 | M.1 | M.1 | [да] | | N/A | [n/a] | | N/A | [n/a] |
| 62 | Требования к горизонтальному размеру головы на изображении | 8.3.4 | M.1 | M.1 | [да] | | N/A | [n/a] | | N/A | [n/a] |
| 63 | Требования к вертикальному размеру головы на изображении | 8.3.5 | M.1 | M.1 | [да] | | N/A | [n/a] | | N/A | [n/a] |
| 64 | Требования к разрешению изображения | 8.4.1 | M.1 | M.1 | [да] | | N/A | [n/a] | | N/A | [n/a] |

*Окончание таблицы А.6.4*

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | Статус профиля идентификации | Поддержка ДСР | Статус профиля верификации | Поддержка ДСР |
| 65 | Требования к положению глаз | 9.2.2 | O | N/A | [N/A] | N/A | [n/a] | O.2 | [да, нет] |
| 66 | Требования к геометрическим параметрам изображения лица условного фронтального типа | 9.2.3 | O | N/A | [N/A] | N/A | [n/a] | O.2 | [да, нет] |
| 67 | Требования к минимальному горизонтальному размеру изображения лица условного фронтального типа | 9.2.4 | O | N/A | [N/A] | N/A | [n/a] | O.2 | [да, нет] |
| 68 | Требования к заполнению | 9.2.5 | O | N/A | [N/A] | N/A | [n/a] | O.2 | [да, нет] |
| 69 | Требования наследования | 9.3.1 | M | M | [да] | M | [да] | M | [да] |
| 70 | Блок информации об изображении | 9.3.2 | M | M | [да] | M | [да] | M | [да] |

Примечание 1 — Параметры, обозначенные «O.1», связаны с фронтальным типом изображения и должны появляться или использоваться совместно.

Примечание 2 — Параметры, обозначенные «O.2», связаны с типом изображения токена и должны появляться или использоваться совместно.

### А.6.5 Данные изображения радужной оболочки глаза (ИСО/МЭК 19794-6:2005)

Таблица А.6.5

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | Статус профиля идентификации | Поддержка ДСР | Статус профиля верификации | Поддержка ДСР |
| 1 | Общие положения | 6.1 | M | M | [да] | M | [да] | M | [да] |
| 2 | Сжатие изображения | 6.2 | M | M | [да] | M | [да] | M | [да] |
| 3 | Предварительная обработка изображения | 6.3 | M | M | [да] | M | [да] | M | [да] |
| 4 | Блок биометрических данных изображения РОГ | 6.4 | M | M | [да] | M | [да] | M | [да] |

*Окончание таблицы А.6.5*

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | Статус профиля идентификации | Поддержка ДСР | Статус профиля верификации | Поддержка ДСР |
| 5 | Структуры заголовков блока биометрических данных изображения РОГ | 6.5 | M | M | [да] | M | [да] | M | [да] |
| 6 | Качество изображения | А.1 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 7 | Уровни градаций серого | А.2 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 8 | Освещение | А.3 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 9 | Контраст | А.4 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 10 | Видимая часть РОГ | А.5 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 11 | Соотношение длин сторон точки | А.6 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 12 | Масштаб изображения | А.7 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 13 | Оптические искажения | А.8 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 14 | Шум | А.9 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 15 | Ориентация изображения | А.10 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 16 | Представление РОГ | А.11 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |

### А.6.6 Данные динамики подписи (ИСО/МЭК 19794-7:2007)

Таблица А.6.6

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | Статус профиля идентификации | Поддержка ДСР | Статус профиля верификации | Поддержка ДСР |
| 1 | Каналы позиции пера X, Y, Z | 6.2 | M | M | [да] | M | [да] | M | [да] |
| 2 | Каналы скорости пера VX, VY | 6.3 | O | O | [да] | O | [да] | O | [да] |
| 3 | Каналы ускорения пера AX, AY | 6.4 | O | O | [да] | O | [да] | O | [да] |
| 4 | Канал времени T | 6.5 | O | O | [да] | O | [да] | O | [да] |
| 5 | Канал дифференциала времени DT | 6.6 | O | O | [да] | O | [да] | O | [да] |

*Окончание таблицы А.6.6*

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | Статус профиля идентификации | Поддержка ДСР | Статус профиля верификации | Поддержка ДСР |
| 6 | Канал силы нажатия пера F | 6.7 | O | O | [да] | O | [да] | O | [да] |
| 7 | Канал состояния пера S | 6.8 | O | O | [да] | O | [да] | O | [да] |
| 8 | Каналы ориентации пера TX, TY, Az, El, R | 6.9 | O | O | [да] | O | [да] | O | [да] |
| 9 | Идентификатор формата записи | 7.3.2 | M | M/na.1 | [да] | M/na.1 | [да] | M/na.1 | [да] |
| 10 | Номер версии стандарта | 7.3.3 | M | M/na.1 | [да] | M/na.1 | [да] | M/na.1 | [да] |
| 11 | Описание каналов | 7.3.4 | M | M/na.1 | [да] | M/na.1 | [да] | M/na.1 | [да] |
| 12 | Резервный байт | 7.3.5 | M | M/na.1 | [да] | M/na.1 | [да] | M/na.1 | [да] |
| 13 | Формат записи данных динамики подписи | 7.4 | M | M/na.1 | [да] | M/na.1 | [да] | M/na.1 | [да] |
| 14 | Данные значений каналов | 7.4.2 | M | M/na.1 | [да] | M/na.1 | [да] | M/na.1 | [да] |
| 15 | Дополнительные данные | 7.4.3 | M | M/na.1 | [да] | M/na.1 | [да] | M/na.1 | [да] |
| 16 | Резервный байт | 7.3.5* | M | M/na.1 | [да] | M/na.1 | [да] | M/na.1 | [да] |
| 17 | Компактный формат | 8 | O | O/M.1 | [да] | O/M.1 | [да] | O/M.1 | [да] |
| 18 | Структура данных параметров алгоритма сравнения | 8.2 | O | O/M.1 | [да, нет] | O/M.1 | [да, нет] | O/M.1 | [да, нет] |
| 19 | Внедрение в структуру данных ЕСФОБД | 8.3 | O | O/M.1 | [да, нет] | O/M.1 | [да, нет] | O/M.1 | [да, нет] |
| 20 | Запись блока данных динамики подписи | 8.4 | O | O/M.1 | [да, нет] | O/M.1 | [да, нет] | O/M.1 | [да, нет] |
| 21 | Данные значений каналов | 8.4.2** | O | O/M.1 | [да, нет] | O/M.1 | [да, нет] | O/M.1 | [да, нет] |
| 22 | Дополнительные данные | 8.4.3*** | O | O | [да] | O | [да] | O | [да] |

Примечание 1 — Записи, отмеченные «M/na.1», являются обязательными, если биометрический эталон не хранится на токене, и необязательными, если биометрический эталон хранится на токене.

Примечание 2 — Записи, отмеченные «O/M.1», являются необязательными, если биометрический эталон не хранится на токене, и обязательными, если биометрический эталон хранится на токене.

---

* *В оригинале ИСО/МЭК 24713-2:2008 допущена опечатка — указан пункт 6.4.7 вместо пункта 7.3.5.*

** *В ИСО/МЭК 19794-7:2005 отсутствует пункт 8.4.2.*

*** *В ИСО/МЭК 19794-7:2005 отсутствует пункт 8.4.3.*

### А.6.7 Данные структуры остова отпечатка пальца (ИСО/МЭК 19794-8:2006)

Таблица А.6.7

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | | Статус профиля идентификации | Поддержка ДСР | | Статус профиля верификации | Поддержка ДСР |
| 1 | Тип контрольной точки | 6.1.1 | M | M | [да] | | M | [да] | | M | [да] |
| 2 | Расположение контрольной точки | 6.1.2 | M | M | [да] | | M | [да] | | M | [да] |
| 3 | Система координат | 6.1.2 | M | M | [да] | | M | [да] | | M | [да] |
| 4 | Допущения, используемые при определении углов | 6.1.3 | M | M | [да] | | M | [да] | | M | [да] |
| 5 | Код направления | 6.2.1 | M | M | [да] | | M | [да] | | M | [да] |
| 6 | Общие правила кодирования остова линии | 6.2.2 | M | M | [да] | | M | [да] | | M | [да] |
| 7 | Конструктивные элементы направления | 6.2.3 | M | M | [да] | | M | [да] | | M | [да] |
| 8 | Организация записи | 7.2 | M | M | [да] | | M | [да] | | M | [да] |
| 9 | Заголовок записи | 7.3 | M | M | [да] | | M | [да] | | M | [да] |
| 10 | Формат идентификатора | 7.3.1 | M | M | [да] | | M | [да] | | M | [да] |
| 11 | Номер версии стандарта | 7.3.2 | M | M | [да] | | M | [да] | | M | [да] |
| 12 | Длина записи | 7.3.3 | M | M | [да] | | M | [да] | | M | [да] |
| 13 | Идентификационный номер типа устройства захвата данных | 7.3.5* | M | M | [да] | | M | [да] | | M | [да] |
| 14 | Число представлений пальца в записи | 7.3.6 | M | M | [да] | | M | [да] | | M | [да] |
| 15 | Разрешение изображения в масштабе | 7.3.7 | M | M | [да] | | M | [да] | | M | [да] |
| 16 | Число битов на запись координат точек начала и конца кода направления | 7.3.8 | M | M | [да] | | M | [да] | | M | [да] |
| 17 | Число битов на запись направления точек начала и окончания кода направления | 7.3.9 | M | M | [да] | | M | [да] | | M | [да] |

** В оригинале ИСО/МЭК 24713-2 в пунктах таблицы 13—21 допущена опечатка в ссылках на базовый стандарт: вместо ссылок на пункты 7.3.5—7.3.13 указаны ссылки на пункты 7.3.4—7.3.12.*

*Продолжение таблицы А.6.7*

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | Статус профиля идентификации | Поддержка ДСР | Статус профиля верификации | Поддержка ДСР |
| 18 | Число битов на запись направления в коде направления | 7.3.10 | M | M | [да] | M | [да] | M | [да] |
| 19 | Размер шага кода направления | 7.3.11 | M | M | [да] | M | [да] | M | [да] |
| 20 | Относительный поперечный размер шага кода направления | 7.3.12 | M | M | [да] | M | [да] | M | [да] |
| 21 | Число направлений в пределах угла 180° | 7.3.13 | M | M | [да] | M | [да] | M | [да] |
| 22 | Заголовок записи отдельного представления отпечатка пальца | 7.4.1 | M | M | [да] | M | [да] | M | [да] |
| 23 | Номер представления | 7.4.1.1* | M | M | [да] | M | [да] | M | [да] |
| 24 | Локализация пальца | 7.4.1.2 | M | M | [да] | M | [да] | M | [да] |
| 25 | Тип отпечатка | 7.4.1.3 | M | M | [да] | M | [да] | M | [да] |
| 26 | Качество пальца | 7.4.1.4 | M | M | [да] | M | [да] | M | [да] |
| 27 | Размер изображения по оси *X* | 7.4.1.5 | M | M | [да] | M | [да] | M | [да] |
| 28 | Размер изображения по оси *Y* | 7.4.1.6 | M | M | [да] | M | [да] | M | [да] |
| 29 | Размер данных остова | 7.4.1.7 | M | M | [да] | M | [да] | M | [да] |
| 30 | Данные остова отпечатка пальца | 7.4.2.2** | M | M | [да] | M | [да] | M | [да] |
| 31 | Дополнительные данные | 7.5 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 32 | Общие поля дополнительных данных | 7.5.1 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 33 | Длина блока дополнительных данных | 7.5.1.1 | M | M | [да] | M | [да] | M | [да] |
| 34 | Код типа сегмента дополнительных данных | 7.5.1.2 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 35 | Длина сегмента дополнительных данных | 7.5.1.3 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |

** В оригинале ИСО/МЭК 24713-2 в пунктах таблицы 23—29 допущена опечатка в ссылках на базовый стандарт: вместо ссылок на пункты 7.4.1.1—7.4.1.7 указаны ссылки на пункты 7.4.2—7.4.8.*

*** В оригинале ИСО/МЭК 24713-2 допущена опечатка — вместо пункта 7.4.2.2 указан пункт 7.4.9.*

*Продолжение таблицы А.6.7*

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | | Статус профиля идентификации | Поддержка ДСР | | Статус профиля верификации | Поддержка ДСР |
| 36 | Область дополнительных данных сегмента | 7.5.1.4 | O | O | [да, нет] | | O | [да, нет] | | O | [да, нет] |
| 37 | Формат данных гребневого счета | 7.5.2 | O | O.1 | [да, нет] | | O.1 | [да, нет] | | O.1 | [да, нет] |
| 38 | Метод определения гребневого счета | 7.5.2.1 | O | O.1 | [да, нет] | | O.1 | [да, нет] | | O.1 | [да, нет] |
| 39 | Данные гребневого счета | 7.5.2.2 | O | O.1 | [да, нет] | | O.1 | [да, нет] | | O.1 | [да, нет] |
| 40 | Формат данных ядра и дельты | 7.5.3 | O | O.2 | [да, нет] | | O.2 | [да, нет] | | O.2 | [да, нет] |
| 41 | Число ядер | 7.5.3.1 | O | O.2 | [да, нет] | | O.2 | [да, нет] | | O.2 | [да, нет] |
| 42 | Тип данных ядра | 7.5.3.2 | O | O.2 | [да, нет] | | O.2 | [да, нет] | | O.2 | [да, нет] |
| 43 | Расположение ядра | 7.5.3.3 | O | O.2 | [да, нет] | | O.2 | [да, нет] | | O.2 | [да, нет] |
| 44 | Ориентация ядра | 7.5.3.4 | O | O.2 | [да, нет] | | O.2 | [да, нет] | | O.2 | [да, нет] |
| 45 | Число дельт | 7.5.3.5 | O | O.2 | [да, нет] | | O.2 | [да, нет] | | O.2 | [да, нет] |
| 46 | Тип данных дельты | 7.5.3.6 | O | O.2 | [да, нет] | | O.2 | [да, нет] | | O.2 | [да, нет] |
| 47 | Расположение дельты | 7.5.3.7 | O | O.2 | [да, нет] | | O.2 | [да, нет] | | O.2 | [да, нет] |
| 48 | Ориентация дельты | 7.5.3.8 | O | O.2 | [да, нет] | | O.2 | [да, нет] | | O.2 | [да, нет] |
| 49 | Формат данных локального качества | 7.5.4 | O | O.3 | [да, нет] | | O.3 | [да, нет] | | O.3 | [да, нет] |
| 50 | Ширина и высота ячейки | 7.5.4.1 | O | O.3 | [да, нет] | | O.3 | [да, нет] | | O.3 | [да, нет] |
| 51 | Число битов, кодирующих оценку локального качества изображения | 7.5.4.2 | O | O.3 | [да, нет] | | O.3 | [да, нет] | | O.3 | [да, нет] |
| 52 | Данные локального качества | 7.5.4.3 | O | O.3 | [да, нет] | | O.3 | [да, нет] | | O.3 | [да, нет] |
| 53 | Данные расположения потовых пор | 7.5.5 | O | O.4 | [да, нет] | | O.4 | [да, нет] | | O.4 | [да, нет] |
| 54 | Разрешение расположения потовых пор | 7.5.5.1 | O | O.4 | [да, нет] | | O.4 | [да, нет] | | O.4 | [да, нет] |
| 55 | Число битов информации о расстоянии между потовыми порами | 7.5.5.2 | O | O.4 | [да, нет] | | O.4 | [да, нет] | | O.4 | [да, нет] |

*Окончание таблицы А.6.7*

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | Статус профиля идентификации | Поддержка ДСР | Статус профиля верификации | Поддержка ДСР |
| 56 | Описание расположения потовой поры | 7.5.5.3 | O | O.4 | [да, нет] | O.4 | [да, нет] | O.4 | [да, нет] |
| 57 | Структурные данные остова отпечатка пальца | 7.5.6 | O | O.5 | [да, нет] | O.5 | [да, нет] | O.5 | [да, нет] |
| 58 | Формат нормального размера структуры остова отпечатка пальца | 8.1 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 59 | Формат компактного размера структуры остова отпечатка пальца | 8.2 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 60 | Размер изображения остова в *x* и *y* координатах | 8.3.1 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 61 | Упорядочение с расширением *x* и *y* координат в формате компактного размера | 8.4 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 62 | Использование дополнительных свойств формата идентификационной карты | 8.5 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 63 | Сравнение параметров и возможностей идентификационной карты | 8.6 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 64 | Владелец формата ЕСФОБД и тип формата | 9 | M | M | [да] | M | [да] | M | [да] |

Примечание 1 — Параметры, обозначенные «O.1», связаны с дополнительной информацией о гребневом счете и должны появляться или использоваться совместно.

Примечание 2 — Параметры, обозначенные «O.2», связаны с дополнительной информацией о ядре и дельте и должны появляться или использоваться совместно.

Примечание 3 — Параметры, обозначенные «O.3», связаны с дополнительной информацией о расположении пор и должны появляться или использоваться совместно.

Примечание 4 — Параметры, обозначенные «O.4», связаны с дополнительной информацией о качестве клетки и должны появляться или использоваться совместно.

Примечание 5 — Параметры, обозначенные «O.5», связаны с дополнительной структурной информацией об остове и должны появляться или использоваться совместно.

### А.6.8 Данные изображения сосудистого русла (ИСО/МЭК 19794-9:2007)

Таблица А.6.8

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | | Статус профиля идентификации | Поддержка ДСР | | Статус профиля верификации | Поддержка ДСР |
| 1 | Порядок следования байтов и разрядов | 6.1 | M | M | [да] | | M | [да] | | M | [да] |
| 2 | Последовательность сканирования | 6.2 | M | M | [да] | | M | [да] | | M | [да] |
| 3 | Пространственное разрешение | 7.1 | M | M | [да] | | M | [да] | | M | [да] |
| 4 | Число уровней градаций серого | 7.2 | M | M | [да] | | M | [да] | | M | [да] |
| 5 | Освещение | 7.3 | M | M | [да] | | M | [да] | | M | [да] |
| 6 | Отношение размеров пикселей | 7.4 | M | M | [да] | | M | [да] | | M | [да] |
| 7 | Нормализация проекции | 7.5 | M | M | [да] | | M | [да] | | M | [да] |
| 8 | Формат хранения изображения | 7.6 | M | M | [да] | | M | [да] | | M | [да] |
| 9 | Область формирования изображения | 7.7 | M | M | [да] | | M | [да] | | M | [да] |
| 10 | Стандартное положение | 7.8 | M | M | [да] | | M | [да] | | M | [да] |
| 11 | Система координат объекта | 7.9 | M | M | [да] | | M | [да] | | M | [да] |
| 12 | Структура блока данных изображения сосудистого русла | 8.1 | M | M | [да] | | M | [да] | | M | [да] |
| 13 | Структура заголовка записи изображения сосудистого русла | 8.2 | M | M | [да] | | M | [да] | | M | [да] |
| 14 | Структура заголовка изображения сосудистого русла | 8.3 | M | M | [да] | | M | [да] | | M | [да] |
| 15 | Поле типа изображения сосудистого русла | 8.3.1 | M | M | [да] | | M | [да] | | M | [да] |
| 16 | Поле длины записи изображения сосудистого русла | 8.3.2 | M | M | [да] | | M | [да] | | M | [да] |
| 17 | Поля горизонтального и вертикального размеров изображения | 8.3.3 | M | M | [да] | | M | [да] | | M | [да] |
| 18 | Поле числа уровней градаций серого | 8.3.4 | M | M | [да] | | M | [да] | | M | [да] |
| 19 | Поле положения изображения и поле свойств бита | 8.3.5 | M | M | [да] | | M | [да] | | M | [да] |

*Окончание таблицы А.6.8*

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | Статус профиля идентификации | Поддержка ДСР | Статус профиля верификации | Поддержка ДСР |
| 20 | Поле угла поворота изображения | 8.3.6 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 21 | Поле формата изображения | 8.3.7 | M | M | [да] | M | [да] | M | [да] |
| 22 | Поле типа освещения | 8.3.8 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 23 | Поле фона изображения | 8.3.9 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 24 | Поле разрешающей способности сканирования по горизонтали | 8.3.10 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 25 | Поле разрешающей способности сканирования по вертикали | 8.3.11 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 26 | Поле отношения размеров пикселей | 8.3.12 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |

### А.6.9 Данные геометрии контура кисти руки (ИСО/МЭК 19794-10:2007)

Таблица А.6.9

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | Статус профиля идентификации | Поддержка ДСР | Статус профиля верификации | Поддержка ДСР |
| 1 | Идентификатор формата | 7.1.1 | M | M | [да] | M | [да] | M | [да] |
| 2 | Номер версии | 7.1.2 | M | M | [да] | M | [да] | M | [да] |
| 3 | Размер записи | 7.1.3 | M | M | [да] | M | [да] | M | [да] |
| 4 | Число ЗГР | 7.1.4 | M | M | [да] | M | [да] | M | [да] |
| 5 | Поле, зарезервированное для будущего использования | 7.1.5 | M | M | [да] | M | [да] | M | [да] |
| 6 | Размер ЗГР | 7.2.1 | M | M | [да] | M | [да] | M | [да] |
| 7 | Индекс ЗГР | 7.2.2 | M | M | [да] | M | [да] | M | [да] |
| 8 | Идентификатор кисти руки | 7.2.3 | M | M | [да] | M | [да] | M | [да] |
| 9 | Состояние руки | 7.2.4 | | | | | | | |
| 10 | Разрешение данных контура | 7.2.5 | M | M | [да] | M | [да] | M | [да] |
| 11 | Геометрическое искажение | 7.2.6 | M | M | [да] | M | [да] | M | [да] |

*Окончание таблицы А.6.9*

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | Статус профиля идентификации | Поддержка ДСР | Статус профиля верификации | Поддержка ДСР |
| 12 | Качество контура кисти руки | 7.2.7 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 13 | Положение камеры по оси *X* | 7.2.8 | M | M | [да] | M | [да] | M | [да] |
| 14 | Положение камеры по оси *Y* | 7.2.9 | M | M | [да] | M | [да] | M | [да] |
| 15 | Положение камеры по оси *Z* | 7.2.10 | M | M | [да] | M | [да] | M | [да] |
| 16 | Положение области интереса по оси *X* | 7.2.11 | M | M | [да] | M | [да] | M | [да] |
| 17 | Положение области интереса по оси *Y* | 7.2.12 | M | M | [да] | M | [да] | M | [да] |
| 18 | Положение области интереса по оси *Z* | 7.2.13 | M | M | [да] | M | [да] | M | [да] |
| 19 | Положение начальной точки контура по оси *X* | 7.2.14 | M | M | [да] | M | [да] | M | [да] |
| 20 | Положение начальной точки контура по оси *Y* | 7.2.15 | M | M | [да] | M | [да] | M | [да] |
| 21 | Алгоритм сжатия данных контура | 7.2.16 | M | M | [да] | M | [да] | M | [да] |
| 22 | Технология регистрации контура кисти руки | 7.2.17 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 23 | Размер дополнительных данных | 7.2.18 | M | M | [да] | M | [да] | M | [да] |
| 24 | Зарезервировано для будущего использования | 7.2.19 | M | M | [да] | M | [да] | M | [да] |
| 25 | Данные контура | 7.2.20 | M | M | [да] | M | [да] | M | [да] |
| 26 | Дополнительные данные | 7.2.21 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |

### А.7 Технические стандарты интерфейса

#### А.7.1 БиоАПИ (ИСО/МЭК 19784-1:2006)

Примечание — В приведенной таблице А.7.1 определены требования соответствия, предъявляемые к поставщикам биометрических услуг (ПБУ), которые должны быть учтены в данном профиле. Это означает, что некоторые функции определяются как обязательные для ПБУ в случае, если приложение использует данную функцию. Требования соответствия, предъявляемые к приложению, ограничены требованиями, определенными в приложении А.1 БиоАПИ, заключающимися в том, чтобы вызов приложений ПБУ соответствовал спецификации БиоАПИ. Требования к использованию определенных вызовов в приложениях БиоАПИ не предъявляются.

Таблица А.7.1

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | Статус профиля идентификации | Поддержка ДСР | Статус профиля верификации | Поддержка ДСР |
| 1 | Системный реестр БиоАПИ | 10.2, 10.1.2 | M | M | [да] | M | [да] | M | [да] |
| 2 | BioSPI_BSP Load | 9.3.1.1 | M | M | [да] | M | [да] | M | [да] |
| 3 | BioSPI_BSP Unload | 9.3.1.2 | M | M | [да] | M | [да] | M | [да] |
| 4 | BioSPI_BSP Attach | 9.3.1.3 | M | M | [да] | M | [да] | M | [да] |
| 5 | BioSPI_BSP Detach | 9.3.1.4 | M | M | [да] | M | [да] | M | [да] |
| 6 | BioSPI_Query units | 9.3.1.5 | M | M | [да] | M | [да] | M | [да] |
| 7 | BioSPI_Query BFPs | 9.3.1.6 | O | M | [да] | M | [да] | M | [да] |
| 8 | BioSPI_Control unit | 9.3.1.7 | O | M | [да] | M | [да] | M | [да] |
| 9* | BioSPI_ Free BIR Handle | 9.3.2.1 | M | M | [да] | M | [да] | M | [да] |
| 10 | BioSPI_Get BIR From Handle | 9.3.2.2 | M | M | [да] | M | [да] | M | [да] |
| 11 | BioSPI_Get Header From Handle | 9.3.2.3 | M | M | [да] | M | [да] | M | [да] |
| 12 | BioSPI_Enable Events | 9.3.3.1 | M | M | [да, нет] | M | [да, нет] | M | [да, нет] |
| 13 | BioSPI_Set GUI Callbacks | 9.3.3.2 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| | | | | | | | | | |
| 14 | BioSPI_Capture | 9.3.4.1 | C | M | [да] | M | [да] | M | [да] |
| 14а | Возвращение необработанных/ проверенных данных | 9.3.4.1 | O | M | [да] | O | [да, нет] | O | [да, нет] |
| 14б | Возвращение качества в полученном заголовке ЗБИ | 9.3.4.1 | O | M | [да] | O | [да, нет] | O | [да, нет] |
| 14в | Подписание ЗБИ (ПБУ) | 9.3.4.1 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 14г | Шифрование ЗБИ (ПБУ) | 9.3.4.1 | O | X (см. примечание д) | [нет] | X (см. примечание д) | [нет] | X (см. примечание д) | [нет] |
| 14д | Определение источника | 9.3.4.1 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 14е | Поддержка приложения контроля GUI | 9.3.4.1 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 15 | BioSPI_Create Template | 9.3.4.2 | C | M | [да] | N/A | [n/a] | N/A | [n/a] |

** В оригинале ИСО/МЭК 24713-2 в нумерации пунктов таблицы А.7.1. допущена ошибка.*

*Продолжение таблицы А.7.1*

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | | Статус профиля идентификации | Поддержка ДСР | | Статус профиля верификации | Поддержка ДСР |
| 15а | Допустимый ввод хранимого шаблона для обновления/ адаптации шаблона | 9.3.4.2 | O | O | [да, нет] | | N/A | [n/a] | | N/A | [n/a] |
| 15б | Получение полезной нагрузки | 9.3.4.2 | O | O | [да, нет] | | N/A | [n/a] | | N/A | [n/a] |
| 15в | Возвращение качества в обработанном заголовке ЗБИ | 9.3.4.2 | O | M | [да] | | N/A | [n/a] | | N/A | [n/a] |
| 15г | Подписание ЗБИ (ПБУ) | 9.3.4.2 | O | O | [да, нет] | | N/A | [да, нет] | | N/A | [да, нет] |
| 15д | Шифрование ЗБИ (ПБУ) | 9.3.4.2 | O | X (см. примечание д) | [нет] | | N/A | [n/a] | | N/A | [n/a] |
| 16 | BioSPI_Process | 9.3.4.3 | C | N/A | [да, нет] | | O | [да, нет] | | O | [да, нет] |
| 16а | Возвращение качества в обработанном заголовке ЗБИ | 9.3.4.3 | O | N/A | [да, нет] | | O | [да, нет] | | O | [да, нет] |
| 16б | Подписание ЗБИ (ПБУ) | 9.3.4.3 | O | N/A | [да, нет] | | O | [да, нет] | | O | [да, нет] |
| 16в | Шифрование ЗБИ (ПБУ) | 9.3.4.3 | O | N/A | [нет] | | X (см. примечание д) | [нет] | | X (см. примечание д) | [нет] |
| 17 | BioSPI_ Process with aux BIR | 9.3.4.4 | O | N/A | [да, нет] | | O | [да, нет] | | O | [да, нет] |
| 18 | BioSPI_ Verify Match | 9.3.4.5 | C | N/A | [n/a] | | N/A | [n/a] | | M | [да] |
| | | | | | | | | | | | |
| 18а | Адаптация модели/шаблона | 9.3.4.5 | O | N/A | [n/a] | | N/A | [n/a] | | O | [да, нет] |
| 18б | Возвращение грубого множества | 9.3.4.5 | См. примечание г) | N/A | [n/a] | | N/A | [n/a] | | O | [да, нет] |
| 18в | Возвращение полезной нагрузки | 9.3.4.5 | O | N/A | [n/a] | | N/A | [n/a] | | O | [да, нет] |
| 19 | BioSPI_ Identify Match | 9.3.4.6 | C | N/A | [n/a] | | M | [да] | | N/A | [n/a] |
| 19а | Возвращение грубого множества | 9.3.4.6 | См. примечание г) | N/A | [n/a] | | O | [да, нет] | | N/A | [n/a] |
| 19б | Поддержка двоичности | 9.3.4.6 | O | N/A | [n/a] | | O | [да, нет] | | N/A | [n/a] |
| 20 | BioSPI_ Enrol | 9.3.4.7 | M | M | [да] | | N/A | [n/a] | | N/A | [n/a] |

*Продолжение таблицы А.7.1*

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | Статус профиля идентификации | Поддержка ДСР | Статус профиля верификации | Поддержка ДСР |
| 20а | Обновление шаблона | 9.3.4.7 | O | O | [да, нет] | N/A | [n/a] | N/A | [n/a] |
| 20б | Получение полезной нагрузки | 9.3.4.7 | O | O | [да, нет] | N/A | [n/a] | N/A | [n/a] |
| 20в | Возвращение необработанных/обработанных данных | 9.3.4.7 | O | M | [да] | N/A | [n/a] | N/A | [n/a] |
| 20г | Возвращение качества в зарегистрированном заголовке ЗБИ | 9.3.4.7 | O | M | [да] | N/A | [n/a] | N/A | [n/a] |
| 20д | Поддержка приложения контроля GUI | 9.3.4.7 | O | O | [да, нет] | N/A | [n/a] | N/A | [n/a] |
| 20е | Подписание ЗБИ (ПБУ) | 9.3.4.7 | O | O | [да, нет] | N/A | [n/a] | N/A | [n/a] |
| 20ж | Шифрование ЗБИ (ПБУ) | 9.3.4.7 | O | X (см. примечание д) | [нет] | N/A | [n/a] | N/A | [n/a] |
| 21 | BioSPI_Verify | 9.3.4.8 | M | N/A | [n/a] | N/A | [n/a] | M | [да] |
| 21а | Адаптация модели/шаблона | 9.3.4.8 | O | N/A | [n/a] | N/A | [n/a] | O | [да, нет] |
| 21б | Возвращение грубого множества | 9.3.4.8 | См. примечание г) | N/A | [n/a] | N/A | [n/a] | O | [да, нет] |
| 21в | Возвращение полезной нагрузки | 9.3.4.8 | O | N/A | [n/a] | N/A | [n/a] | O | [да, нет] |
| 21г | Возвращение необработанных/обработанных данных | 9.3.4.8 | O | N/A | [n/a] | N/A | [n/a] | O | [да, нет] |
| 21д | Поддержка приложения контроля GUI | 9.3.4.8 | O | N/A | [n/a] | N/A | [n/a] | O | [да, нет] |
| 21е | Подписание ЗБИ (ПБУ) | 9.3.4.8 | O | N/A | [n/a] | N/A | [n/a] | O | [да, нет] |
| 21ж | Шифрование ЗБИ (ПБУ) | 9.3.4.8 | O | N/A | [n/a] | N/A | [n/a] | O | [да, нет] |
| 22 | BioSPI_Identify | 9.3.4.9 | C | N/A | [n/a] | M | [да] | N/A | [n/a] |
| 22а | Возвращение грубого множества | 9.3.4.9 | См. примечание г) | N/A | [n/a] | O | [да, нет] | N/A | [n/a] |
| 22б | Поддержка двоичности | 9.3.4.9 | O | N/A | [n/a] | O | [да, нет] | N/A | [n/a] |
| 22в | Возвращение необработанных/обработанных данных | 9.3.4.9 | O | N/A | [n/a] | O | [да, нет] | N/A | [n/a] |

*Продолжение таблицы А.7.1*

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | Статус профиля идентификации | Поддержка ДСР | Статус профиля верификации | Поддержка ДСР |
| 22г | Поддержка приложения контроля GUI | 9.3.4.9 | O | N/A | [n/a] | O | [да, нет] | N/A | [n/a] |
| 22д | Подписание ЗБИ (ПБУ) | 9.3.4.9 | O | N/A | [n/a] | O | [да, нет] | N/A | [n/a] |
| 22е | Шифрование ЗБИ (ПБУ) | 9.3.4.9 | O | N/A | [n/a] | X (см. примечание д) | [нет] | N/A | [n/a] |
| 23 | BioSPI_Import | 9.3.4.10 | O | M | [да] | N/A | [n/a] | N/A | [n/a] |
| | | | | | | | | | |
| 24 | BioSPI_ db Open | 9.3.5.1 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 25 | BioSPI_ db Close | 9.3.5.2 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 26 | BioSPI_ db Create | 9.3.5.3 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 27 | BioSPI_ db Delete | 9.3.5.4 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 28 | BioSPI_ db Set Marker | 9.3.5.5 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 29 | BioSPI_ db Free Marker | 9.3.5.6 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 30 | BioSPI_ db Store BIR | 9.3.5.7 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 31 | BioSPI_ db Get BIR | 9.3.5.8 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 32 | BioSPI_db Ge tNext BIR | 9.3.5.9 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 33 | BioSPI_db Delete BIR | 9.3.5.10 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| | | | | | | | | | |
| 34 | BioSPI_Set Power Mode | 9.3.6.1 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 35 | BioSPI_ Set Indicator Status | 9.3.6.2 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 36 | BioSPI_ Get Power Mode | 9.3.6.3 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 37 | BioSPI_Calibrate Sensor | 9.3.6.4 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| | | | | | | | | | |
| 38 | BioSPI_Cancel | 9.3.7.1 | M | M | [да, нет] | M | [да, нет] | M | [да, нет] |
| 39 | BioSPI_Free | 9.3.7.2 | M | M | [да, нет] | M | [да, нет] | M | [да, нет] |

Примечания

а) Требования БиоАПИ применимы к биометрической технологии, такой как представленный в БиоАПИ совместимый модуль ПБУ.

б) Функции базы данных применяются только с: 1) автономными устройствами, 2) базами данных, контролируемыми ПБУ, 2а) смарт-картами (хранение на карте), 2б) механизмом поиска/сопоставления (один-ко-многим).

в) См. приложение А.4.6.2 спецификации БиоАПИ для описания дополнительных возможностей.

*Окончание таблицы А.7.1*

г) Возвращение показателей является обязательным; однако ПБУ имеет возможность возвращения непрерывных или ступенчатых/дополнительных (грубых) показателей. Это описано, но не предусмотрено в БиоАПИ.

д) Кодировка ЗБИ ПБУ запрещена в соответствии с данным профилем для обеспечения совместимости данных между ПБУ различных изготовителей. Кодировка с помощью приложения является необязательной.

е) Во время регистрации образца важно получить качественную информацию для принятия решения относительно перерегистрации (т. е. сравнивая его с пороговым значением критерия качества). Качество не является критичным для ЗБИ, предназначенных для немедленного сопоставления.

ж) Качество остается дополнительным параметром в 15а, так как является выходным параметром функции BioAPI_Process, которая не используется в процессе регистрации (BioAPI_Create Template используется при регистрации). (Статус может быть изменен на N/A, если это необходимо).

### А.7.2 ЕСФОБД (ИСО/МЭК 19785-1:2006)

Таблица А.7.2

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | Статус профиля идентификации | Поддержка ДСР | Статус профиля верификации | Поддержка ДСР |
| 1 | Стандартный биометрический заголовок (СБЗ) | 6.2.1 | M | M | [да] | M | [да] | M | [да] |
| 2 | Опции безопасности SBH | 6.2.1.1 | M | M | [да] | M | [да] | M | [да] |
| 3 | Опции сохранности | 6.2.1.2 | M | M | [да] | M | [да] | M | [да] |
| 4 | Заголовок записи ЕСФОБД | 6.2.1.3 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 5 | Заголовок версии patron | 6.2.1.4 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 6 | Биометрический тип | 6.2.1.5 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 7 | Тип биометрических данных | 6.2.1.7 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 8 | Биометрический подтип | 6.2.1.6 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 9 | Биометрические цели | 6.2.1.8 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 10 | Качество биометрических данных | 6.2.1.9 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 11 | Биометрическая дата создания | 6.2.1.10 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 12 | Период действительности | 6.2.1.11 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 13 | Индекс | 6.2.1.13 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 14 | Запрос/Подтверждение | 6.2.1.14 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 15 | Полезная нагрузка | 6.2.1.15 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |

*Окончание таблицы А.7.2*

| СТ базового стандарта | | | | СТ профиля и ДСР | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Пункт | Вопрос/Свойство | Ссылка в базовом стандарте | Статус базового стандарта | Статус профиля регистрации | Поддержка ДСР | Статус профиля идентификации | Поддержка ДСР | Статус профиля верификации | Поддержка ДСР |
| 16 | Подзаголовок/Счет базовой структуры | 6.2.1.16 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 17 | Разработчик | 6.2.1.12 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 18 | Владелец формата BDB | 6.2.1.17.1 | M | M | [да] | M | [да] | M | [да] |
| 19 | Тип формата BDB | 6.2.1.17.2 | M | M | [да] | M | [да] | M | [да] |
| 20 | Идентификатор продукта (PID) | 6.2.1.18 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 21 | Блок биометрических данных | 6.2.2 | M | M | [да] | M | [да] | M | [да] |
| 22 | Блок защиты информации | 6.2.3 | O | O | [да, нет] | O | [да, нет] | O | [да, нет] |
| 23 | Элементы данных | 6.2.5 | M | M | [да] | M | [да] | M | [да] |

Использование формата TLV — патрона в смарт-картах и в других токенах является обязательным (см. ИСО/МЭК 19785-3, пункт 11).

**Приложение В**
**(справочное)**

## Дополнительная информация

Настоящее приложение содержит дополнительную информацию, которая может быть использована администрацией аэропорта при вводе в эксплуатацию биометрической системы контроля доступа. Данная информация представлена только в качестве руководства и не устанавливает новых или дополнительных требований к системам, которые соответствуют требованиям настоящего стандарта.

**Отказоустойчивость**

В целях повышения отказоустойчивости устройства контроля доступа должны иметь такие автономные возможности, как хранение для урегулирования ситуаций, когда отсутствует или недоступна сеть. В тех случаях, когда сеть доступна, посредством нее должно производиться безопасное сохранение ее ревизионных и транзакционных записей (изображение каждого проходящего человека и проезжающего транспортного средства, полученное при помощи веб камер) на основной сервер. Система должна предоставлять эффективные средства для индексирования и поиска ошибок, являющихся статистическими, и оперативно выявлять попытки атак и отклонения от нормы. Она должна иметь возможность соотносить такие разрозненные записи о событиях, как изображения или логи, и объединять все транзакции в одну согласованную интерпретацию и при этом помечать все отклонения от нормы. Что касается зон или областей доступа, крайне значимым является возможность визуализации данных зон и постоянного отображения всего, что в них происходит. Также необходимо наличие определенного программного обеспечения для универсального механизма генерации отчетов.

**Проверка жизненности в биометрических системах**

*Введение*

Проверка жизненности в биометрических системах гарантирует, что только настоящие отпечатки пальцев, изображения лица, радужной оболочки глаза и иные характеристики могут быть применены для создания действительного биометрического шаблона. Считается, что биометрические системы способны проверить жизненность на основе биометрического образца. Результаты недавних испытаний, осуществленных научными институтами и СМИ, показывают, что многие ведущие современные биометрические системы подвержены атакам, при которых предъявленные поддельные отпечатки пальцев, статичные изображения лица или статичные изображения радужной оболочки глаза успешно используются как биометрические образцы. Данные поддельные образцы обрабатываются биометрической системой для создания шаблона и верификации зарегистрированных субъектов. Способы атак различны: предъявление отпечатков пальцев из желатина, накладывание изображения радужной оболочки глаза на контактную линзу и даже использование дыхания для того, чтобы на поверхности датчика проявился след отпечатка пальца предыдущего пользователя системой. Наиболее опасна ситуация, при которой биометрическая система создает действительный эталон при предъявлении части тела неживого человека. Подобные ситуации являются недопустимыми, и те системы, которые не способны выдержать атак подобного рода, должны быть запрещены. С тех пор, как биометрия широко используется в государственном и частном секторах для идентификации граждан, безопасности сетей, пограничного контроля, аутентификации в терминале для производства платежей в месте совершения покупки, в сфере биометрических технологий вопрос проверки жизненности должен быть поставлен остро. Если биометрические системы так легко подвержены обману, то их пока нельзя воспринимать в качестве нового средства решения проблем безопасности.

*Принцип проверки жизненности*

Биометрические системы состоят из элементов получения и элементов обработки. Элементы получения записывают, изображают или другим образом захватывают необработанные данные: отпечатки пальцев, изображения лица, фотографии и т. д. Элементы обработки сканируют эти необработанные данные для выявления отличительных или идентифицируемых характеристик и преобразовывают эту информацию в биометрический эталон. Процесс обнаружения жизненности может быть осуществлен на стадии получения, при этом данные от неживого человека не будут приниматься, или на стадии обработки, — данные от неживого человека не будут обрабатываться. Вопрос в том, как проверить жизненность; например, в чем состоит разница между живым пальцем и неживым/поддельным? Теоретически проверка жизненности основана на утверждении, что одно или более свойств биометрического образца соответствуют свойствам, связанным с «живыми» биометрическими образцами. Биометрическая система должна быть разработана и создана с учетом этого утверждения. Необходимо уделять особое внимание элементам получения и элементам обработки биометрической системы для проверки жизненности и методам их обработки. Возможно, окажется необходимым внедрение дополнительных датчиков для проверки жизненности и методов обработки данных.

*Обман биометрической системы*

Как было отмечено ранее, существует несколько способов обмануть биометрическую систему:

1) получить биометрическую характеристику силой, например отрезав палец;

2) заставить человека предъявить биометрическую характеристику;

3) получить биометрический образец без участия человека, например снять отпечаток пальца с объекта, к которому прикоснулся человек, или сфотографировать данный отпечаток пальца;

4) сделать копию биометрической характеристики при участии человека;

5) внести поддельную биометрическую информацию в электронном виде (изображение) сразу после стадии получения;

6) внести поддельную биометрическую информацию в электронном виде (шаблон) сразу после стадии обработки.

Каждый способ обмана может быть обнаружен разными методами, но все эти способы могут быть классифицированы как проверка жизненности, кроме пункта 2. Данный способ обмана не может быть обнаружен методами проверки жизненности. Что касается пунктов 5 и 6, то все зависит от природы входного сигнала.

*Проверка жизненности на практике*

**Регистрация**

Практически во всех случаях процесс регистрации является подконтрольным процессом, в котором должны быть задействованы все процедуры и проверки для того, чтобы предъявление поддельных биометрических данных вызвало как можно больше затруднений. В этом случае применение в биометрических системах дополнительных мер по автоматической проверке жизненности не понадобится.

**Верификция**

Для процесса верификации в дополнение к предъявлению биометрической характеристики требуется ввод ПИН-кода или, как описано в настоящем стандарте, токена.

**Обман**

Системе требуется действительный токен и действительная биометрическая информация. Проверка жизненности крайне необходима в неконтролируемых системах и особенно — в удаленных пунктах.

**Идентификация**

В данном случае для получения доступа требуется лишь хорошо скопированная поддельная биометрическая информация. Очевидно, что неконтролируемый вход, на котором применяется биометрическая идентификация, является наиболее слабым элементом всей системы безопасности. Разработка эффективного способа проверки жизненности в биометрической системе способна улучшить ситуацию, но необходимо признать, что любая система проверки жизненности может быть обманута. Проблема безопасности не может быть решена при помощи только биометрии, но в том случае, если биометрия является частью общей концепции безопасности и если ее разработчик принимает во внимание возможность обмана биометрического идентификационного номера, приемлемое решение проблемы безопасности может быть найдено.

**Биометрическая система контроля доступа с использованием смарт-карты**

Биометрическая система контроля доступа с использованием смарт-карты является общей архитектурой, описывающей систему, которая обеспечивает безопасность точки входа на базе биометрической аутентификации с использованием смарт-карты. Соответствие (применение) данной архитектуры предполагает использование безопасных передач посредством криптографической защиты передаваемых данных, таких как биометрический эталон, информация о конечном пользователе, контрольный код смарт-карты. Также необходимо наличие схем предотвращения таких неправомерных атак, как атака путем коррекции эталона. Необходимо обеспечить обновление системы для устранения любых возможных «лазеек», которые обнаруживаются после предоставления аппаратного устройства конечному пользователю. Обновление программно-аппаратного обеспечения необходимо осуществлять по безопасным каналам с целью предотвращения загрузки вредоносного кода, способного обойти систему. В случае системы с бесконтактными смарт-картами разработчик должен внедрить в систему устройство радиотехнической защиты для снижения риска электромагнитного перехвата информации и наложения информации в процессе аутентификации. Журналы событий должны содержать дату и время событий в целях проверки безопасности.

В случае с системами, применяющими биометрическое сопоставление вне карт как способ аутентификации в системе, использующей смарт-карты, необходимо наличие и соблюдение схемы управления безопасностью для защиты информации от попадания на неавторизированные терминалы. В случае с такими областями применения биометрии, как контроль иммиграции, где требуется высокий уровень безопасности, необходимо принимать еще более надежные меры, например по проверке жизненности для предотвращения атак с использованием поддельных биометрических данных, и обеспечивать надлежащие способы оповещения администрации об атаках. Результат биометрического сопоставления должен быть сессией, помеченной цифровым способом контроллером смарт-карт, или системой с сопоставлением на карте, что в большей степени безопасно.

Пользовательский интерфейс (ПИ) должен быть удобен в использовании для любого конечного пользователя, руководство по его эксплуатации должно быть понятным, у пользователя не должно возникать проблем с предоставлением биометрической характеристики данной модальности. ПИ должен предоставлять надлежащую обратную связь, чтобы конечный пользователь был осведомлен о ходе процесса аутентификации, и обеспечивать пользователю помощь в случае возникновения ошибки системы или проблемы при получении биометрического образца.

**Приложение С**
**(справочное)**

## Меры по обеспечению безопасности

Примечание — В данном приложении описаны общие меры по обеспечению безопасности, которые не являются ни исчерпывающими, ни конкретными для представленной реализации системы. Вследствие этого их необходимо воспринимать как исходную точку для разработки профиля безопасности для конкретной системы.

### С.1 Подходы

Так как биометрическая система контроля доступа нуждается в постоянном усовершенствовании безопасности, необходимо учитывать как требования к безопасности, так и требования к функциональности и возможности взаимодействия. Данные требования включают в себя как свойственные биометрическим системам, так и вообще информационным системам требования.

В процессе анализа требований к безопасности необходимо оценивать значимость ресурсов, которые должны быть защищены, и потенциальные угрозы для них. После того как риски безопасности идентифицированы и учтено соотношение издержки/результат, можно задействовать надлежащие меры по противодействию угрозам.

Более того, необходимость учитывать эффективность функций информационной безопасности и управления операциями должна быть обоснована, так как эффективность всей системы безопасности определяется эффективностью самого слабого звена системы. Вследствие этого необходимо обращать пристальное внимание как на наличие, так и на согласованность мер по противодействию и совместно учитывать технические и операционные составляющие.

### С.2 Репрезентативный перечень угроз

**Угрозы, связанные с функциями информационных систем**

| Угроза | Описание |
|---|---|
| Попытка выдать себя за другое лицо посредством искажения или фальсификации | Угрозы, при которых атакующий использует свой собственный биометрический эталон вместо зарегистрированного биометрического эталона посредством искажения, фальсификации или замещения биометрического эталона при попытке выдать себя за зарегистрированного пользователя |
| Попытка выдать себя за другое лицо посредством изменения пороговых значений | Угрозы, при которых атакующий искажает такие параметры аутентификации, как пороговые значения, и пытается сделать так, чтобы результат верификации идентификационной информации был положительным при попытке выдать себя за зарегистрированного пользователя |
| Утечка биометрического шаблона | Угроза, при которой происходит утечка биометрической информации сотрудника посредством незаконного считывания биометрического шаблона с токена |
| Утечка информации о сотрудниках | Угроза, при которой происходит утечка информации о сотрудниках посредством незаконного считывания с биометрической системы аутентификации |

**Угрозы, связанные с действиями**

| Угроза | Описание |
|---|---|
| Инфраструктура информационной безопасности | Организациям, использующим биометрические системы аутентификации, рекомендуется обеспечить безопасность данных и создать структуру управления безопасностью с целью отслеживания условий ее работы |
| Безопасность при определении задания и комплектовании штатов | Необходимо определить ответственность сотрудников за обеспечение безопасности для снижения риска ошибки, связанной с человеческим фактором, кражами, незаконными действиями или неправильной эксплуатацией оборудования |
| Обучение сотрудников | Сотрудники, эксплуатирующие систему аутентификации, должны быть хорошо обучены обращению с ней, должны быть осведомлены обо всем, что связано с безопасностью данных, чтобы возможные риски угрозы безопасности были сведены к минимуму |

*Продолжение*

| Угроза | Описание |
|---|---|
| Физическая безопасность и безопасность окружающей среды | Для предотвращения несанкционированного доступа к оборудованию и рабочим данным |
| Порядок действий и ответственность | Для обеспечения исправного и безопасного функционирования биометрических систем аутентификации необходимо определить ответственность и порядок действий по управлению всем оборудованием по обработке информации |
| Ответные действия при возникновении особых ситуаций и неисправностей | С целью сведения вреда от особых ситуаций и неисправностей к минимуму сотрудники обязаны сообщить о возникновении событий или происшествий, которые могут негативно повлиять на безопасность, а также об уязвимых местах системы |
| Попытка выдать себя за другое лицо при помощи артефактов | Угрозы, при которых атакующий использует физические артефакты по отношению к устройству захвата биометрического образца при попытке выдать себя за зарегистрированного пользователя |
| Попытка выдать себя за другое лицо при помощи атак «piggyback» | Угрозы, при которых зарегистрированный пользователь проходит аутентификацию, а сторонний человек проникает в помещение вместе с зарегистрированным пользователем |
| Регистрация сотрудников-самозванцев | Угрозы, при которых сотрудники, имеющие доступ в помещение с ресурсами, являются самозванцами, способными создать аутентификационный токен |
| Попытка выдать себя за другое лицо путем использования альтернативных действий | Угрозы, при которых атакующий намеренно вызывает ложный недопуск или отказ в сборе данных с целью применить уязвимый альтернативный метод, таким образом выдав себя за другое лицо |
| Попытка выдать себя за другое лицо, связанная с точностью аутентификации | Угрозы, при которых используются слабые места в системе защиты с целью выдать зарегистрированного пользователя за другое лицо |
| Утечка данных вследствие недостаточного уровня управления | Угрозы, при которых происходит утечка данных вследствие недостаточного уровня управления носителем информации, который производит запись данных в биометрическую систему аутентификации |
| Утечка данных вследствие ошибки в настройках сети | Угроза, при которой происходит утечка данных вследствие генерации незаконного доступа, так как сеть настроена неверно из-за ошибки эксплуатации и т. д. |
| Утечка данных из-за неверного поступка администратора | Угроза, при которой происходит утечка данных из-за неверного поступка системного администратора |

**Приложение ДА**
**(справочное)**

## Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации приведены в таблице ДА.1.

Таблица ДА.1

| Обозначение ссылочного международного стандарта | Степень соответствия | Обозначение и наименование соответствующего национального стандарта |
|---|---|---|
| ИСО/МЭК 19784-1:2006 | IDT | ГОСТ Р ИСО/МЭК 19784-1—2007 «Автоматическая идентификация. Идентификация биометрическая. Биометрический программный интерфейс. Часть 1. Спецификация биометрического программного интерфейса» |
| ИСО/МЭК 19785-1:2006 | IDT | ГОСТ Р ИСО/МЭК 19785-1—2008 «Автоматическая идентификация. Идентификация биометрическая. Единая структура форматов обмена биометрическими данными. Часть 1. Спецификация элементов данных» |
| ИСО/МЭК 19785-3:2007 | — | * |
| ИСО/МЭК 19794-2:2005 | IDT | ГОСТ Р ИСО/МЭК 19794-2—2005 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца — контрольные точки» |
| ИСО/МЭК 19794-3:2006 | IDT | ГОСТ Р ИСО/МЭК 19794-3—2009 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 3. Спектральные данные изображения отпечатка пальца» |
| ИСО/МЭК 19794-4:2005 | IDT | ГОСТ Р ИСО/МЭК 19794-4—2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца» |
| ИСО/МЭК 19794-5:2005 | IDT | ГОСТ Р ИСО/МЭК 19794-5—2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица» |
| ИСО/МЭК 19794-6:2005 | IDT | ГОСТ Р ИСО/МЭК 19794-6—2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза» |
| ИСО/МЭК 19794-7:2007 | IDT | ГОСТ Р ИСО/МЭК 19794-7—2009 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 7. Данные динамики подписи» |
| ИСО/МЭК 19794-8:2006 | IDT | ГОСТ Р ИСО/МЭК 19794-8—2009 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 8. Данные структуры остова отпечатка пальца» |
| ИСО/МЭК 19794-9:2007 | IDT | ГОСТ Р ИСО/МЭК 19794-9—2009 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 9. Данные изображения сосудистого русла» |
| ИСО/МЭК 19794-10:2007 | IDT | ГОСТ Р ИСО/МЭК 19794-10—2010 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 10. Данные геометрии контура кисти руки» |
| ИСО/МЭК 19795-1:2006 | IDT | ГОСТ Р ИСО/МЭК 19795-1—2007 «Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура» |
| ИСО/МЭК 19795-2:2007 | IDT | ГОСТ Р ИСО/МЭК 19795-2—2008 «Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 2. Методы проведения технологического и сценарного испытаний» |
| ИСО/МЭК 24713-1:2008 | — | * |

* 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 стандарта:

- IDT — идентичный стандарт.

## Библиография


[1] ISO/IEC 7816 (all parts), Identification cards — Integrated circuit cards

[2] ISO/IEC 7816-11:2004, Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods

[3] ISO/IEC 9646-7:1995/Cor.1:1997, Information technology — Open Systems Interconnection — Conformance testing methodology and framework — Part 7: Implementation Conformance Statements — Technical Corrigendum 1

[4] ISO/IEC 9796:1991, Information technology — Security techniques — Digital signature scheme giving message recovery

[5] ISO/IEC 11770 (all parts), Information technology — Security techniques — Key management

[6] ISO/IEC 15408 (all parts), Information technology — Security techniques — Evaluation criteria for IT security

[7] ISO/IEC 18031:2005, Information technology — Security techniques — Random bit generation

[8] ISO/IEC 18032:2005, Information technology — Security techniques — Prime number generation

[9] ISO/IEC 18033 (all parts), Information technology — Security techniques — Encryption algorithms

[10] ISO 19092, Financial services — Biometrics — Security framework

[11] NIST IR 6887, Government Smart Card Interoperability Specification (GSC-IS)

[12] ITU-T X.509, Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks



УДК 004.93 ' 1:006.89 ОКС 35.040 П85

Ключевые слова: автоматическая идентификация, биометрическая идентификация, контроль доступа, безопасность, аэропорт

Редактор *Н.Н. Кузьмина*
Технический редактор *Н.С. Гришанова*
Корректор *В.И. Варенцова*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 09.08.2012. Подписано в печать 10.09.2012. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 5,12. Уч.-изд. л. 4,80. Тираж 114 экз. Зак. 764.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.

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

Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ.
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.

gost.e-ecolog.ru