ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 24713-3— 2016

Информационные технологии

БИОМЕТРИЯ

Биометрические профили для взаимодействия и обмена данными

Часть 3

Биометрическая верификация и идентификация моряков

(ISO/IEC 24713-3:2009, Information technology — Biometric profiles for interoperability and data interchange — Part 3: Biometrics-based verification and identification of seafarers, IDT)

Издание официальное

Москва
Стандартинформ
2016

Предисловие

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 перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 098 «Биометрия и биомониторинг»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 7 июня 2016 г. № 534-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 24713-3:2009 «Информационные технологии. Биометрические профили для взаимодействия и обмена данными. Часть 3. Биометрическая верификация и идентификация моряков» (ISO/IEC 24713-3:2009 «Information technology — Biometric profiles for interoperability and data interchange — Part 3: Biometrics-based verification and identification of seafarers», IDT).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2012 (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

6 Некоторые элементы настоящего стандарта могут быть объектами патентных прав. Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК) не несут ответственности за установление подлинности каких-либо или всех таких патентных прав

Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в годовом (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующие информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

Международная организация труда (далее — МОТ) в ответ на запрос Международной морской организации утвердила Конвенцию № 185 (пересмотренную) 2003 года об удостоверениях личности моряков (далее — УЛМ). Согласно данной конвенции у всех моряков из ратифицированных стран должно быть удостоверение личности, которое имеет единый формат, определенные физические элементы защиты и использует биометрию для привязки удостоверения личности к моряку. В настоящее время Конвенция № 185 предписывает использование двух отпечатков пальцев, хранящихся в двумерном штрихкоде, но биометрическая модальность и носитель данных могут быть изменены при условии сохранения обратной совместимости.

В целях поддержки системы УЛМ, обеспечивающей взаимодействие в глобальном масштабе, в настоящем стандарте определен биометрический профиль, устанавливающий использование биометрии для верификации и идентификации моряков на различных этапах выдачи и проверки документа. В настоящем стандарте определены базовые стандарты и критерии для применения данных стандартов в приложениях выдачи УЛМ, а для привязки каждого документа к моряку, которому он выдан, используется биометрия. В настоящем стандарте рассмотрены процессы биометрической регистрации, верификации и идентификации моряков для того, чтобы биометрические компоненты системы могли быть использованы надлежащим образом. В настоящем стандарте также рассматриваются другие компоненты системы, влияющие на использование биометрических технологий, такие как носители информации биометрических данных и защита системы. Настоящий стандарт предназначен для использования в морском судоходстве, но может быть использован и в других областях, где требуются биометрическая верификация и идентификация держателей документов при выдаче или проверке документов.

Биометрические данные используются для проверки личности при выдаче документа, для проверки по списку разыскиваемых лиц и базе данных моряков с выданными удостоверениями для предотвращения ситуации, когда у одного моряка имеется несколько УЛМ.

Использование биометрических данных также включает в себя верификацию, когда в пункте проверки лицом, предположительно моряком — владельцем карты, предъявляется карта. Такие пункты проверки могут включать в себя входы в порты, на трапы корабля, в пункты пересечения границы, где моряк должен быть проверен иммиграционными органами, и любые другие ситуации, когда моряк должен подтвердить свою личность в качестве моряка. Предполагается, что такая верификация должна выполняться не только в помещении в контролируемых условиях, но и на открытом воздухе в сложных условиях, включая дождливую погоду, соленые брызги, высокую влажность и высокую температуру. Биометрическое оборудование и УЛМ должны функционировать при всех вышеперечисленных условиях.

Настоящий стандарт не противоречит существующей международной Конвенции № 185, утвержденной МОТ и ратифицированной различными государствами — членами МОТ. Напротив, методики настоящего стандарта могут быть использованы для соответствия требованиям текущей версии Конвенции МОТ № 185. В то же время в настоящем стандарте представлены альтернативные методики для их использования МОТ в будущем, если будут изменены технические документы, связанные с Конвенцией МОТ № 185 или ее приложениями. В связи с этим подчеркивается важность обратной совместимости. В настоящем стандарте используются концепции шаблона отпечатков двух пальцев на основе контрольных точек для верификации моряков, отображения фотографии подписи в видимой области УЛМ и использования двумерного штрихкода как носителя данных, основополагающий выбор которых уже сделан МОТ. Альтернативные технологии в настоящем стандарте определены таким образом, чтобы обеспечить обратную совместимость с существующими УЛМ.

Настоящий стандарт определяет формат ведущей организации ЕСФОБД (приложение В) и блок защиты информации ЕСФОБД (приложение С), которые подходят для условия ограниченности количества информации для записи в двумерном штрихкоде и могут применяться в других условиях ограниченного объема памяти.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

БИОМЕТРИЯ

Биометрические профили для взаимодействия и обмена данными

Часть 3

Биометрическая верификация и идентификация моряков

Information technologies. Biometrics. Biometric profiles for interoperability and data interchange.
Part 3. Biometric-based verification and identification of seafarers

Дата введения — 2017—07—01

1 Область применения

Настоящий стандарт определяет биометрический профиль, включающий в себя форматы обмена данными, системные требования и биометрические процедуры для УЛМ.

Область применения может быть расширена на ситуации, где требуется совместимое удостоверение личности на основе биометрии, но основной целью настоящего стандарта является использование биометрии на УЛМ.

В Конвенции МОТ № 185 уже введено комплексное стратегическое руководство по биометрической верификации и идентификации моряков, и настоящий стандарт основывается на указанном руководстве. Обсуждение любых вопросов стратегии, помимо включенных в Конвенцию МОТ № 185 или противоречащих им, выходит за рамки настоящего стандарта.

2 Соответствие

Все УЛМ, системы выдачи УЛМ и системы биометрической верификации или идентификации моряков соответствуют настоящему стандарту, если они соответствуют обязательным требованиям раздела 6 и обязательных приложений настоящего стандарта.

3 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты, которые необходимо учитывать при его использовании. В случае датированных ссылок необходимо пользоваться только указанной редакцией. В случае недатированных ссылок следует пользоваться последней редакцией ссылочных документов, включая любые поправки и изменения к ним.

ISO/IEC 7501-1 Identification cards — Machine readable travel documents — Part 1: Machine readable passport (Карты идентификационные. Машиносчитываемые паспортно-визовые документы. Часть 1. Машиносчитываемый паспорт)

ISO/IEC 7501-3 Identification cards — Machine readable travel documents — Part 3: Machine readable official travel documents (Карты идентификационные. Машиносчитываемые паспортно-визовые документы. Часть 3. Машиносчитываемые официальные документы)

Издание официальное

ISO/IEC 8824-1:2002[1] Information technology — Abstract Syntax Notation One (ASN.1) — Part 1: Specification of basic notation [Информационные технологии. Абстрактная синтаксическая нотация версии один (АСН.1). Часть 1. Спецификация основной нотации]

ISO/IEC 8825-1:2002[2] Information technology — ASN.1 encoding rules — Part 1: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) [Информационные технологии. Правила кодирования АСН.1. Часть 1. Спецификация базовых (BER), канонических (CER) и отличительных (DER) правил кодирования»]

ISO/IEC 8825-2:2002[3] Information technology — ASN.1 encoding rules — Part 1. Specification of Packed Encoding Rules (PER) [Информационные технологии. Правила кодирования АСН.1. Часть 2. Спецификация правил уплотненного кодирования (PER)]

ISO/IEC 15438:2006[4] Information technology — Automatic identification and data capture techniques — PDF417 bar code symbology specification (Информационные технологии. Методы автоматической идентификации и сбора данных. Спецификации на символику штрихкода PDF417)

ISO/IEC 19785-1:2006[5] Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification (Информационные технологии. Единая структура форматов обмена биометрическими данными. Часть 1. Спецификация элементов данных)

ISO/IEC 19785-3:2007[6] Information technology — Common Biometric Exchange Formats Framework — Part 3: Patron format specifications (Информационные технологии. Единая структура форматов обмена биометрическими данными. Часть 3. Спецификации форматов ведущей организации)

ISO/IEC 19794-2:2005[7] Information technology — Biometric data interchange formats — Part 2: Finger minutiae data (Информационные технологии. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца — контрольные точки)

ISO/IEC 19794-4:2005[8] Information technology — Biometric data interchange formats — Part 4: Finger image data (Информационные технологии. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца)

ISO/IEC 19794-5:2005[9] Information technology — Biometric data interchange formats — Part 5: Face image data (Информационные технологии. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица)

ISO/IEC 19795-4:2008 Information technology — Biometric performance testing and reporting — Part 4: Interoperability performance testing (Информационные технологии. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 4. Испытания на совместимость)

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

ISO/IEC 29109-1 Information technology — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Part 1: Generalized conformance testing methodology (Ин-

---

[1] Заменен на ISO/IEC 8824-1:2015. Однако для однозначного соблюдения требования настоящего стандарта, выраженного в датированной ссылке, рекомендуется использовать только указанное в этой ссылке издание.

[2] Заменен на ISO/IEC 8825-1:2015. Однако для однозначного соблюдения требования настоящего стандарта, выраженного в датированной ссылке, рекомендуется использовать только указанное в этой ссылке издание.

[3] Заменен на ISO/IEC 8825-2:2015. Однако для однозначного соблюдения требования настоящего стандарта, выраженного в датированной ссылке, рекомендуется использовать только указанное в этой ссылке издание.

[4] Заменен на ISO/IEC 15438:2015. Однако для однозначного соблюдения требования настоящего стандарта, выраженного в датированной ссылке, рекомендуется использовать только указанное в этой ссылке издание.

[5] Заменен на ISO/IEC 19785-1:2015. Однако для однозначного соблюдения требования настоящего стандарта, выраженного в датированной ссылке, рекомендуется использовать только указанное в этой ссылке издание.

[6] Заменен на ISO/IEC 19785-3:2015. Однако для однозначного соблюдения требования настоящего стандарта, выраженного в датированной ссылке, рекомендуется использовать только указанное в этой ссылке издание..

[7] Заменен на ISO/IEC 19794-2:2011. Однако для однозначного соблюдения требования настоящего стандарта, выраженного в датированной ссылке, рекомендуется использовать только указанное в этой ссылке издание.

[8] Заменен на ISO/IEC 19794-4:2011. Однако для однозначного соблюдения требования настоящего стандарта, выраженного в датированной ссылке, рекомендуется использовать только указанное в этой ссылке издание.

[9] Заменен на ISO/IEC 19794-5:2011. Однако для однозначного соблюдения требования настоящего стандарта, выраженного в датированной ссылке, рекомендуется использовать только указанное в этой ссылке издание.

формационные технологии. Методология испытаний на соответствие форматам обмена биометрическими данными, определенным в комплексе стандартов ИСО/МЭК 19794. Часть 1. Обобщенная методология испытаний на соответствие)

4 Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК 19794-1, а также следующие термины с соответствующими определениями:

Примечание — Некоторые термины не определены, но использованы в настоящем стандарте. В частности, «орган проверки УЛМ», «орган выдачи УЛМ» и «координационный центр» являются терминами, которые определяются юридическими лицами — представителями МОТ и могут различаться в разных странах. Данные термины используются в Конвенции МОТ № 185, но их точное определение лучше оставить толкованию правовых экспертов МОТ. Дальнейшие объяснения можно получить в Конвенции МОТ № 185 [3] или путем проведения консультаций с МОТ.

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

4.2 **биометрическая регистрация** (biometric enrolment): Процесс создания и сохранения записи биометрических данных, содержащей биометрический(ие) контрольный(ые) шаблон(ы) и небиометрические данные индивида.

4.3 **биометрический признак** (biometric feature): Цифровое представление информации, извлеченное из биометрических образцов и используемое для сравнения.

4.4 **биометрическая модель** (biometric model): Хранимая функция (зависит от субъекта биометрических данных), созданная из одного или более биометрических признаков.

4.5 **биометрический контрольный шаблон** (biometric reference): Один или более хранимых биометрических образцов, биометрических шаблонов или биометрических моделей, относящихся к субъекту биометрических данных и используемых для сравнения.

4.6 **зарегистрированная личность** (enrolee): Человек, биометрический контрольный шаблон которого записан для выпуска УЛМ.

4.7 **чип ИС** (IC chip): Процессор и устройство памяти, содержащие информацию для верификации личности моряка и встроенные в УЛМ для считывания в пункте проверки УЛМ, оснащенном соответствующим оборудованием.

Примечание — Термин «бесконтактная интегральная схема» имеет то же значение.

4.8 **моряк** (seafarer): Лицо, трудящееся по найму, занятое или работающее в любом качестве на борту судна (за исключением военных кораблей), обычно используемого в морском судоходстве.

4.9 **удостоверение личности моряка; УЛМ** (Seafarers' Identity Document; SID): Документ, содержащий идентификационные сведения о моряке, в том числе демографическую информацию, фотографию моряка и биометрические данные, хранимые в штрихкоде PDF417 и опционально в чипе ИС.

Примечание — Предполагается, что в ближайшее время наличие чипа ИС на УЛМ будет опциональным, но по мере перевода большей части выпускаемых документов на технологию чипа ИС биометрическая верификация с использованием чипа ИС станет повсеместной.

4.10 **пункт проверки УЛМ** (SID verification station): Система аппаратного и программного обеспечения, которая поддерживает биометрическую верификацию моряка по информации, записанной на УЛМ, и, опционально, проверку УЛМ по защищенной электронной базе данных органа выдачи УЛМ в режиме онлайн[1)].

Примечание — Один орган проверки УЛМ часто имеет несколько пунктов проверки УЛМ, некоторые из которых должны функционировать на судах или в других сложных условиях, где электронный доступ отсутствует.

[1)] Онлайн — осуществляемый в режиме реального времени.

5 Сокращения

В настоящем стандарте применены следующие сокращения:

ЕСФОБД — Единая структура форматов обмена биометрическими данными (Common Biometric Exchange Formats Framework, CBEFF);

МОТ — Международная организация труда (International Labour Organization, ILO);

УЛМ — Удостоверение личности моряка (Seafarers' Identity Document, SID).

6 Требования

6.1 Общие положения

В данном разделе представлены требования для системы УЛМ, обеспечивающей взаимодействие в глобальном масштабе, для биометрической верификации и идентификации моряков. Требования сосредоточены на биометрических аспектах области применения, но также затронуты другие аспекты, влияющие на использование биометрии. Данные требования должны находиться в соответствии с нормативными требованиями Конвенции (пересмотренной) 2003 года об удостоверениях личности моряков (№ 185) [3] и должны обеспечить обратную совместимость с существующими методиками МОТ и уже выпущенными УЛМ. В настоящее время в существующей Конвенции МОТ № 185 есть требования, которые с большой вероятностью не будут изменяться, и настоящий стандарт нормативно предъявляет их для всех операций биометрической верификации и идентификации моряков. С разрешения МОТ для определения требований в настоящем стандарте цитируются определенные части Конвенции МОТ № 185. Соответствующие разделы Конвенции МОТ № 185 представлены в 6.2 (оригинальная нумерация изменена ввиду цитирования без полного текста Конвенции МОТ № 185).

6.2 Требования Конвенции МОТ № 185 к УЛМ

6.2.1 Физические характеристики документа

УЛМ составляется в простой форме, изготавливается из прочных материалов с учетом особых условий работы в море и является пригодным для машинного считывания. Используемые материалы:

a) препятствуют по мере возможности подделке или подлогу этого документа и позволяют легко обнаруживать изменения;

b) доступны для всех правительств при минимальных затратах и обеспечивают надежное достижение цели, поставленной выше в перечислении a).

Примечание 1 — Данное требование исходит из статьи 3 пункта 2 Конвенции МОТ № 185 [3].

Примечание 2 — Более подробная информация по данному требованию о схеме расположения и спецификации документа изложена в ИСО/МЭК 7501-1 — для документа-буклета размером TD-3 или в ИСО/МЭК 7501-3 — для документа-карты размером TD-1 (что предпочтительнее).

6.2.2 Демографические данные, включенные в документ

В УЛМ включаются только следующие сведения о его владельце:

a) имя полностью (фамилия, имя и другие части имени, если таковые имеются);

b) пол;

c) дата и место рождения;

d) гражданство;

e) любые особые физические приметы, которые могут оказаться полезными для идентификации личности;

f) цифровая фотография или оригинал фотографии;

g) подпись.

Примечание — Это требование исходит из статьи 3 пункта 7 Конвенции МОТ № 185 [3].

6.2.3 Биометрические данные, включенные в документ

Независимо от положений 6.2.2, УЛМ должно также содержать шаблон биометрических элементов или представленные в иной форме биометрические данные владельца при условии соблюдения следующих предварительных условий:

a) биометрические данные могут быть получены без нарушения неприкосновенности частной жизни соответствующих лиц, без причинения им неудобств, без риска для их здоровья или посягательства на их личное достоинство;

b) биометрические данные должны быть визуально различимы в УЛМ, причем возможность их воспроизводства с шаблона или с другой формы представления должна быть исключена;

Примечание — Это требование интерпретируется как то, что шаблон отпечатка пальца, являющийся биометрическим представлением, должен быть видимым путем кодирования в двумерный штрихкод. Так как шаблон отпечатка пальца по ИСО/МЭК 19794-2 состоит из бифуркаций и конечных точек, что является только частью информации оригинальных биометрических данных отпечатка пальца, то таким образом удовлетворяется требование исключить возможность их воспроизводства.

c) необходимое для получения и проверки биометрических данных оборудование должно быть удобным в эксплуатации и в целом доступным для правительств по низкой стоимости;

d) оборудование, необходимое для проверки биометрических данных, можно легко и надежно эксплуатировать в портах и других местах, в том числе на борту судна, где обычно проводится проверка личности моряков компетентными органами;

e) система, в рамках которой должны использоваться биометрические данные (в том числе оборудование, технологии и применяемые процедуры), позволяет получать результаты, которые имеют единообразный характер и обеспечивают надежную идентификацию личности.

Примечание — Данное требование исходит из статьи 3 пункта 8 Конвенции МОТ № 185 [3].

6.2.4 Видимость данных

Все данные о моряке вносятся в УЛМ таким образом, чтобы они были визуально различимы. Морякам обеспечивается беспрепятственный доступ к оборудованию, позволяющему им проверять любые касающиеся их данные, которые нельзя прочитать невооруженным глазом. Такой доступ предоставляется органом выдачи УЛМ или от его имени.

Примечание — Данное требование исходит из статьи 3 пункта 9 Конвенции МОТ № 185 [3].

6.2.5 Защищенная электронная база

Каждое государство — член МОТ обеспечивает, чтобы записи о каждом выданном им УЛМ, об УЛМ, действие которого временно приостановлено им или которое оно изъяло, хранились в электронной базе данных. Принимаются необходимые меры для защиты этой базы данных от внедрения в нее или несанкционированного доступа к ней.

Примечание 1 — Данное требование исходит из статьи 4 пункта 1 Конвенции МОТ № 185 [3].

Примечание 2 — Подробное содержание базы данных описывается в других статьях Конвенции МОТ № 185 [3], однако для целей настоящего стандарта оно представлено в 6.5.4.

Примечание 3 — Обычно существует отдельная база данных системы выдачи УЛМ, используемая для записи демографических данных и выдачи УЛМ, однако это не регламентируется ни в Конвенции МОТ № 185 [3], ни в настоящем стандарте.

6.2.6 Ограничения содержания базы данных

Информация, содержащаяся в данной базе данных, ограничивается лишь теми сведениями, которые необходимы для проверки УЛМ или статуса моряка при полном соблюдении права моряков на конфиденциальность своих персональных данных и удовлетворении всех действующих требований в отношении защиты данных.

Примечание — Данное требование исходит из статьи 4 пункта 2 Конвенции МОТ № 185 [3].

6.2.7 Доступ к базе данных

Каждое государство — член МОТ назначает постоянно действующий координационный центр, имеющий целью удовлетворять запросы, поступающие от иммиграционных служб или других компетентных органов всех государств — членов МОТ, относительно подлинности и действительности УЛМ, выданных его органом. Подробные сведения о постоянно действующем координационном центре направляются в Международное бюро труда, которое ведет список, передаваемый всем государствам — членам МОТ.

К сведениям, указанным в 6.2.5, обеспечивается постоянный и незамедлительный доступ для иммиграционных служб или других компетентных органов в государствах — членах МОТ с помощью электронных средств или через координационный центр, предусмотренный в 6.2.5.

Примечание — Данное требование исходит из статьи 4 пунктов 4 и 5 Конвенции МОТ № 185 [3].

6.2.8 Защита и конфиденциальность данных

Для целей Конвенции МОТ №185 вводятся надлежащие ограничения для того, чтобы исключить какой-либо обмен данными — в частности фотографиями — без наличия механизма, обеспечивающего соблюдение соответствующих норм, касающихся защиты данных и частной жизни.

Государства — члены МОТ обеспечивают, чтобы содержащиеся в электронной базе данных персональные данные использовались только для проверки УЛМ.

Примечание — Данное требование исходит из статьи 4 пунктов 6 и 7 Конвенции МОТ № 185 [3].

6.3 Подходящие биометрические модальности

Хотя для использования моряками подходят многие биометрические модальности, существующей практикой разрешено использование двух отпечатков пальцев, предпочтительно по одному с каждой руки. Эти отпечатки пальцев хранятся в одном шаблоне с двумя представлениями отпечатков пальцев, формат которого соответствует обычному формату карты (включая заголовок записи), определенному в ИСО/МЭК 19794-2 и подробно описанному в стандарте ILO SID-0002 [4]. С целью обеспечения обратной совместимости любые другие модальности должны использоваться в дополнение к шаблонам отпечатков пальцев на основе контрольных точек.

Так как на практике на УЛМ обычно печатается фотография моряка, то для большинства моряков, как правило, регистрируются как отпечатки пальцев, так и изображения лица. Все приложения биометрической верификации и идентификации, которые соответствуют настоящему стандарту, должны использовать отпечаток пальца как обязательную биометрическую модальность, а изображение лица — как необязательную дополнительную.

6.4 Эксплуатационные характеристики

МОТ определила эксплуатационные характеристики, предполагаемые достаточными для верификации моряков в портах и на судах. Однако не определены эксплуатационные характеристики для идентификации моряков, которые могут зависеть от проверок анкетных данных или проверок дублирования документа, когда моряк регистрируется в одной из электронных баз данных, описанных в 6.2.5, и уже имеет УЛМ. С учетом зависимости эксплуатационных характеристик идентификации от качества входных биометрических данных и отсутствия детализированных стандартов методологии тестирования производительности простейшим решением является принять существующие установленные МОТ эксплуатационные характеристики как минимальные.

Биометрические системы, проводящие биометрическую регистрацию или верификацию моряков согласно настоящему стандарту, должны быть способны демонстрировать определенные количественные эксплуатационные характеристики разнородной биометрической системы (в соответствии с ИСО/МЭК 19795-4), измеряемые обобщенной вероятностью ложного допуска при выполнении транзакции (GFAR) и обобщенной вероятностью ложного недопуска при выполнении транзакции (GFRR). А именно: средний GFRR разнородной биометрической системы при GFAR, равном 1 %, должен быть менее 1 % для всех систем в разнородной группе; максимальный GFRR при GFAR, равном 1 %, должен быть менее 2 % для любых комбинаций систем регистрации и верификации. Разнородные группы могут быть определены как системы, включающие в себя только регистрацию или только верификацию, либо оба этапа сразу.

Любые тесты, предназначенные для определения, удовлетворяют ли биометрические системы пороговым значениям эксплуатационных характеристик разнородной биометрической системы, и соответствующие настоящему стандарту, должны удовлетворять требованиям ИСО/МЭК 19795-4.

6.5 Форматы хранения данных и носители информации

6.5.1 Общие положения

Вопросы конфиденциальности при хранении изображений отпечатков пальцев могут препятствовать внедрению систем, основанных на изображениях отпечатков пальцев. Кроме того, при использовании изображений отпечатков пальцев возрастает себестоимость УЛМ ввиду хранения большего количества данных.

По указанным причинам формат хранения отпечатков пальцев в УЛМ должен соответствовать ИСО/МЭК 19794-2.

Вопросы конфиденциальности не должны возникать при использовании изображений лица, так как на практике на УЛМ обычно печатается фотография моряка. Поэтому формат хранения изображений лица должен соответствовать ИСО/МЭК 19794-5.

Хотя все УЛМ, созданные до публикации настоящего стандарта, основаны на более ранних документах МОТ и используют формат записи контрольных точек отпечатка пальца в соответствии с предыдущей версией ИСО/МЭК 19794-2 и стандартом ILO SID-0002 [4], в будущем программные анализаторы должны быть способны по байтам заголовка определять, является ли запись записью старого образца или нового образца, и интерпретировать оставшуюся часть записи должным образом. Ввиду обратной совместимости настоящий стандарт не может быть ограничен использованием последних версий форматов данных, и все системы и документы для выдачи УЛМ, претендующие на соответствие настоящему стандарту, должны использовать только версии форматов данных, представленные в А.6 (приложение А). Единственные ограничения должны быть введены в отношении объема памяти носителей информации, используемых для хранения данных, и возможности достижения эксплуатационных характеристик разнородной биометрической системы, описанных в 6.4. Рекомендуется, но не требуется, чтобы системы верификации, соответствующие настоящему стандарту, поддерживали биометрическое сравнение с использованием устаревшего формата отпечатков пальцев на основе контрольных точек, описанного в стандарте ILO SID-0002 [4].

Биометрические данные, используемые для верификации и идентификации моряков в контексте настоящего стандарта, должны храниться в защищенной электронной базе данных (как описано в 6.2.5) и на УЛМ. На всех УЛМ, соответствующих Конвенции МОТ № 185, для хранения записи контрольных точек двух отпечатков пальцев по ИСО/МЭК 19794-2 используется штрихкод PDF417, и, следовательно, все УЛМ, соответствующие настоящему стандарту, должны включать такой штрихкод, определенный в соответствии с ИСО/МЭК 15438.

6.5.2 Двумерный штрихкод

Для того, чтобы штрихкод был разборчивым, он должен быть напечатан большим настолько, насколько это позволяет отведенная область документа. Допустимая область определяется макетом карт размером ID-1 в соответствии с ИСО/МЭК 7501-3 (для УЛМ, являющихся картами) и макетом страницы данных паспорта в соответствии с ИСО/МЭК 7501-1 (для УЛМ, являющихся буклетом размером ID-3). Пространство для дополнительных печатных полей определяется после того, как напечатаны все обязательные поля, такие как фотография моряка и машиносчитываемая зона документа. Конкретное расположение двумерного штрихкода зависит от размера документа.

Для буклетов размером ID-3 штрихкод должен располагаться непосредственно справа от печатной фотографии моряка (зоны V по ИСО/МЭК 7501-1) и непосредственно над машиносчитываемой зоной (зоной VII по ИСО/МЭК 7501-1). В целях экономии пространства для других необходимых элементов данных отведенная область для двумерного штрихкода с необходимыми свободными зонами должна быть не более 21,35 мм в высоту и должна быть не ближе, чем на 23,2 мм, к нижней границе документа, поскольку нижние 23,2 мм выделяются для машиносчитываемой зоны. Штрихкод также должен быть ограничен по ширине границей печатной фотографии (зоной V) с левой стороны и непечатаемой областью 2 мм у границы документа с правой стороны. Определить точную ширину штрихкода невозможно, так как в соответствии с ИСО/МЭК 7501-1 ширина фотографии является относительно гибкой величиной.

Для карт размером ID-1 штрихкод должен быть напечатан на обратной стороне карты относительно печатной фотографии, в верхней части стороны карты при расположении машиносчитываемой зоны внизу. Максимальный размер двумерного штрихкода с необходимыми свободными зонами должен составлять 85,6 мм в ширину и 27,8 мм в высоту, поскольку согласно ИСО/МЭК 7501-3 двумерный штрихкод должен быть полностью напечатан в зоне VI.

Чтобы обеспечить хранение контрольных точек отпечатков пальцев в ограниченном объеме двумерного штрихкода, в штрихкоде должен храниться только шаблон, включающий в себя запись контрольных точек двух отпечатков пальцев в формате типа 3 ЕСФОБД или в формате типа 4 ЕСФОБД, как определено в ИСО/МЭК 19794-2 и представлено в А.6.2 (приложение А). Данная запись должна сопровождаться заголовком формата ведущей организации ЕСФОБД, представленным в приложении В, и блоком защиты информации ЕСФОБД, представленным в приложении С. Использование формата ведущей организации ЕСФОБД и блока защиты информации ЕСФОБД описано в А.6.4.

Данные, содержащиеся в двумерном штрихкоде, должны быть зашифрованы и распечатаны с использованием спецификации символики PDF417, определенной в ИСО/МЭК 15438. Точный размер символов данных штрихкодов, а также количество строк и столбцов должны определяться компетентным органом изготовления документов в зависимости от размера документа и используемых технологий печати. Единственными обязательными требованиями являются использование уровня коррекции ошибок, равного 5, и то, что штрихкод должен быть читаемым коммерческими портативными считыва-

телями штрихкодов. Одним из рекомендуемых вариантов является использование символов штрихкодов размером *X*, равным 0,170 мм, и размером *Y*, равным 0,511 мм.

6.5.3 Бесконтактная интегральная схема

Если УЛМ содержит бесконтактную интегральную схему, то должны быть соблюдены положения по 6.2. В частности, в бесконтактной интегральной схеме не должно содержаться никакой другой информации о моряке, кроме перечисленной в 6.2.2 и 6.2.3, и эта информация должна быть видна на документе (например, фотография, напечатанные персональные данные или отпечатки пальцев, зашифрованные в штрихкоде на УЛМ). Однако емкость бесконтактной интегральной схемы не ограничена пределами емкости штрихкода, и существует больше возможностей в использовании конкретных типов форматов ЕСФОБД.

Интегральная схема должна содержать данные отпечатков пальцев, состоящие из записи контрольных точек двух отпечатков пальцев формата ЕСФОБД типа 3 или 4, как определено в ИСО/МЭК 19794-2 и указано в А.6.2 (приложение А). Интегральная схема должна также содержать данные изображения лица, представляющие цифровое представление фотографии, напечатанной на документе, которые хранятся в записи формата ИСО/МЭК 19794-5, как указано в А.6.3 (приложение А). Запись контрольных точек отпечатков пальцев должна быть упакована в запись данных ЕСФОБД, определенную в приложении В и указанную в А.6.4 (приложение А). Как и в случае двумерного штрихкода, обязательно наличие блока защиты информации и цифровой подписи биометрических данных с использованием метода, описанного в 6.6.

Данные изображения отпечатка пальца, как определено в ИСО/МЭК 19794-4 и указано в А.6.1 (приложение А), не должны храниться в бесконтактной интегральной схеме, и их использование ограничивается защищенными электронными базами данных государств — членов МОТ.

Поскольку использование бесконтактной интегральной схемы является опциональным и необязательным, в настоящем стандарте не приводится точная спецификация блоков данных, хранимых на чипе ИС. При наличии чипа рекомендуется следовать спецификации для электронных паспортов, содержащих данные изображения лица и контрольных точек отпечатка пальца. Ожидается, что МОТ будет проводить обсуждения по данному вопросу и опубликует дополнительную документацию по спецификации после консультации с другими заинтересованными органами, такими как Международная организация гражданской авиации. Обсуждение данного вопроса выходит за рамки настоящего стандарта.

6.5.4 Защищенная электронная база данных

В защищенной электронной базе данных каждого государства — члена МОТ должны храниться ключевые данные (см. таблицу 1) по каждому УЛМ, выданному этим государством. База данных должна быть доступной согласно 6.2.7 для компетентных органов проверки УЛМ, которым по какой-либо причине необходимо сделать запрос по конкретным УЛМ или конкретным морякам. Защищенная электронная база данных необходима для ведения учета выданных, приостановленных или изъятых документов, а также для сохранения достаточной информации для проведения проверки отдельных УЛМ или статусов моряков. Доступ к этой информации должен предоставляться компетентным органам проверки УЛМ, прошедшим проверку подлинности, при условии, что органы проверки УЛМ защищены от случайного раскрытия информации или раскрытия информации из-за использования открытого канала. Методы защиты информации для обозначенных ситуаций изложены в разделе 6. Защищенная электронная база данных должна сохранять все запросы по проверкам записей УЛМ в системный журнал. Рекомендуется, чтобы системные журналы хранились не менее десяти лет в зависимости от национальных законодательных требований.

Скорее всего, любая система изготовления и выдачи УЛМ будет иметь большую базу данных, содержащую полную информацию о каждом моряке, каждом выданном документе, все данные, используемые в процессе изготовления документа, и системный журнал всех действий, предпринятых в отношении каждого моряка и документа. Такие базы данных, как правило, являются фирменными решениями, которые зависят от конкретного программного обеспечения и процедур, используемых органами выдачи УЛМ. Они также могут зависеть от отдельных законодательных требований в таких вопросах, как регистрировать ли у моряков полный набор десяти отпечатков пальцев для проверки безопасности во время процесса регистрации, и если да, то сохранять или удалять ли эти изображения отпечатков пальцев после завершения проверки безопасности.

Защищенная электронная база данных согласно настоящему стандарту должна быть отделена от любой фирменной базы данных системы выдачи документов (отделение может быть физическим или электронным). База данных должна содержать для каждого УЛМ данные, определенные в настоящем

разделе и которые считаются достаточными для обеспечения проведения проверки УЛМ и моряков. Элементы данных перечислены в таблице 1 с указанием того, являются ли они обязательными или необязательными, а также с хронологической пометкой: присутствуют ли они в официальных электронных базах УЛМ, которые основаны на технических документах МОТ, опубликованных до публикации настоящего стандарта.

Таблица 1 — Элементы данных в защищенной электронной базе данных

№	Элемент данных	Описание данных	Обязательный или необязательный	Наличие в официальных электронных базах УЛМ
1	Орган выдачи, указанный на УЛМ	Текстовая строка переменной длины, содержащая код ИСО государства выдачи из трех символов (см. ИСО/МЭК 7501-1), название и полный адрес организации, выдавшей УЛМ, а также имя и должность лица, разрешающего выдачу УЛМ	Обязательный	Да
2	Полное имя моряка, как указано на УЛМ	Текстовая строка переменной длины, содержащая полное имя моряка	Обязательный	Да
3	Уникальный номер УЛМ	12-символьная текстовая строка, содержащая код ИСО государства выдачи из трех символов (см. ИСО/МЭК 7501-1) и 9-символьный номер УЛМ, уникальный среди всех УЛМ, выданных в данном государстве	Обязательный	Да
4	Дата окончания срока действия, приостановления или изъятия документа	10-символьная текстовая строка (с кодировкой ASCII), содержащая дату окончания срока действия/приостановления/изъятия документа в формате дд/мм/гг	Обязательный	Да
5	Статус даты документа	1-символьная текстовая строка (с кодировкой ASCII), кодирующая смысловое значение поля даты, записанной в элементе 4. Допустимые значения: D — дата является датой окончания срока действия документа, S — дата является датой приостановления документа, W — дата является датой изъятия документа	Обязательный	Да
6	Шаблон отпечатка пальца, представленный на УЛМ	Бинарная запись переменной длины контрольных точек двух отпечатков пальцев по ИСО/МЭК 19794-2, упакованная в запись ЕСФОБД с блоком защиты информации, в точности соответствующая двумерному штрихкоду на УЛМ, как описано в 6.5.2	Обязательный (если это не запрещено законодательными требованиями)	Да Может быть в формате ИСО/МЭК 19794-2, указанном в стандарте ILO SID-0002 [4]
7	Изображение лица, представленное на УЛМ	Бинарная строка переменной длины, содержащая изображение лица, идентичное напечатанной на УЛМ фотографии, хранимое в записи изображения лица по ИСО/МЭК 19794-5, как определено в А.6.3 (приложение А), и дополненное заголовком ЕСФОБД и блоком защиты информации ЕСФОБД, как определено в А.6.4 (приложение А)	Обязательный	Да Может быть простым изображением не в формате ИСО/МЭК 19794-5

Окончание таблицы 1

№	Элемент данных	Описание данных	Обязательный или необязательный	Наличие в официальных электронных базах УЛМ
8	Изображения отпечатков пальцев, относящиеся к записи контрольных точек двух отпечатков пальцев, хранимой на УЛМ	Бинарная строка переменной длины, содержащая изображения двух отпечатков пальцев, которые относятся к записи контрольных точек двух отпечатков пальцев, закодированной в двумерном штрихкоде на УЛМ. Данные изображения должны быть закодированы в одну запись изображений отпечатков пальцев по ИСО/МЭК 19794-4, как определено в А.6.1 (приложение А)	Необязательный	Нет
9	Подробная информация обо всех запросах по УЛМ	Внутренние системные журналы базы данных, записывающие проверку на подлинность органа проверки УЛМ, осуществляющего запрос, детали, используемые для проверки органа проверки полномочия, дату и время запроса и уникальный номер документа УЛМ, по которому сделан запрос. Для записи данной информации используется внутренний формат каждого органа выдачи УЛМ, так как эта информация предназначена не для обмена, а для обеспечения аудиторских отчетов для органов выдачи УЛМ и для запросов моряков по своим личным УЛМ	Обязательный	Да

В целях обеспечения конфиденциальности и безопасности данных указанные элементы данных должны быть защищены и не распространяться, кроме органов проверки УЛМ, прошедших проверку с использованием процедур, описанных в 6.8.

6.6 Требования безопасности

6.6.1 Общие положения

Есть три основные проблемы безопасности, которые имеют отношение к биометрической верификации и идентификации моряков и которые рассматриваются в настоящем стандарте.

6.6.2 Защита биометрических данных на УЛМ

Данные изображения лица, которые должны храниться на бесконтактной интегральной схеме при ее наличии на УЛМ, аналогичны содержанию информации печатной фотографии. Поэтому криптографической защиты данных не требуется.

Записи контрольных точек отпечатков пальцев, как правило, считаются более уязвимыми, но существующая политика МОТ не требует криптографической защиты записей контрольных точек от считывания в случае, если они не могут быть прочитаны при условии, что карта не предъявлена моряком добровольно.

В случае хранения записи контрольных точек в штрихкоде она будет отсканирована, только если моряк добровольно предъявит документ так, чтобы штрихкод мог быть отсканирован. Только в исключительных случаях, например законной конфискации УЛМ или потери моряком УЛМ, допускается сканирование штрихкода без разрешения моряка.

В случае хранения записи контрольных точек на бесконтактной интегральной схеме (при ее наличии) самым простым решением является использование метода базового контроля доступа (БКД), используемого обычно для электронных паспортов.

Таким образом, биометрические данные, хранимые в УЛМ, не шифруются, но при наличии бесконтактной интегральной схемы доступ к ней должен быть защищен с помощью метода базового контроля доступа, используемого обычно для электронных паспортов.

6.6.3 Проверка подлинности биометрических данных на УЛМ

В целях предотвращения мошенничества необходимо убедиться, что биометрические данные, хранимые на УЛМ, фактически совпадают с биометрическими характеристиками моряка и что создание УЛМ и кодирование данных проведено уполномоченным органом выдачи УЛМ. Одним из способов сделать это являются доступ к защищенной электронной базе данных органа выдачи УЛМ и проверка подлинности УЛМ. Поскольку многие пункты проверки УЛМ могут быть расположены в портах или на судах, где отсутствует коммуникационная инфраструктура для доступа к электронным базам данных всех органов выдачи УЛМ, должен быть метод непосредственной проверки подлинности УЛМ.

Проверка подлинности должна проводиться с использованием цифровой подписи, содержащейся в блоке защиты информации ЕСФОБД. Так как криптографические функции относятся только к цифровой подписи (хеш-шифрование), то нет необходимости скрывать соответствующие ключи, алгоритмы и параметры, используемые для проверки цифровой подписи, однако их источник должен быть проверен. В идеальном случае после получения с УЛМ глобального уникального номера документа необходимые параметры для проверки цифровой подписи (и, следовательно, биометрических данных) могут быть получены в режиме онлайн с использованием защищенной инфраструктуры открытых ключей PKI от доверенной третьей стороны, такой как МОТ.

В случае, когда доступ для получения указанных параметров (и любой информации об аннулировании) в режиме онлайн с использованием защищенной инфраструктуры открытых ключей PKI отсутствует, пункт верификации должен проводить скачивание и сохранение алгоритмов и параметров от доверенной третьей стороны в момент времени, когда доступ в режиме онлайн появляется. Хранимая информация должна обновляться не менее чем 1 раз в месяц.

В машиносчитываемой зоне УЛМ и в блоке защиты информации ЕСФОБД каждой биометрической записи данных, хранимой на документе, находится 12-символьный глобально уникальный номер документа (см. таблицу 1), идентичный хранимому в защищенной электронной базе данных. Загруженная информация должна содержать параметры и открытый ключ, использованные для передачи сообщения и цифровой подписи при производстве УЛМ. Такая информация должна содержаться для каждого органа выдачи УЛМ для каждой группы номеров УЛМ, назначенных тем органом, от которого требуется отдельный открытый ключ. Загруженная информация должна также содержать список уникальных номеров документов любых карт, аннулированных в течение месяца.

Для управления безопасным распространением данной информации необходимо наличие единого главного координационного центра (как это предлагается для проверки в режиме онлайн в 6.8.3) либо использование упрощенной инфраструктуры открытых ключей, такой как Директория открытых ключей ИКАО, используемая для электронных паспортов. Определение механизма управления выходит за рамки настоящего стандарта, но сведения, представленные в настоящем пункте, имеют важное значение для успешного функционирования такой системы.

Примечание — Данные параметры не должны храниться втайне, но они должны быть получены из надежного источника, в противном случае пункт проверки не сможет обнаружить сфальсифицированные карты с помощью параметров и открытого ключа, полученного от органа выдачи сфальсифицированной карты. Таким образом, любой загружаемый список, хранимый в пункте проверки УЛМ, должен быть защищен от несанкционированного доступа (физическими методами).

6.6.4 Безопасность защищенной электронной базы данных

Для защиты данных, содержащихся в защищенной электронной базе данных, важно, чтобы использовались передовые технологии ИТ-безопасности. Обсуждение данного вопроса выходит за рамки настоящего стандарта, но включает в себя такие вопросы, как предоставление доступа к базе данных только уполномоченному персоналу, запись в системные журналы всех запросов доступа и изменений базы данных и обеспечение регулярного контроля этих системных журналов. Доступ к базе данных должен предоставляться органам проверки УЛМ только с помощью процедур, описанных в 6.8, и любые данные должны передаваться только прошедшим проверку подлинности органам проверки УЛМ и быть защищены во время передачи.

6.6.5 Общие требования безопасности

Существуют многочисленные требования безопасности, являющиеся общими для всех биометрических приложений, и они должны соблюдаться в биометрической верификации и идентификации моряков. Нецелесообразно повторять все требования в настоящем стандарте, но для эффективного использования настоящего стандарта перечислены некоторые основные положения.

Используемые биометрические устройства регистрации должны быть устойчивы к суровым условиям окружающей среды (включая соленые брызги), функционировать в портах и на судах и в то же время обладать достаточным разрешением для предотвращения подмены.

Верификация моряков должна включать в себя этап проверки подлинности УЛМ по защищенной электронной базе данных или путем проверки цифровой подписи в блоке защиты информации ЕСФОБД.

Биометрические системы регистрации и верификации должны быть сконструированы таким образом, чтобы было трудно внедрить данные в систему или удалить данные из системы через незаконные каналы. Это позволит защитить целостность процесса выдачи и защитить системы верификации от атак повторного воспроизведения и атак типа «злоумышленник в середине».

После того как компонент системы регистрации или верификации завершил свою функцию, использованные данным компонентом данные не должны быть доступны в этом компоненте. Например, биометрические устройства регистрации должны очистить свою память после получения последовательности биометрических данных, и компоненты сравнения и сопоставления должны удалить биометрические данные из памяти после вычисления показателя сравнения и принятия решения.

В данном пункте перечислены только некоторые передовые методы общей информационной безопасности. Рекомендуется следовать методам, подробно описанным в [5], [6] и [7], где это применимо, и при условии, что они не противоречат ни одному из конкретных требований настоящего стандарта.

6.7 Процедуры биометрической регистрации

Каждый орган выдачи УЛМ должен проверить правомочность индивида на получение УЛМ. Это может быть проверка того, что физическое лицо является квалифицированным моряком, по национальным учебным записям, трудовым книжкам или другим источникам. Это также может быть проверка личности и гражданства моряка по документам, удостоверяющим личность, и существующим национальным базам данных. Эти процессы могут меняться в разных органах выдачи УЛМ, так как предоставляемые документы и базы данных различны в разных странах, так же как нормативные требования.

Определенные процедуры в процессе УЛМ обязательны для всех органов выдачи УЛМ. В частности, орган выдачи УЛМ должен зарегистрировать демографические и биометрические данные моряка и ввести их в систему выдачи, чтобы они стали частью защищенной электронной базы данных и были включены в УЛМ, если удостоверение выдается моряку. Записываемых демографических данных должно быть достаточно для изготовления УЛМ, в том числе машиносчитываемой зоны, соответствующей ИСО/МЭК 7501-3. Как минимум, записываемые демографические данные должны включать следующее:

a) первичная идентификация — основное имя моряка;

b) вторичная идентификация — второе имя моряка;

c) национальность — трехсимвольный код страны, представляющий гражданство моряка (см. ИСО/МЭК 7501-1);

d) место рождения — место рождения моряка;

e) дата рождения — дата рождения моряка, записанная в соответствии с григорианским календарем в формате «год, месяц и день»;

f) пол — пол моряка.

Биометрические данные моряка должны быть получены в процессе регистрации в рамках общего процесса выдачи и изготовления УЛМ.

Биометрическая регистрация должна включать в себя регистрацию изображения лица, которое соответствует полному фронтальному типу изображения лица согласно ИСО/МЭК 19794-5, и кодирование изображения в запись по ИСО/МЭК 19794-5, как определено в 6.5.3 и 6.5.4. Биометрическая регистрация также должна включать в себя регистрацию по крайней мере двух отпечатков пальцев, которые опционально могут быть сохранены в защищенной электронной базе данных как запись изображения отпечатка пальца по ИСО/МЭК 19794-4 и на которых должны быть определены контрольные точки для создания записи контрольных точек отпечатка пальца по ИСО/МЭК 19794-2. Запись по ИСО/МЭК 19794-2 в обязательном порядке должна храниться в защищенной базе данных УЛМ (если это не запрещено законодательными требованиями) и на УЛМ.

При регистрации биометрических характеристик лица и отпечатков пальцев орган выдачи УЛМ (или его пункт регистрации) должен уделять особое внимание получению изображений высокого ка-

чества для содействия органам проверки УЛМ (см. 6.8). Регистрация изображения отпечатка пальца плохого качества может привести к множеству контрольных точек пальца, которое невозможно будет успешно сравнить с множеством контрольных точек, полученным при обработке изображений отпечатков пальца во время верификации. Органы выдачи УЛМ могут обратиться к поставщикам оборудования биометрической регистрации за учебными материалами по съемке изображений максимально высокого качества. Примеры того, что необходимо учитывать во время регистрации отпечатков пальцев:

- контроль уровней температуры, влажности и освещения окружающей среды, при которых проводится биометрическая регистрация, в соответствии с рекомендациями изготовителя оборудования;
- позиционирование датчика отпечатков пальцев на оптимальной высоте и при оптимальном угле наклона;
- контроль и реагирование на повышенную влажность или сухость пальца моряка;
- взаимодействие с моряком по правильному расположению плоской части пальца (вместо кончика пальца) в контакте с поверхностью с достаточным давлением;
- проверка того, что палец моряка не повернут слишком сильно на поверхности датчика.

Должны быть разработаны процедуры контроля качества для оценки соответствия качества изображений, регистрируемых отдельными сотрудниками регистрации (и отдельными пунктами, если в органе выдачи УЛМ имеется более одного пункта регистрации), высокому уровню. Периодические отчеты должны оценивать это соответствие и давать рекомендации, если существуют способы получать изображения отпечатков пальцев более высокого качества.

Какие именно два пальца будут зарегистрированы, определяется в момент регистрации при проведении попыток зарегистрировать пальцы в порядке, описанном далее. Если палец не может быть зарегистрирован из-за плохого качества получаемого изображения или если это невозможно в принципе (вследствие инвалидности или повреждения пальца), то регистрируется следующий палец по списку.

В записи контрольных точек двух отпечатков пальцев, хранящейся в базе данных и на УЛМ, первый относится к первому пальцу из списка, который удалось успешно зарегистрировать, а второй — ко второму из списка, который удалось успешно зарегистрировать.

Рекомендуется использовать три попытки регистрации пальца. Если во всех трех попытках получено изображение неудовлетворительного качества, то необходимо перейти к регистрации следующего пальца. До завершения процесса регистрации также рекомендуется провести пробную верификацию обоих выбранных пальцев и в случае неудачной верификации продолжить регистрацию других пальцев из списка:

a) указательный палец правой руки;
b) указательный палец левой руки;
c) большой палец правой руки;
d) большой палец левой руки;
e) средний палец правой руки;
f) средний палец левой руки;
g) безымянный палец правой руки;
h) безымянный палец левой руки;
i) мизинец правой руки;
j) мизинец левой руки.

Биометрические системы не являются абсолютно точными и подходящими для всех людей. В частности, люди с нечитаемыми отпечатками пальцев, так же как и другие, имеют право на уважение и безопасность. Поэтому должен быть предусмотрен запасной вариант для тех, у кого не получилось зарегистрировать любые два пальца из вышеприведенного списка. Решением является создание представления пальца, являющегося изображением пальца, который не получается зарегистрировать. В случае, если возможна регистрация только одного пальца из вышеприведенного списка, то данный палец должен быть закодирован в первом представлении записи контрольных точек двух отпечатков пальцев, а второе представление должно быть закодировано по шаблону, описанному в приложении А, с фиксированными значениями некоторых элементов из таблицы 2. Если не может быть зарегистрирован ни один отпечаток пальца, то оба представления отпечатка пальца в записи формата ИСО/МЭК 19794-2 должны быть закодированы по шаблону, описанному в приложении А, с фиксированными значениями некоторых элементов из таблицы 2. Это позволяет моряку, чьи отпечатки пальцев не удается зарегистрировать, получить действительное УЛМ с цифровой подписью. Когда пункты проверки УЛМ работают с такими УЛМ, необходимо знать, что данный способ выбран по уважительной причине. В этом случае для верификации моряка может быть использована защищенная электронная

база данных органа выдачи соответствующего УЛМ, хотя для этого потребуется, чтобы пункт проверки УЛМ имел доступ в режиме онлайн.

Разумеется, у большинства моряков не будет проблем с регистрацией правого и левого указательных пальцев; и орган выдачи УЛМ может, в зависимости от местного законодательства и практик, регистрировать отпечатки всех пальцев, чтобы провести идентификационные проверки по биометрическим базам лиц, разыскиваемых компетентными органами, или чтобы предотвратить повторную выдачу УЛМ моряку, у которого уже есть действительное удостоверение. Как описано в 6.5.4, любые дополнительные отпечатки пальцев, не входящие в число первых двух успешно зарегистрированных из вышеприведенного списка, не должны храниться в защищенной электронной базе данных.

Таблица 2 — Характеристики пальца, отпечаток незарегистрированного пальца

№	Элемент данных	Статус	Оператор	Операнд
12	Наименование пальца	M	EQ	0
13	Номер представления пальца	M	EQ	0
14	Тип отпечатка пальца	M	EQ	0, 1, 8
15	Качество изображения отпечатка пальца	M	EQ	0x65 — если отпечаток пальца не может быть зарегистрирован из-за физических ограничений моряка; 0x66 — если отпечаток пальца не может быть зарегистрирован из-за плохого качества
16	Число контрольных точек отпечатка пальца	M	EQ	0

6.8 Процедуры биометрической верификации

6.8.1 Общие положения

Органы проверки УЛМ могут проводить биометрическую верификацию моряков в портах, на борту судов до прибытия судна в порт и на других пунктах пересечения границы, где моряки могут присоединяться транзитом или покидать свои корабли.

В некоторых случаях органы проверки УЛМ имеют электронный доступ к защищенной электронной базе данных органа выдачи УЛМ моряка, чья верификация проводится. В других случаях доступ в режиме онлайн отсутствует. Поэтому процедура биометрической верификации предписывает сначала использовать процедуру в режиме офлайн[1)], в которой для биометрической верификации моряка используются данные на УЛМ и кэшированные данные. Там, где это удобно или необходима дополнительная аутентификация моряка, могут также использоваться процедуры в режиме онлайн.

Все системы верификации УЛМ, соответствующие настоящему стандарту, должны поддерживать процедуру биометрической верификации в режиме офлайн, описанную в 6.8.2. Системы могут опционально поддерживать процедуру биометрической верификации в режиме онлайн, описанную в 6.8.3. Все защищенные электронные базы данных, соответствующие настоящему стандарту, должны поддерживать процедуру биометрической верификации в режиме онлайн, описанную в 6.8.3, так как возможны ситуации, когда системы верификации с поддержкой процедуры биометрической верификации в режиме онлайн будут обращаться к ним из любых определенных государств с запросами о моряках. Опционально может поддерживаться ручная резервная процедура для особых обстоятельств, когда отсутствует подключение к сети Интернет. Для такой процедуры в двусторонних договоренностях между органом проверки УЛМ и органом выдачи УЛМ обязательно должен быть оговорен вопрос, что координационный центр органа выдачи УЛМ может должным образом проверять подлинность органа проверки УЛМ до предоставления информации о любых моряках из своей защищенной электронной базы данных. Такие двусторонние договоренности не рассматриваются в настоящем стандарте.

6.8.2 Процедура биометрической верификации в режиме офлайн

Любая система биометрической верификации моряков, соответствующая настоящему стандарту, должна использоваться под контролем и поддерживать функции, перечисленные ниже.

[1)] Офлайн — осуществляемый в автономном режиме работы.

a) Считывание штрихкода PDF417 (см. ИСО/МЭК 15438), напечатанного на УЛМ (см. 6.5.2), и декодирование записи контрольных точек двух отпечатков пальцев по ИСО/МЭК 19794-2, хранимой в штрихкоде.

b) Проверка подлинности записи отпечатков пальцев по ИСО/МЭК 19794-2 с помощью цифровой подписи записи и отображение результата: может ли быть аутентифицирована подпись. Для этого требуется, чтобы пункт проверки УЛМ имел данные о подлинном открытом ключе органа выдачи УЛМ.

c) Отображение соответствующей информации, если оба пальца в штрихкоде являются незарегистрированными (см. 6.7), чтобы представитель пункта проверки УЛМ мог принять соответствующие меры. В обратном случае необходимо попросить моряка жестами или словами поместить на биометрический сканер отпечатков пальцев первый палец, который хранится в записи контрольных точек отпечатков пальцев по ИСО/МЭК 19794-2 (обычно указательный палец правой руки).

d) Сканирование отпечатка пальца, помещенного на биометрический сканер отпечатков пальцев, и проведение сравнения с первым пальцем записи контрольных точек отпечатков пальцев по ИСО/МЭК 19794-2, извлеченной из штрихкода.

e) При сравнении сканируемого пальца и записи контрольных точек пальца, извлеченной из штрихкода, используется порог, установленный в независимом испытании по достижению эксплуатационных характеристик разнородной биометрической системы, удовлетворяющих требованиям 6.4. Допускается в общей сложности три попытки размещения первого пальца, после этого дается указание поместить второй палец записи по ИСО/МЭК 19794-2. Если второй палец является незарегистрированным (см. 6.7), то такое указание не дается, и информация отображается таким образом, чтобы представитель пункта проверки УЛМ мог принять соответствующие меры.

f) Если три попытки сравнения второго пальца и записи также оказались неуспешными (в общей сложности шесть попыток), то необходимо указать, что биометрическая верификация моряком не пройдена, чтобы представитель пункта проверки УЛМ мог принять соответствующие меры.

g) Если показатель сравнения первого или второго пальца выше порога сравнения на любой попытке размещения, то необходимо отобразить, что биометрическая верификация моряком не пройдена. Далее указания на размещение пальца не даются.

Система биометрической верификации может также поддерживать дополнительные функции в режиме офлайн, перечисленные ниже.

h) Считывание машиносчитываемой зоны (МСЗ) УЛМ и использование этих данных для более быстрого поиска корректного открытого ключа, необходимого для проверки цифровой подписи, заполнения базы данных органа проверки УЛМ или реализации базового контроля доступа к бесконтактной интегральной схеме на УЛМ.

i) Использование метода базового контроля доступа для доступа к чипу ИС на карте при его наличии и считывание записи контрольных точек отпечатков пальцев по ИСО/МЭК 19794-2 и/или записи изображения лица по ИСО/МЭК 19794-5. Запись контрольных точек отпечатков пальцев может быть использована для верификации моряка по отпечаткам пальцев так, как было описано ранее. Запись изображения лица может быть использована для биометрической верификации моряка по изображению лица или для простого визуального отображения в системе проверки.

j) Регистрация изображения лица моряка и сравнение его с записью изображения лица по ИСО/МЭК 19794-5. Количество попыток и эксплуатационные характеристики не установлены в настоящем стандарте, так как верификация по изображению лица не является основным способом биометрической верификации моряков.

k) Если показатель сравнения зарегистрированного изображения лица и записи изображения лица по ИСО/МЭК 19794-5 превышает значение порога, установленного органом проверки УЛМ, то необходимо отобразить, что моряк прошел биометрическую верификацию по изображению лица.

6.8.3 Процедура биометрической верификации в режиме онлайн

Для проведения биометрической верификации в режиме онлайн необходимо, чтобы орган проверки УЛМ имел доступ в Интернет и права удаленного доступа к защищенной электронной базе данных органа выдачи проверяемого УЛМ. Единый всемирный главный координационный центр должен управлять правами доступа всех органов проверки УЛМ и координационных центров органов выдачи УЛМ. Должны быть определены стандартные процедуры выдачи и передачи сертификатов для предоставления органам проверки УЛМ и выдачи необходимого доступа к защищенному серверу, управляемому главным координационным центром, и для предоставления серверу доступа к защищенным электронным базам данных каждого координационного центра.

После того как на сервере главного координационного центра проведена проверка подлинности органа проверки УЛМ, органу проверки УЛМ предоставляется доступ к защищенной веб-странице или другому равнозначному механизму на центральном сервере. На данной веб-странице органы проверки УЛМ могут делать запросы по отдельным УЛМ или по группам УЛМ путем загрузки файлов манифеста с информацией по запрашиваемым УЛМ. Далее главный координационный центр направляет запрос на сервер, подключенный к защищенной электронной базе данных соответствующего координационного центра или координационных центров, и собирает все ответы в одну форму по всем УЛМ в запросе. При отображении результатов должна быть возможность скачать файл с результатами запроса. Поскольку существует несколько типов запросов, как описано далее, орган проверки УЛМ должен указать на защищенной веб-странице главного координационного центра, какой именно тип запроса требуется. Поскольку некоторые элементы данных в защищенной электронной базе данных не являются обязательными, то возможно, что в результатах запроса будут содержаться только обязательные запрашиваемые элементы данных для группы моряков, включенных в файл манифеста. Поэтому структура итогового файла запроса должна быть достаточно гибкой. Кроме того, данные, предоставляемые координационными центрами, могут быть ограничены местными законами о конфиденциальности, поэтому сервер главного координационного центра должен поддерживать разрешения координационных центров, которые указывают, какие необязательные элементы данных, если таковые имеются, будут предоставлены государствам — членам МОТ при запросе.

Различные типы запросов, описанные ниже, предполагают, что орган проверки УЛМ получил информацию по элементам 1—4 из таблицы 1 либо до прибытия моряка (что является требованием Конвенции МОТ № 185), либо непосредственно с УЛМ, представленного моряком по прибытии. Если информация направляется заранее, например при подготовке корабля к постановке в док в первом порту в новой стране, то предоставляемый файл манифеста может содержать информацию обо всех моряках этого судна, и настоятельно рекомендуется, чтобы органы проверки УЛМ требовали направляемую им информацию о прибывающих моряках в том же формате файла манифеста, который будет передаваться далее при подаче запроса. Следовательно, все запросы от органов проверки УЛМ должны содержать информацию по элементам 1—4 таблицы 1. Во всех случаях координационный центр должен предоставить результат проверки, корректны ли четыре элемента данных. Это может быть простой ответ «да» или «нет», но координационный центр может также предоставить корректное значение для каждого из четырех предоставленных элементов и для элемента 5, или отправить сообщение, что не было найдено ни одного совпадающего УЛМ. Так как текстовые строки запроса органа проверки УЛМ могут быть неправильными из-за ошибок сканирования или опечаток, рекомендуется использовать номер УЛМ в качестве первичного ключа, и если это не удается, то проводить поиск по имени моряка и дате срока действия УЛМ.

Дополнительные элементы данных, выходящие за рамки простого ответа и коррекции элементов 1—4, могут включать в себя изображение лица, шаблон отпечатка пальца или изображение отпечатка пальца. Запросы в координационные центры, которые не рассылают отпечатки пальцев моряков и предоставляют службу биометрического сравнения на своем сервере, могут содержать шаблоны отпечатков пальцев. Данный тип запроса может быть осуществлен только в присутствии моряка, так как необходимо приложить пальцы к устройству проверки, чтобы могли быть зарегистрированы отпечатки пальцев, извлечен шаблон контрольных точек по ИСО/МЭК 19794-2 и включен в файл манифеста для загрузки на сервер главного координационного центра. Так как данная процедура достаточно обременительна, она допускается, но не рекомендуется для общего использования. Данная процедура может использоваться для моряков, на УЛМ которых повреждены штрихкоды. Различные типы запросов приведены далее.

1. Орган проверки УЛМ отправляет значения элементов 1—4 из таблицы 1 и получает «да» или «нет» как ответ о достоверности этих данных, корректные значения элементов 1—5 из таблицы 1 или сообщение, что соответствующие УЛМ или моряк не могут быть найдены.

2. Аналогично запросу типа 1, за исключением того, что ответ на запрос также включает в себя элемент 7 из таблицы 1, а именно запись изображения лица по ИСО/МЭК 19794-5, что позволяет провести биометрическую или визуальную проверку моряка как по фотографии на УЛМ, так и по записи в защищенной электронной базе данных их координационного центра.

3. Аналогично запросу типа 1, за исключением того, что ответ на запрос также включает в себя элемент 6 из таблицы 1, а именно запись контрольных точек отпечатков пальцев по ИСО/МЭК 19794-2, что позволяет провести биометрическую проверку моряка по записи в защищенной электронной базе данных их координационного центра.

4. Аналогично запросу типа 1, за исключением того, что ответ на запрос также включает в себя элемент 8 из таблицы 1, а именно запись изображения отпечатка пальца по ИСО/МЭК 19794-4, что позволяет провести биометрическую проверку моряка по записи в защищенной электронной базе данных их координационного центра. Преимуществом использования изображений отпечатков пальцев является то, что они могут использоваться при биометрических проверках программным обеспечением сравнения, которое не поддерживает формат ИСО/МЭК 19794-2, и возможно повышение точности. Недостатком их использования является то, что требуется передавать большие объемы данных, и возможна перегрузка мощностей координационного центра. Кроме того, многие координационные центры могут не поддерживать изображение отпечатка пальца в качестве дополнительного элемента данных в своих защищенных электронных базах данных или не поддерживать такой запрос.

5. Аналогично запросу типа 2, за исключением того, что ответ на запрос также включает в себя элемент 6 из таблицы 1, что позволяет провести биометрическую проверку моряка как по изображению лица, так и по отпечатку пальца.

6. Аналогично запросу типа 2, за исключением того, что ответ на запрос также включает в себя элемент 8 из таблицы 1, что позволяет провести биометрическую проверку моряка как по изображению лица, так и по отпечатку пальца.

7. Аналогично запросу типа 1, за исключением того, что орган проверки УЛМ включает в запрос запись контрольных точек двух отпечатков пальцев по ИСО/МЭК 19794-2 [см. А.6.2 (приложение А)]. Ответ на запрос включает указание, совпадают ли первый и второй пальцы с соответствующими пальцами в элементе 6 для этого УЛМ в защищенной электронной базе данных координационного центра.

Первый тип запроса в приведенном списке должен поддерживаться всеми координационными центрами, которые утверждают соответствие настоящему стандарту, и для всех органов проверки УЛМ, авторизованных через главный координационный центр, должен предоставляться ответ. Все другие типы запросов поддерживаются дополнительно, и каждый координационный центр должен иметь возможность решать, каким государствам — членам МОТ будут предоставляться ответы на запросы типов 2—7. Так как каждый орган проверки УЛМ должен пройти аутентификацию безопасным способом на сервере главного координационного центра, на сервере должна храниться соответствующая информация, в том числе государство — член МОТ, связанное с органом проверки УЛМ, и копия цифрового сертификата, которая включается органом проверки УЛМ в каждый запрос. Это требуется для того, чтобы серверы координационных центров могли заполнить элемент 9 из таблицы 1 и приняли решение, стоит ли отвечать на запросы типов 2—7. В случаях, когда сервер координационного центра не отвечает на запрос, должно быть направлено сообщение о статусе отсутствия ответа, вызвано ли оно отсутствием необходимых данных в защищенной электронной базе данных, таких как дополнительные элементы данных, или ограничением доступа, установленным координационным центром.

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 — СТ (список требований)], которым подвергается статус пунктов в каждой проформе Декларации о соответствии реализации (далее — ДСР), включая последующие изменения требований к ответам, которые необходимо дать.

Ниже приведены используемые обозначения, для которых в базовом стандарте определены 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 ДСР 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

Далее описаны процедуры по заполнению 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 (или наименование параграфа соответствующего базового стандарта), оператора и операнда, определяющих допустимые значения, и ссылку (ссылки) на определенный пункт в базовом стандарте. Существует также столбец статуса, в котором указывается, являются ли значения этого пункта обязательными, необязательными и т. д. В левой части проформы

ДСР указаны требования для каждого элемента в базовом стандарте, а в правой части проформы ДСР указаны требования настоящего профиля.

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 большое количество 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 «x.<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 [ ] (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

В таблицах А.6.1, А.6.2, А.6.3.1 и А.6.4 изложены требования настоящего профиля с соответствующими требованиями базовых стандартов. Пояснения по значениям операторов и операндов и то, как интерпретировать данные требования, можно найти в описании испытаний на соответствие уровня 1 и уровня 2 в ИСО/МЭК 29109-1.

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

Таблица А.6.1 — Данные изображения отпечатка пальца (ИСО/МЭК 19794-4)

СТ базового стандарта						СТ профиля и ДСР			
№	Элемент данных	Оператор	Операнд	Ссылка на базовый стандарт	Статус	Оператор	Операнд	Статус	Поддержка
	Общий заголовок записи								
1	Идентификатор формата	EQ	0x46495200	Таблица 2, пункт 8.2.2	M	EQ	0x46495200	M	
2	Номер версии стандарта	EQ	0x30313000	Таблица 2, пункт 8.2.3	M	EQ	0x30313000	M	
3	Длина записи	EQ	От 47 до 2^{48}	Таблица 2, пункт 8.2.4	M	EQ	От 47 до 2^{48}	M	
4	Идентификатор биометрического сканера отпечатков пальцев	NONE		Таблица 2, пункт 8.2.5	M	NONE		M	
5	Уровень настроек получения изображения	EQ	10, 20, 30, 31, 35, 40, 41	Таблицы 1 и 2, пункт 8.2.6	M	EQ	30, 31, 35, 40, 41	M	
6	Число изображений пальцев/ладоней	EQ	От 1 до 256	Таблица 2, пункт 8.2.7	M	EQ	2	M	
7	Единица измерения разрешения	EQ	От 1 до 2	Таблица 2, пункт 8.2.8	M	EQ	От 1 до 2	M	
8	Разрешение сканирования по горизонтали	EQ	От 49 до 394 п/см/ от 125 до 1000 п/дюйм	Таблицы 1 и 2, пункт 8.2.9	M	EQ	От 197 до 394 п/см/ от 500 до 1000 п/дюйм	M	
9	Разрешение сканирования по вертикали	EQ	От 49 до 394 п/см/ от 125 до 1000 п/дюйм	Таблицы 1 и 2, пункт 8.2.10	M	EQ	От 197 до 394 п/см/ от 500 до 1000 п/дюйм	M	
10	Разрешение изображения по горизонтали	LTE	{Разрешение сканирования по горизонтали}	Таблица 2, пункт 8.2.11	M	LTE	{Разрешение сканирования по горизонтали}	M	
11	Разрешение изображения по вертикали	LTE	{Разрешение сканирования по вертикали}	Таблица 2, пункт 8.2.12	M	LTE	{Разрешение сканирования по вертикали}	M	

Окончание таблицы А.6.1

СТ базового стандарта						СТ профиля и ДСР			
№	Элемент данных	Оператор	Операнд	Ссылка на базовый стандарт	Статус	Оператор	Операнд	Статус	Поддержка
12	Разрядность шкалы градаций серого	EQ	От 1 до 16	Таблицы 1 и 2, пункт 8.2.13	M	EQ	От 1 до 16	M	
13	Алгоритм сжатия изображения	EQ	От 0 до 5	Таблицы 2 и 3, пункт 8.2.14	M	MO	2, 4, 5	M	
14	Зарезервированное поле	EQ	0	Таблица 2, пункт 8.2.15	M	EQ	0	M	
	Заголовок записи пальца								
15	Длина блока данных	EQ	От 15 до 2^{32}	Таблица 4, пункт 8.3.2	M	EQ	От 15 до 2^{32}	M	
16	Наименование пальца/ части ладони	EQ	От 0 до 10, от 13 до 15/от 20 до 36	Таблицы 4, 5 и 6, пункт 8.3.3	M	EQ	От 1 до 10	M	
17	Число представлений	EQ	От 1 до 256	Таблица 4, пункт 8.3.4	M	EQ	От 1 до 256	M	
18	Номер представления	EQ	От 1 до 256	Таблица 4, пункт 8.3.5	M	EQ	От 1 до 256	M	
19	Качество изображения отпечатка пальца/ладони	EQ	–1, –2, от 0 до 100	Таблица 4, пункт 8.3.6	M	EQ	–1, –2, от 0 до 100	M	
20	Тип изображения отпечатка пальца	EQ	От 0 до 3, от 7 до 9	Таблицы 4 и 7, пункт 8.3.7	M	EQ	0, 1, 8, 9	M	
21	Горизонтальный размер изображения	EQ	От 1 до 65535	Таблица 4, пункт 8.3.8	M	EQ	От 1 до 65535	M	
22	Вертикальный размер изображения	EQ	От 1 до 65535	Таблица 4, пункт 8.3.9	M	EQ	От 1 до 65535	M	
23	Зарезервированное поле	EQ	0	Таблица 4, пункт 8.3.10	M	EQ	0	M	
	Данные изображения								

А.6.2 Данные записи контрольных точек отпечатка пальца (ИСО/МЭК 19794-2)

Таблица А.6.2 — Данные записи контрольных точек отпечатка пальца (ИСО/МЭК 19794-2)

СТ базового стандарта						СТ профиля и ДСР			
№	Элемент данных	Оператор	Операнд	Ссылка на базовый стандарт	Статус	Оператор	Операнд	Статус	Поддержка
	Допускаются только тип 3 и тип 4 формата ЕСФОБД								
	Заголовок записи								
1	Идентификатор формата	EQ	0x464D5200	Таблица 7, пункт 7.3.1	M	EQ	0x464D5200	M	
2	Номер версии стандарта	EQ	0x20323000	Таблица 7, пункт 7.3.2	M	EQ	0x20323000	M	
3	Длина записи	EQ	От 24 до 4294967295	Таблица 7, пункт 7.3.3	M	EQ	От 36 до 556	M	
4	Сертификаты сканеров	NONE		Таблица 7, пункт 7.3.4	M	NONE		M	
5	Идентификатор биометрического сканера отпечатков пальцев	NONE		Таблица 7, пункт 7.3.5	M	NONE		M	
6	Размер изображения по горизонтали	NONE		Таблица 7, пункт 7.3.6	M	NONE		M	
7	Размер изображения по вертикали	NONE		Таблица 7, пункт 7.3.7	M	NONE		M	
8	Разрешение изображения по горизонтали	GTE/ EQ/ EQ	98/1000/100	Таблица 7, пункты 6.3.1, 7.3.8, 8.2	M	EQ	1000	M	
9	Разрешение изображения по вертикали	GTE/ EQ/ EQ	98/1000/100	Таблица 7, пункты 6.3.1, 7.3.9, 8.3	M	EQ	1000	M	
10	Число представлений пальцев	EQ	От 0 до 176	Таблица 7, пункты 7.3.10, 7.4.1.2	M	EQ	2	M	
11	Зарезервированное поле	EQ	0	Таблица 7, пункт 7.3.11	M	EQ	0	M	

Окончание таблицы А.6.2

СТ базового стандарта						СТ профиля и ДСР			
№	Элемент данных	Оператор	Операнд	Ссылка на базовый стандарт	Статус	Оператор	Операнд	Статус	Поддержка
	Формат записи отдельного представления пальца								
12	Наименование пальца	EQ	От 0 до 10	Таблицы 2 и 7, пункт 7.4.1.1	M	EQ	От 0 до 10	M	
13	Номер представления пальца	EQ	От 0 до 15	Таблица 7, пункт 7.4.1.2	M	EQ	0	M	
14	Тип изображения отпечатка пальца	MO	0, 1, 2, 3, 8	Таблицы 3 и 7, пункт 7.4.1.3	M	MO	0, 1, 8	M	
15	Качество изображения отпечатка пальца	EQ	От 0 до 100	Таблица 7, пункт 7.4.1.4	M	EQ	От 0 до 102	M	
16	Число контрольных точек отпечатка пальца	EQ	От 1 до 255	Таблица 7, пункт 7.4.1.5	M	EQ	От 0 до 52	M	
	Данные контрольных точек отпечатка пальца								
17	Тип контрольной точки	EQ	От 0 до 2	Таблица 8, пункт 8.2	M	EQ	От 0 до 2	M	
18	Координата *X* контрольной точки	EQ	От 0 до 16383	Таблица 8, пункт 8.2	M	EQ	От 0 до 16383	M	
19	Зарезервированное поле	EQ	0	Таблица 8, пункт 8.2	M	EQ	0	M	
20	Координата *Y* контрольной точки	EQ	От 0 до 16383	Таблица 8, пункт 8.2	M	EQ	От 0 до 16383	M	
21	Ориентация контрольной точки	EQ	От 0 до 255	Таблица 8, пункт 8.2	M	EQ	От 0 до 255	M	
	Дополнительные данные								
22	Длина области дополнительных данных	EQ	0	Таблица 7, пункты 7.5.1.1, А.4	M	EQ	0	M	

А.6.3 Данные изображения лица (ИСО/МЭК 19794-5)

Таблица А.6.3.1 — Данные изображения лица (ИСО/МЭК 19794-5)

СТ базового стандарта						СТ профиля и ДСР			
№	Элемент данных	Оператор	Операнд	Ссылка на базовый стандарт	Статус	Оператор	Операнд	Статус	Поддержка
	Заголовок записи								
1	Идентификатор формата	EQ	0x46414300	Таблица 2, пункт 5.4.1	M	EQ	0x46414300	M	
2	Номер версии стандарта	EQ	0x30313000	Таблица 2, пункт 5.4.2	M	EQ	0x30313000	M	
3	Длина записи	EQ	От 57 до (2^{32} — 1)	Таблица 2, пункт 5.4.3	M	EQ	От 57 до (2^{32} — 1)	M	
4	Число изображений лица	EQ	От 1 до 65535	Таблица 2, пункт 5.4.4	M	EQ	1	M	
	Данные изображения лица								
	Информация								
5	Длина данных записи изображения лица	EQ	От 43 до (2^{32} — 15)	Пункт 5.5.1	M	EQ	От 43 до (2^{32} — 15)	M	
6	Число контрольных точек	EQ	От 0 до 65535	Пункт 5.5.2	M	EQ	От 0 до 65535	M	
7	Пол	EQ	От 0 до 2, 255	Таблица 3, пункт 5.5.3	M	EQ	От 0 до 2, 255	M	
8	Цвет глаз	EQ	От 0 до 7, 255	Таблица 4, пункт 5.5.4	M	EQ	От 0 до 7, 255	M	
9	Цвет волос	EQ	От 0 до 7, 255	Таблица 5, пункт 5.5.5	M	EQ	От 0 до 7, 255	M	
10	Маска свойств	EQ	От 0x00 до 0x7FF	Таблица 6, пункт 5.5.6	M	EQ	От 0x00 до 0x7FF	M	
11	Выражение	EQ	От 0 до 7, от 32768 до 65535	Таблица 7, пункты 5.5.7, 7.2.3	M	EQ	От 0 до 7	M	

Продолжение таблицы А.6 3.1

СТ базового стандарта						СТ профиля и ДСР			
№	Элемент данных	Оператор	Операнд	Ссылка на базовый стандарт	Статус	Оператор	Операнд	Статус	Поддержка
12	Угловая координата — поворот	EQ	От 0 до 181	Пункты 5.5.8.1, 7.2.2	M	MO	0, 1, 2, 3, 179, 180, 181 Соответствует диапазону от минус 5° до плюс 5°	M	
13	Угловая координата — наклон	EQ	От 0 до 181	Пункты 5.5.8.2, 7.2.2	M	EQ	0, 1, 2, 3, 179, 180, 181 Соответствует диапазону от минус 5° до плюс 5°	M	
14	Угловая координата — отклонение	EQ	От 0 до 181	Пункты 5.5.8.3, 7.2.2	M	EQ	От 0 до 5, от 177 до 181 Соответствует диапазону от минус 8° до плюс 8°	M	
15	Погрешность угловой координаты — поворот	EQ	От 0 до 181	Пункт 5.5.9	M	EQ	От 0 до 181	M	
16	Погрешность угловой координаты — наклон	EQ	От 0 до 181	Пункт 5.5.9	M	EQ	От 0 до 181	M	
17	Погрешность угловой координаты — отклонение	EQ	От 0 до 181	Пункт 5.5.9	M	EQ	От 0 до 181	M	
	Контрольная(ые)точка(и)								
18	Тип контрольной точки	EQ	1	Таблица 8, пункт 5.6.1	M	EQ	1	O.1	
19	Код контрольной точки	EQ	См. примечание 1	Таблица 8, рисунки 6 и 7, пункт 5.6.2	M	EQ	См. примечание 1	O.1	
20	Координата *X*	EQ	От 0 до ({Горизонтальный размер изображения} — 1)	Таблица 8	M	EQ	От 0 до ({Горизонтальный размер изображения} — 1)	O.1	

Окончание таблицы А.6.3.1

СТ базового стандарта						СТ профиля и ДСР			
№	Элемент данных	Оператор	Операнд	Ссылка на базовый стандарт	Статус	Оператор	Операнд	Статус	Поддержка
21	Координата Y	EQ	От 0 до ({Вертикальный размер изображения} — 1)	Таблица 8	M	EQ	От 0 до ({Вертикальный размер изображения} — 1)	O.1	
22	Зарезервированное поле	EQ	0	Таблица 8	M	EQ	0	O.1	
	Информация об изображении								
23	Тип изображения лица	EQ	От 0 до 2	Таблица 10, пункт 5.7.1		EQ	1	M	
24	Тип данных изображения	MO	0, 1	Таблица 11, пункт 5.7.2		MO	0, 1	M	
25	Горизонтальный размер изображения	C	См. примечание 2	Пункты 5.7.3, 8.3, 8.4.1, таблица 15		C	См. примечание 2	M	
26	Вертикальный размер изображения	C	См. примечание 2	Пункты 5.7.4, 8.3, 8.4.1, таблица 15		C	См. примечание 2	M	
27	Цветовое пространство	MO	От 0 до 4, от 128 до 255	Таблица 12, пункты 5.7.5, 7.4.2.3		MO	1, 2, 3	M	
28	Тип источника	MO	От 0 до 7, от 128 до 255	Таблица 13, пункт 5.7.6		MO	От 0 до 7, от 128 до 255	M	
29	Тип устройства	EQ	От 0 до 65535	Пункт 5.7.7		EQ	От 0 до 65535	M	
30	Качество	EQ	0	Пункт 5.7.8		EQ	0	M	
	Данные изображения								

Примечание 1 — Значение кода каждой контрольной точки вычисляется по формуле $A \times 16 + B$, где A — основное значение, B — дополнительное значение в таблице А.6.3.2. Это означает, что диапазон значений кодов контрольных точек должен соответствовать указанному в таблице А.6.3.2.

Таблица А.6.3.2 — Допустимый диапазон контрольных точек

Основные значения	Дополнительные значения	Диапазон
2	От 1 до 14	От 33 до 46
3	От 1 до 14	От 49 до 62
4	От 1 до 6	От 65 до 70
5	От 1 до 4	От 81 до 84
6	От 1 до 4	От 97 до 100
7	1	113
8	От 1 до 10	От 129 до 138
9	От 1 до 15	От 145 до 159
10	От 1 до 10	От 161 до 170
11	От 1 до 6	От 177 до 182
12	От 1 до 4	От 193 до 196

Примечание 2 — Соотношения горизонтального размера изображения, вертикального размера изображения, горизонтального размера головы, вертикального размера головы и положения лица определены в пунктах 8.3.1—8.3.6 Изменения № 2 ИСО/МЭК 19794-5.

А.6.4 ИСО/МЭК 19785 (ЕСФОБД)

В приложения В и С включена дополнительная информация о формате ведущей организации ЕСФОБД и блоке защиты информации, представленных в данном разделе. Максимальная длина записи ЕСФОБД, заполненной в соответствии с настоящим пунктом и включающей в себя блок биометрических данных (ББД) из записи контрольных точек двух отпечатков пальцев в соответствии с А.6.2, составляет 635 байтов. Это значение включает в себя 3 байта стандартного биометрического заголовка, максимальные 556 байтов записи контрольных точек двух отпечатков пальцев и 76 байтов блока защиты информации. Ссылки в таблице А.6.4 на базовый стандарт даны на приложения В и С настоящего стандарта, а не на ИСО/МЭК 19785. Пояснения значений различных элементов формата ведущей организации ЕСФОБД можно найти в ИСО/МЭК 19785-1 и ИСО/МЭК 19785-3.

Таблица А.6.4 — ИСО/МЭК 19785 (ЕСФОБД)

СТ базового стандарта						СТ профиля и ДСР			
№	Элемент данных	Оператор	Операнд	Ссылка на базовый стандарт	Статус	Оператор	Операнд	Статус	Поддержка
	Формат ведущей организации ЕСФОБД (приложение В) (стандартный биометрический заголовок)								
1	Владелец формата ББД	EQ	От 0 до 65535	B.10.1	M	EQ	0 (для идентификатора 257 и ведущей организации ИСО/МЭК СТК1/ПК37)	M	1 бит
2	Тип формата ББД	EQ	От 0 до 65535	B.10.1	M	EQ	0b0000011 или 0b0000100	M	7 битов
3	Зарезервированное поле	EQ	0	B.10.1	M	EQ	0b0000	M	4 бита
4	Длина ББД			B.10.1	M	EQ	От 36 до 556	M	12 битов
5	ББД			B.10,1	M			M	
	Блок защиты информации (приложение С)								
6	Орган проверки УЛМ	C	См. примечание 1	C.1	M	EQ	См. примечание 1	M	3 бита
7	Уникальный номер документа	C	См. примечание 2	C.1	M	EQ	См. примечание 2	M	9 битов
8	Подпись	C	См. примечание 3	C.1	M	EQ	См. примечание 3	M	64 бита

Примечание 1 — В трех байтах записывается трехсимвольная строка, которая присутствует в зоне визуальной проверки УЛМ и соответствует коду ИСО государства выдачи документа. Данная строка должна соответствовать напечатанной в зоне визуальной проверки и символам с 3-го по 5-й первой строки машиносчитываемой зоны.

Примечание 2 — В девяти байтах записывается девятисимвольная строка, которая присутствует в зоне визуальной проверки УЛМ как номер УЛМ (не включая три символа кода ИСО государства). Данная строка должна соответствовать напечатанной в зоне визуальной проверки, при этом, если номер УЛМ менее 9 символов в длину, оставшиеся символы должны быть заполнены нулями.

Примечание 3 — Для цифровой подписи должны быть использованы SHA-256 для хэширования и ECDSA для подписывания, как указано в приложении С.

Приложение В
(обязательное)

Формат ведущей организации ЕСФОБД для УЛМ

В.1 Владелец

ИСО/МЭК СТК 1/ПК 37.

В.2 Идентификатор владельца

257 (0x0101). Данный идентификатор присвоен биометрической организации ИСО/МЭК СТК 1/ПК 37 по ИСО/МЭК 19785-2.

В.3 Наименование формата ведущей организации

Формат ведущей организации ИСО/МЭК СТК 1/ПК 37 для УЛМ.

В.4 Идентификатор формата ведущей организации

9 (0x0009). Данный идентификатор присвоен в соответствии с ИСО/МЭК 19785-2.

В.5 Идентификатор объектов АСН.1 для данного формата

{iso registration-authority cbeff(19785) biometric-organization(0) jtc1-sc37(257) patron format(1) sid(9)}
Или значение в нотации XML:
1.1.19785.0.257.1.9

В.6 Область применения

Настоящее приложение определяет минимальный формат ведущей организации для простых структур ББД, разработанных для использования на УЛМ. Формат может быть использован в других областях, в которых необходимо минимизировать стандартный биометрический заголовок (СБЗ) в целях снижения объема памяти или полосы пропускания передачи и снижения затрат на обработку за счет информационного содержания, которые допускают возможную потерю при использовании выравнивания байтов и для которых необходимо значение INTEGRITY при отсутствии ENCRYPTION. Допустимый блок защиты информации ЕСФОБД определен в приложении С.

В.7 Идентификатор версии

Формату ведущей организации присвоен следующий идентификатор версии: основное значение — (0), вспомогательное значение — (0).

В.8 Версия ЕСФОБД

Спецификации формата, определенной в настоящем приложении, присвоена следующая версия: основное значение — (2), вспомогательное значение — (0).

В.9 Общие положения

Настоящее приложение определяет минимально возможный формат ведущей организации. Спецификация формата ведущей организации определена на основе нотации АСН.1 (см. ИСО/МЭК 8824-1) и спецификации правил уплотненного кодирования АСН.1 (ИСО/МЭК 8825-2).

Формат ведущей организации для УЛМ формально определяется путем применения правил уплотненного кодирования без выравнивания PER к типу формата УЛМ, определенному в В.10.1.

Пример кодирования формата ведущей организации с абстрактными значениями, демонстрирующий размер и кодирование каждого поля СБЗ, представлен в таблице В.1. Размер СБЗ должен составлять три байта, если

a) формат ББД стандартизирован ПК37 и значение типа формата менее 64;

b) длина ББД менее 2048 байтов.

Размер СБЗ может быть больше, если данные условия не выполнены.

Примечание — Формат данных, использованный в двумерных штрихкодах на УЛМ и описанный в настоящем стандарте, обеспечивает выполнение данных условий.

Таблица В.1 — СБЗ формата ведущей организации УЛМ (3 байта)

Владельцем формата является ПК37?	Тип формата менее 64?	Значение типа формата	Зарезервированное поле	Длина ББД менее 2048 байтов?	Длина ББД
1 бит 0, если владелец формата — ПК37	1 бит 0, если тип формата менее 64	6 битов Может быть больше, если тип формата ≥ 64 (что невозможно для текущей версии настоящего профиля)	4 бита Дополняет СБЗ до 3 байтов в текущей версии настоящего профиля	1 бит 0, если длина ББД менее 2048 байтов	11 битов Может быть больше, если длина ББД ≥ 2048 байтов (что невозможно для текущей версии настоящего профиля)

В.10 Побитовая спецификация формата ведущей организации

В.10.1 Спецификация

Нотация спецификации определена в ИСО/МЭК 8824-1. Должен быть указан тип данных UNALIGNED версии BASIC-PER (см. ИСО/МЭК 8824-1).

```
CBEFF-SID-PATRON-FORMAT {iso standard 24713 sid (3) modules(0) patron-format(0)}
    -- Значение данного модуля 1.0.24713.3.0.0 для входа в модуль базы данных
DEFINITIONS
AUTOMATIC TAGS ::=
BEGIN
IMPORTS SID-Security-Block FROM SID-SECURITY-BLOCK {iso standard 24713 sid (3)
modules(0) security-block(1)};

SID-format ::= SEQUENCE {
    /* Данный формат ведущей организации содержит только обязательные элементы данных и использует по-
    элементное кодирование для оптимального использования пространства кодирования.*/
    /* Данный формат ведущей организации поддерживает только абстрактные значения lues NO ENCRYPTION
    и INTEGRITY, которые кодируются как поля с нулевой длиной.*/
    /* Данный формат ведущей организации поддерживает только блок защиты информации {iso registration-
    authority cbeff(19785) biometric-organization(0) jtc1-sc37(257) SB-formats(2) sid(3)}, определенный в приложе-
    нии С*/

    bdb-format      SEQUENCE {
                    owner INTEGER (0..65535) DEFAULT 257,
                        -- 257 — идентификатор биометрической организации ИСО/МЭК СТК 1/ПК 37. Для значения
                        257 кодируется в 1 бите.
                    type INTEGER (0..63, .... 64..65535)},
                        -- Кодируется в 7 битах для идентификаторов ЕСФОБД менее 64.
    reserved    BIT STRING (SIZE (4))('0000'B),
                    -- Кодируется в 4 битах, для настоящей версии стандарта все биты имеют нулевое значение.
    sb-format       SEQUENCE {
                    owner INTEGER (257) /*Нулевое кодирование*/,
                    type INTEGER (3) /*Нулевое кодирование*/ },
    bdb         OCTET STRING (SIZE(0..2047, ..., 2048 .. MAX)),
                    -- Кодируется в 12 битах плюс длина ББД.
    sb              SID-Security-Block }
END
```

В.11 Декларация о соответствии формату ведущей организации (ДСФВО)

Информация об элементах данных, определенных ЕСФОБД для ДСФВО формата ведущей организации ЕСФОБД, приведена в таблицах В.11.1—В.11.3.

B.11.1 Информация о формате

Таблица B.11.1 — Информация о формате

Необходимая информация	Ссылка на формат
Наименование ведущей организации	См. B.1
Идентификатор ведущей организации	См. B.2
Наименование формата ведущей организации	См. B.3
Идентификатор ведущей организации	См. B.4
Идентификатор формата ACH.1 ведущей организации	См. B.5
Описание области применения	См. B.6
Версия формата ведущей организации	См. B.7
Версия ЕСФОБД	См. B.8

B.11.2 Элементы данных и абстрактные значения, установленные ЕСФОБД

Таблица B.11.2 — Элементы данных и абстрактные значения, установленные ЕСФОБД

Наименование элемента данных ЕСФОБД	Обязательный/ необязательный	Наименование элемента данных в формате	Определено абстрактное значение ?	Определен способ записи абстрактных значений ?
CBEFF_BDB_format_owner	Обязательный	Владелец	Да	Да
CBEFF_BDB_format_type	Обязательный	Тип	Да	Да
CBEFF_BDB_encryption_options	Обязательный	Поле нулевой длины	Да	Да
CBEFF_BIR_integrity_options	Обязательный	Поле нулевой длины	Да	Да
CBEFF_SB_format_owner	Обязательный	Поле нулевой длины	Да	Да
CBEFF_SB_format_type	Обязательный	Поле нулевой длины	Да	Да

B.11.3 Элементы данных и абстрактные значения, определяемые ведущей организацией ЕСФОБД

Таблица B.11.3 — Элементы данных и абстрактные значения, определяемые ведущей организацией ЕСФОБД

Наименование элемента данных формата ведущей организации	Обязательный/ необязательный	Наименование элемента данных в формате	Определено абстрактное значение ?	Определен способ записи абстрактных значений ?
Нет	N/A	N/A	N/A	N/A

Приложение С
(обязательное)

Блок защиты информации ЕСФОБД для УЛМ

С.1 Общие положения

Блок защиты информации (БЗИ) предназначен для использования в УЛМ, но может быть использован в других документах с ограниченным объемом хранения биометрических данных. Данный блок обеспечивает целостность и аутентификацию источника данных при помощи цифровых подписей. Минимальный размер блока достигается путем использования алгоритма цифровой подписи на эллиптических кривых (Elliptic Curve Digital Signature Standard, ECDSA) и двоичного кодирования полученной подписи и идентификатора алгоритма. БЗИ определяет идентификаторы алгоритмов и правила кодирования цифровых подписей ECDSA при использовании SHA-256 в качестве алгоритма хеширования. Базовыми документами указанных алгоритмов являются публикации Национального института стандартов и технологий (NIST) «Draft Secure Hash Standard» [1] и «Draft Digital Signature Standard» [2] и публикация ANSI X9.62-2005 [8]. БЗИ содержит:

a) три символа ASCII кода ИСО государства выдачи карты (см. ИСО/МЭК 7501-1);

b) девять цифр в кодировке ASCII, идентифицирующие номер документа, который является уникальным среди всех документов, выданных в государстве выдачи.

Примечание — Комбинация элементов a) и b) образует глобально уникальный номер УЛМ, который может быть использован совместно с внеполосным механизмом для поиска всех параметров, в частности открытого ключа органа выдачи УЛМ, необходимого для проверки цифровой подписи в БЗИ. Детали внеполосных механизмов не рассматриваются в настоящем стандарте и определяются отдельными двухсторонними соглашениями между органами проверки и органами выдачи УЛМ, или между органами проверки УЛМ, органами выдачи УЛМ и единым главным координационным центром, управляемым МОТ в соответствии с 6.8.3. Предполагается, что данная информация будет поступать постоянно и будет храниться в хэше в случае необходимости проверки УЛМ в режиме офлайн;

c) цифровая подпись (64 байта).

Цифровая подпись всегда используется совместно с односторонней хэш-функцией. В данном блоке защиты информации ББД ЕСФОБД, который должен быть подписан (СБЗ и ББД), обрабатывается хэш-функцией SHA-256, создавая выходное значение длиной 256 битов (32 байта). Данное значение затем форматируется для подписания алгоритмом ECDSA. При подписании алгоритм ECDSA создает два значения, обычно обозначаемые как *r* и *s*. Для создания значения подписи они объединяются следующим образом:

signature = r, s.

Данное бинарное значение становится значением поля подписи.

Размер каждого компонента подписи (*r* и *s*) равен длине ключа (32 байта или 256 битов).

В итоге SHA-256 с кодированием ECDSA с длиной ключа 256 битов дает размер хэша 32 байта и размер подписи 64 байта.

Более подробная информация по созданию цифровых подписей находится в [2].

С.2 Владелец БЗИ

ИСО/МЭК СТК 1/ПК 37.

С.3 Идентификатор владельца БЗИ

257 (0x0101). Данный идентификатор присвоен биометрической организации ИСО/МЭК СТК 1/ПК 37 по ИСО/МЭК 19785-2.

С.4 Наименование формата БЗИ

Формат блока защиты информации ИСО/МЭК СТК 1/ПК 37 для УЛМ.

С.5 Идентификатор формата БЗИ

3(0x0003). Данный идентификатор присвоен в соответствии с ИСО/МЭК 19785-2.

С.6 Идентификатор объектов ASN.1 для данного формата БЗИ

{iso registration-authority cbeff(19785) biometric-organization(0) jtc1-sc37(257) sbformat(1) sid(3)}

Или значение в нотации XML:

1.1.19785.0.257.1.3

С.7 Идентификатор версии

Формату блока защиты информации присвоен следующий идентификатор версии: основное значение — (0), вспомогательное значение — (0).

С.8 Спецификация БЗИ

Нотация спецификации определена в ИСО/МЭК 8824-1. Должен быть указан тип данных UNALIGNED версии BASIC-PER (см. ИСО/МЭК 8824-1).

```
SID-SECURITY-BLOCK {iso standard 24713 sid (3) modules(0) security-block(1)}
-- Значение данного модуля 24713.3.0.1 для входа в модуль базы данных
DEFINITIONS
AUTOMATIC TAGS ::=
BEGIN
SID-Security-Block ::= SEQUENCE {
        sid-issuing-authority          IA5String (SIZE(3)),
                -- Трехсимвольный код страны органа, выдающего документ, по ИСО/МЭК 7501-1
unique-document-number          IA5String (SIZE(9)),
                -- Уникальный для органа, выдающего документ. Используется для определения параметров алгоритма безопасности внеполосных механизмов
signature-r                                    OCTET STRING (SIZE(32)) ,
signature-s                                    OCTET STRING (SIZE(32))
                -- Содержание подписи определено в С.1 --
}
END
```

С.9 Размер элементов БЗИ

sid-issuing-authority	3 байта
unique-document-number	9 байтов
signature-r	32 байта
signature-s	32 байта

Общий размер составляет 76 байтов.

Элементы sid-issuing-authority и unique-document-number необходимы для восстановления открытого ключа органа выдачи данного УЛМ или, что чаще, группы УЛМ, включающей в себя рассматриваемое УЛМ.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO/IEC 7501-1	IDT	ГОСТ Р ИСО/МЭК 7501-1—2013 «Карты идентификационные. Машиносчитываемые паспортно-визовые документы. Часть 1. Машиносчитываемый паспорт»
ISO/IEC 7501-3	IDT	ГОСТ Р ИСО/МЭК 7501-3—2013 «Карты идентификационные. Машиносчитываемые паспортно-визовые документы. Часть 3. Машиносчитываемые официальные документы»
ISO/IEC 8824-1:2002	IDT	ГОСТ Р ИСО/МЭК 8824-1—2001 «Информационная технология. Абстрактная синтаксическая нотация версии один (АСН.1). Часть 1. Спецификация основной нотации»
ISO/IEC 8825-1:2002	IDT	ГОСТ Р ИСО/МЭК 8825-1—2003 «Информационная технология. Правила кодирования АСН.1. Часть 1. Спецификация базовых (BER), канонических (CER) и отличительных (DER) правил кодирования»
ISO/IEC 8825-2:2002	IDT	ГОСТ Р ИСО/МЭК 8825-2—2003 «Информационная технология. Правила кодирования АСН.1. Часть 2. Спецификация правил уплотненного кодирования (PER)»
ISO/IEC 15438:2006	—	*
ISO/IEC 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»
ISO/IEC 19785-3:2007	—	*
ISO/IEC 19794-2:2005	IDT	ГОСТ Р ИСО/МЭК 19794-2—2013 «Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца — контрольные точки»
ISO/IEC 19794-4:2005	IDT	ГОСТ Р ИСО/МЭК 19794-4—2014 «Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца»
ISO/IEC 19794-5:2005	IDT	ГОСТ Р ИСО/МЭК 19794-5—2013 «Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица»
ISO/IEC 19795-4:2008	IDT	ГОСТ Р ИСО/МЭК 19795-4—2011 «Информационные технологии. Биометрия. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 4. Испытания на совместимость»
ISO/IEC 24713-1:2008	IDT	ГОСТ Р ИСО/МЭК 24713-1—2013 «Информационные технологии. Биометрические профили для взаимодействия и обмена данными. Часть 1. Общая архитектура биометрической системы и биометрические профили»

Окончание таблицы ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO/IEC 29109-1	IDT	ГОСТ Р ИСО/МЭК 29109-1—2012 «Информационные технологии. Биометрия. Методология испытаний на соответствие форматам обмена биометрическими данными, определенным в комплексе стандартов ИСО/МЭК 19794. Часть 1. Обобщенная методология испытаний на соответствие»

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

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

- IDT — идентичные стандарты.

Библиография

[1] FIPS 180-3 — Federal Information Processing Standard «Draft Secure Hash Standard» (draft) [Федеральный стандарт обработки информации «Безопасное хэширование» (проект)]

[2] FIPS 186-3 — Federal Information Processing Standard «Draft Digital Signature Standard» (draft) [Федеральный стандарт обработки информации «Электронная цифровая подпись» (проект)]

[3] ILO Convention No. 185 — Seafarers' Identity Documents Convention (Revised), 2003 [Конвенция МОТ № 185 «Об удостоверениях личности моряков» (обновленная), 2003 г.]

[4] ILO SID-0002 Convention No. 185 — Seafarers' Identity Documents Convention (Revised), 2003 — The standard for the biometric template required by the Convention, Second impression (with modifications), 2005, ISBN 92-2-115788-1 [Конвенция МОТ № 185 «Об удостоверениях личности моряков» (обновленная), 2003 г. Стандарт для биометрических шаблонов в соответствии с требованиями Конвенции МОТ № 185. Второе издание (с изменениями), 2005 г.]

[5] ISO/IEC 11770-1:1996[1)] — Information technology — Security techniques — Key management — Part 1: Framework (Информационные технологии. Методы обеспечения безопасности. Менеджмент ключей. Часть 1. Структура)

[6] ISO/IEC TR 14516:2002 — Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services

(Информационные технологии. Методы защиты. Руководящие указания по использованию и управлению службами доверительной третьей стороны)

[7] ISO/IEC 17799:2005[2)] — Information technology — Security techniques — Code of practice for information security management (Информационные технологии. Методы и средства обеспечения безопасности. Свод правил по менеджменту информационной безопасности)

[8] ANSI X9.62-2005 — Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Standard (ECDSA) (Криптография с открытым ключом для индустрии финансовых услуг: алгоритм с открытым ключом для создания цифровой подписи)

[1)] Заменен на ISO/IEC 11770-1:2010.

[2)] Заменен на ISO/IEC 27002:2013.

УДК 004.93'1:006.89:006.354 ОКС 35.040 П85

Ключевые слова: информационные технологии, биометрия, биометрический профиль, биометрическая верификация моряков, биометрическая идентификация моряков

Редактор *Л.И. Потапова*
Технический редактор *В.Н. Прусакова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 22.06.2016. Подписано в печать 04.07.2016. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 4,65. Уч.-изд. л. 4,21. Тираж 24 экз. Зак. 1581

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4
www.gostinfo.ru info@gostinfo.ru