МЕЖГОСУДАРСТВЕННЫЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ
(МГС)

INTERSTATE COUNCIL FOR STANDARDIZATION, METROLOGY AND CERTIFICATION
(ISC)

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ ISO/IEC 24713-1— 2013

Информационные технологии

БИОМЕТРИЧЕСКИЕ ПРОФИЛИ ДЛЯ ВЗАИМОДЕЙСТВИЯ И ОБМЕНА ДАННЫМИ

Часть 1

Общая архитектура биометрической системы и биометрические профили

(ISO/IEC 24713-1:2008, IDT)

Издание официальное

Москва
Стандартинформ
2018

gost.e-ecolog.ru

Предисловие

Цели, основные принципы и основной порядок проведения работ по межгосударственной стандартизации установлены в ГОСТ 1.0—2015 «Межгосударственная система стандартизации. Основные положения» и ГОСТ 1.2—2015 «Межгосударственная система стандартизации. Стандарты межгосударственные, правила и рекомендации по межгосударственной стандартизации. Правила разработки, принятия, обновления и отмены»

Сведения о стандарте

1 ПОДГОТОВЛЕН Закрытым акционерным обществом «Папилон» (ЗАО «Папилон») при консультативной поддержке Ассоциации автоматической идентификации «ЮНИСКАН/ГС1 РУС» на основе официального перевода на русский язык англоязычной версии международного стандарта, указанного в пункте 5, который выполнен ЗАО «Папилон»

2 ВНЕСЕН Федеральным агентством по техническому регулированию и метрологии

3 ПРИНЯТ Межгосударственным советом по стандартизации, метрологии и сертификации (протокол от 27 сентября 2013 г. № 59-П)

За принятие проголосовали:

Краткое наименование страны по МК (ИСО 3166) 004—97	Код страны по МК (ИСО 3166) 004—97	Сокращенное наименование национального органа по стандартизации
Беларусь	BY	Госстандарт Республики Беларусь
Киргизия	KG	Кыргызстандарт
Молдова	MD	Молдова-Стандарт
Россия	RU	Росстандарт
Таджикистан	TJ	Таджикстандарт
Узбекистан	UZ	Узстандарт

4 Приказом Федерального агентства по техническому регулированию и метрологии от 17 декабря 2013 г. № 2282-ст межгосударственный стандарт ГОСТ ISO/IEC 24713-1—2013 введен в действие в качестве национального стандарта Российской Федерации с 1 сентября 2014 г.

5 Настоящий стандарт идентичен международному стандарту ISO/IEC 24713-1:2008 «Информационные технологии. Профили биометрические для взаимодействия и обмена данными. Часть 1. Общая архитектура биометрической системы и биометрические профили» («Information technology — Biometric profiles for interoperability and data interchange — Part 1: Overview of biometric systems and biometric profiles», IDT).

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

6 ВВЕДЕН ВПЕРВЫЕ

7 Следует обратить внимание на то, что некоторые элементы настоящего стандарта могут быть объектом патентного права. ИСО и МЭК не несут ответственность за установление подлинности какихлибо или всех таких патентных прав

8 ПЕРЕИЗДАНИЕ. Октябрь 2018 г.

*Информация об изменениях к настоящему стандарту публикуется в ежегодном 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 ежемесячном информационном указателе «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, оформление, 2018

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

Содержание

1 Область применения ... 1
2 Нормативные ссылки ... 1
3 Термины и определения ... 1
4 Обозначения и сокращения ... 4
5 Унифицированная биометрическая система ... 4
5.1 Концептуальная схема унифицированной биометрической системы ... 4
5.2 Концептуальные компоненты унифицированной биометрической системы ... 5
5.3 Функции унифицированной биометрической системы ... 6
6 Взаимодействие биометрической системы и приложения ... 8
6.1 Общие положения ... 8
6.2 Жизненный цикл ИД ... 8
6.3 Субъект и конечный пользователь ... 9
6.4 Биометрическое решение в сравнении с авторизацией ... 10
7 Средства сопряжения биометрической системы и приложения ... 12
7.1 Программный интерфейс приложений (ПИП) ... 12
7.2 Интерфейс протокола ... 12
7.3 Аппаратный интерфейс электронного устройства ввода/вывода ... 12
8 Разработка биометрических профилей на базе биометрических стандартов ... 13
8.1 Взаимосвязь базовых биометрических стандартов и их использование в биометрических профилях ... 13
8.2 Группы стандартов ... 14
8.3 Использование базовых биометрических стандартов для разработки биометрических профилей ... 14
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов межгосударственным стандартам ... 16
Библиография ... 17

Введение

Настоящий стандарт является основополагающим стандартом комплекса стандартов ISO/IEC 24713, устанавливающих требования к биометрическим профилям для обеспечения функционального взаимодействия и обмена данными. Стандарт предназначен для использования в качестве справочного руководства по внедрению унифицированной биометрической системы или системы, использующей стандартизированные биометрические профили.

Стандарт устанавливает общие требования к биометрическим системам и представляет собой руководство по использованию различных базовых стандартов применительно к биометрическим профилям для обеспечения функционального взаимодействия и обмена данными между биометрическими приложениями и системами.

Настоящий стандарт входит в комплекс стандартов и технических отчетов, которые были разработаны подкомитетом ИСО/МЭК СТК 1/ПК 37, с целью обеспечения взаимодействия и обмена данными между биометрическими приложениями и системами. Стандарты ИСО/МЭК СТК 1/ПК 37 устанавливают требования, которые направлены на разрешение сложных задач, связанных с применением биометрии в различных областях, связанных с идентификацией личности, как в среде открытых систем, так и внутри одной закрытой системы.

Примечание — Открытые системы строятся на стандартизированных и открыто опубликованных форматах данных, интерфейсах и протоколах для обеспечения взаимодействия и обмена данными с другими системами, которые могут включать устройства и программное обеспечение от различных изготовителей. Закрытая система может также строиться на таких стандартах и может включать устройства и программное обеспечение от различных производителей, но такая система не должна взаимодействовать и обмениваться данными с другими системами.

Стандарты, устанавливающие требования к форматам обмена биометрическими данными и биометрическим интерфейсам, необходимы для достижения полноценного обмена данными и взаимодействия в процессе биометрического распознавания в среде открытых систем. Стандарты на форматы обмена биометрическими данными, биометрические интерфейсы и биометрические профили, разрабатываемые ИСО/МЭК СТК 1/ПК 37, предназначены для использования в различных специфических областях.

Стандарты на форматы обмена биометрическими данными устанавливают структуру записи биометрических данных, подлежащих передаче, для различных биометрических модальностей. Стандарты ИСО/МЭК СТК 1/ПК 37 на форматы обмена биометрическими данными устанавливают требования к структуре записи биометрических данных для того, чтобы стороны, которые заранее условились об обмене, были способны их прочитать и применить. Кроме того, при использовании стандартизованного формата обмена данными стороны, которые получают данные, записанные в таком формате, могут их прочитать и без предварительного соглашения.

Стандарты на биометрические интерфейсы включают в себя единую структуру форматов обмена биометрическими данными (ЕСФОБД) и биометрический программный интерфейс (БиоАПИ). Данные стандарты поддерживают обмен биометрическими данными в рамках одной системы или между различными системами. Стандарт ЕСФОБД определяет основную структуру стандартизованной записи биометрической информации (ЗБИ), которая включает запись биометрических данных с дополнительными метаданными, такими как данные о дате ввода, об истечении срока их хранения, данные о кодировании и т.д. Стандарт БиоАПИ определяет программный интерфейс приложений для открытой системы, который поддерживает передачу информации между приложениями программного обеспечения и лежит в основе сервисов биометрических технологий. БиоАПИ также определяет формат ЗБИ в соответствии с ЕСФОБД для хранения и передачи данных, полученных в рамках использования БиоАПИ.

Стандарты на биометрические профили регламентируют использование базовых стандартов (например на форматы обмена биометрическими данными и биометрический программный интерфейс, а также, возможно, и стандартов небиометрического применения) для конкретных применений. Стандарты на биометрические профили устанавливают функциональные задачи (например контроль физического доступа сотрудников аэропорта) и требования по использованию базовых стандартов для обеспечения взаимодействия в рамках конкретной функциональной задачи.

М Е Ж Г О С У Д А Р С Т В Е Н Н Ы Й С Т А Н Д А Р Т

Информационные технологии

БИОМЕТРИЧЕСКИЕ ПРОФИЛИ ДЛЯ ВЗАИМОДЕЙСТВИЯ И ОБМЕНА ДАННЫМИ

Часть 1
Общая архитектура биометрической системы и биометрические профили

Information technology. Biometric profiles for interoperability and data interchange.
Part 1. Overview of biometric systems and biometric profiles

Дата введения — 2014—09—01

1 Область применения

Настоящий стандарт устанавливает и определяет функциональные блоки и компоненты унифицированной биометрической системы и индивидуальные характеристики каждого компонента. В настоящем стандарте описана унифицированная биометрическая ссылочная архитектура, включающая в себя соответствующие базовые биометрические стандарты, для обеспечения взаимодействия и обмена данными.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты. При использовании ссылок на документы с указанной датой утверждения, необходимо пользоваться только данной редакцией. Если дата утверждения не приведена, следует пользоваться последней редакцией ссылочных документов, включая любые поправки и изменения к ним:

ISO/IEC 19794-1:2006 Information technology — Biometric data interchange formats — Part 1: Framework (Информационные технологии. Форматы обмена биометрическими данными. Часть 1. Структура)

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **программный интерфейс приложений;** ПИП (application programming interface; API): Программный интерфейс, который может использоваться для связи и сопряжения между приложением и биометрической системой.

Примечание 1 — Программный интерфейс приложений (ПИП) — это машинный код, используемый разработчиком приложения. Разработчик приложения может добавить или заменить любую биометрическую систему, совместимую с его ПИП.

Примечание 2 — Интерфейсы ПИП часто описываются качественными степенями — высокий уровень или низкий уровень. Высокий уровень означает, что интерфейс относится к приложению, а низкий уровень означает, что интерфейс относится к устройству.

3.2 **приложение** (application): Установленное на оборудовании программное обеспечение, используемое для выполнения широкого перечня требований.

Примечание — В данном контексте приложение включает в себя биометрическую систему для удовлетворения ряда требований, касающихся верификации или идентификации личности конечного пользователя, так чтобы идентификатор конечного пользователя мог быть применен для облегчения взаимодействия конечного пользователя с системой.

Издание официальное

Пример — Основным требованием к системе учета рабочего времени с использованием какого-либо биометрического признака является ее способность регистрировать время начала и окончания работы для корректного начисления заработной платы работнику. Такая система использует биометрический признак для проверки утверждения, что именно личность данного работника ассоциируется системой с его ИД-номером в те моменты, когда работник взаимодействует с биометрическим устройством на входе в рабочее помещение и при выходе из него.

3.3 **базовый стандарт** (base standard): Основополагающий стандарт с элементами, содержащими опции/допустимые варианты.

Примечание — Базовые стандарты могут использоваться в разнообразных приложениях, для каждого из которых может быть полезным фиксирование дополнительных элементов в стандартизированном профиле с целью достижения функциональной совместимости между экземплярами конкретного приложения.

3.4 **биометрический** (biometric): Относящийся к предметной области биометрии.

3.5 **биометрия** (biometrics): Автоматизированное распознавание личности человека, основанное на его поведенческих или биологических характеристиках.

3.6 **биометрические данные** (biometric data): Информация, извлеченная из биометрического образца и используемая для построения шаблона, с которым сравнивается ранее полученный шаблон.

3.7 **биометрические функции** (biometric functions): Процедуры или действия по биометрической регистрации (3.19), верификации (3.35) и/или идентификации (3.25) внутри биометрической системы.

3.8 **данные биометрического обмена;** ДБО (biometric interchange data; BID): Биометрические данные, отформатированные согласно одному или нескольким стандартам обмена, как это определяется стандартами комплекса ISO/IEC 19794.

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

Примечание — Биометрические профили определяют специфические значения или условия из ряда допустимых вариантов, описанных в соответствующих базовых стандартах, с целью поддержки взаимообмена данными между приложениями и взаимодействия систем.

3.10 **биометрический образец** (biometric sample): Необработанные данные, представляющие собой биометрическую характеристику конечного пользователя, как они были захвачены биометрической системой.

3.11 **биометрическая система** (biometric system): Автоматизированная (как правило) система, которая предоставляет возможность:

1) получить биометрический образец непосредственно от конечного пользователя или образец, предоставленный в соответствии с какой-либо экспертно-криминалистической технологией;

2) извлекать биометрические данные из полученного образца или же выводить биометрические признаки из биометрических данных в виде, пригодном для сопоставления с одним или несколькими контрольными шаблонами;

3) сравнивать биометрические признаки с теми, что содержатся в одном или нескольких контрольных шаблонах;

4) определять степень сходства в соответствии с индексом или другим (метрическим или иным) показателем или, как вариант, ранжировать шаблоны в соответствии с уровнем сходства, определяемым индексом или другим метрическим показателем;

5) возвращать результат приложению с указанием, была ли идентификация и/или верификация выполнена успешно;

6) хранить биометрические данные и связанную с ними системную информацию и управлять этими данными.

Примечание — Биометрические системы можно разделить на два класса, а именно:

- монобиометрические системы: когда биометрическая система использует одну единственную биометрическую модальность, алгоритм или датчик;
- мультибиометрические системы: когда биометрическая система использует несколько биометрических модальностей и/или чувствительных датчиков и/или алгоритмов.

3.12 **компоненты биометрической системы** (biometric system components): Части или элементы системы, которые выполняют определенные задачи, необходимые системе для ее нормального функционирования.

Пример — Примеры компонентов биометрической системы — захват, обработка и сравнение.

3.13 **биометрический шаблон** (biometric template): Биометрические данные, полученные из биометрического образца или набора биометрических образцов, пригодные для хранения в качестве контрольных для последующего сравнения.

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

3.15 **сравнение** (comparison): Процесс определения сходства между запросным и контрольным шаблонами.

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

3.17 **решение** (decision): Результат сравнения индекса совпадения и порогового значения.

Примечание — Решение может быть положительным или отрицательным (отказ).

3.18 **конечный пользователь** (end-user): Человек, который взаимодействует с биометрической системой для своей регистрации или идентификации.

3.19 **биометрическая регистрация** (enrolment): Процесс сбора биометрических образцов от конечного пользователя и последующей подготовки и хранения биометрических контрольных шаблонов, а также, при необходимости, других данных, связанных с личностью конечного пользователя.

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

3.21 **ложный допуск** (false acceptance): Событие, заключающееся в том, что биометрическая система неверно идентифицирует личность человека или ошибочно подтверждает личность человека, выдающего себя за другого.

3.22 **ложный недопуск** (false rejection): Отказ биометрической системы в идентификации конечного пользователя или в верификации зарегистрированной личности конечного пользователя.

3.23 **идентификатор** (identifier): Строка уникальных данных, используемая в биометрической системе в качестве ключа, связывающего биометрические признаки (атрибуты) человека с описательными характеристиками (атрибутами) личности этого человека.

3.24 **личность** (identity): Понятие личности человека в общем смысле.

Примечание — Атрибуты, которые могут быть использованы для определения личности, включают имя человека, аспекты его индивидуальности или физической внешности, предыдущую историю транзакций между приложением и конечным пользователем, национальность, образование, имя работодателя/место работы, категорию допуска, финансово-кредитную историю. В биометрической системе личность человека устанавливается, как правило, при его регистрации в системе в соответствии с предъявляемыми им документами, например свидетельством о рождении, паспортом т.п.

3.25 **идентификация** как функция биометрической системы (identification <biometric system function>): Функция, которая выполняет поиск «один ко многим» для получения списка кандидатов.

Пример — BioAPI_IdentifyMatch.

Примечание — Функция идентификации может использоваться для проверки запроса на регистрацию в регистрационной базе данных без ввода биометрического идентификатора.

3.26 **мультибиометрическая система** (multiple biometric): Определение биометрической системы, объединяющей в себе более одной биометрической технологии.

3.27 **запись** (record): Шаблон и другая информация о конечном пользователе, например права доступа.

3.28 **индекс совпадения** (score): Численное значение, результат сравнения, определяющий степень сходства или соотношения между биометрическим образцом и контрольным шаблоном.

3.29 **стандарт** (standard): Учрежденный на основе консенсуса и одобренный официальным органом документ, который предоставляет для общего и регулярного пользования правила, рекомендации или параметры действий или их результаты, нацеленные на достижение оптимальной степени порядка в данном контексте.

Примечание — Стандарты должны основываться на консолидированных результатах научной работы, технологических исследований и опыта, и должны быть нацелены на стимулирование оптимальной выгоды для сообщества.

3.30 **субъект** (subject): Конечный пользователь, чьи биометрические данные предназначаются для регистрации или сравнения.

3.31 **токен/носитель данных** (token): Физическое устройство, содержащее определенную информацию о конечном пользователе или предъявителе/держателе.

3.32 **пороговое значение** (threshold): Граничная величина индекса совпадения, используемая программой сравнения для автоматического принятия решения допустить или отклонить контрольный шаблон, сравниваемый с запросным шаблоном.

Примечание — Если индекс совпадения, полученный при сравнении, выше порогового значения, то контрольный шаблон помещается в список кандидатов, если нет — отклоняется. Пороговое значение регулируется так, чтобы биометрическая система обеспечивала необходимую избирательность в зависимости от требований конкретного биометрического приложения.

3.33 **пользователь** (user): Человек, ответственный за управление и/или внедрение и/или администрирование биометрической системы, в отличие от конечного пользователя, чьи биометрические данные непосредственно захватываются ею.

3.34 **проверка достоверности** (validation): Процесс, демонстрирующий, что рассматриваемая система удовлетворяет требованиям, предъявляемым к данной системе, во всех отношениях.

3.35 **верификация** (verification): Функция биометрической системы, выполняющая сравнение запросного образца с указанным шаблоном, хранящимся в системе, в режиме «один к одному» и возвращающая результат в виде индекса совпадения или решения о совпадении.

3.36 **биометрические признаки** (biometric features): Отличительные и повторяющиеся характеристики биометрического образца, которые могут храниться в составе шаблона в базе данных или использоваться при сравнении с каким-либо определенным шаблоном.

4 Обозначения и сокращения

В настоящем стандарте применены следующие сокращения:

ДБО (BID) — данные биометрического обмена (biometric interchange data);

ИД (ID) — идентификация (identification);

ПИН (PIN) — персональный идентификационный номер (personal identification number);

ПИП (API) — программный интерфейс приложений (application programming interface).

5 Унифицированная биометрическая система

5.1 Концептуальная схема унифицированной биометрической системы

При большом разнообразии биометрических приложений и технологий можно сделать некое обобщение биометрических систем. Во всех биометрических системах присутствуют общие элементы. Биометрические образцы регистрируются у субъекта с помощью датчиков. Данные с датчика передаются в устройство обработки, которое извлекает отличительные, но повторяющиеся характеристики биометрического образца (его признаки), и отбрасывает все прочие элементы. Выделенные таким образом признаки записываются в базу данных в виде биометрического шаблона или сравниваются с отдельным шаблоном или с несколькими шаблонами, хранящимися в базе данных. Целью этого сравнения является определение степени совпадения шаблонов. Решение о подтверждении подлинности выносится на основании оценки степени сходства признаков биометрического образца и признаков, записанных в шаблоне или шаблонах, с которыми этот образец сравнивается.

Рисунок 1 показывает направление информационного потока внутри унифицированной биометрической системы, состоящей из подсистем, обеспечивающих захват данных, обработку сигнала, хранение, сравнение и принятие решения. Данная схема иллюстрирует как процесс регистрации, так и работу систем верификации, и идентификации. В следующих разделах документа детально описана каждая из перечисленных подсистем. Следует заметить, что в любой реально действующей биометрической системе эти концептуальные компоненты могут отсутствовать или не соответствовать в точности реальным физическим компонентам.

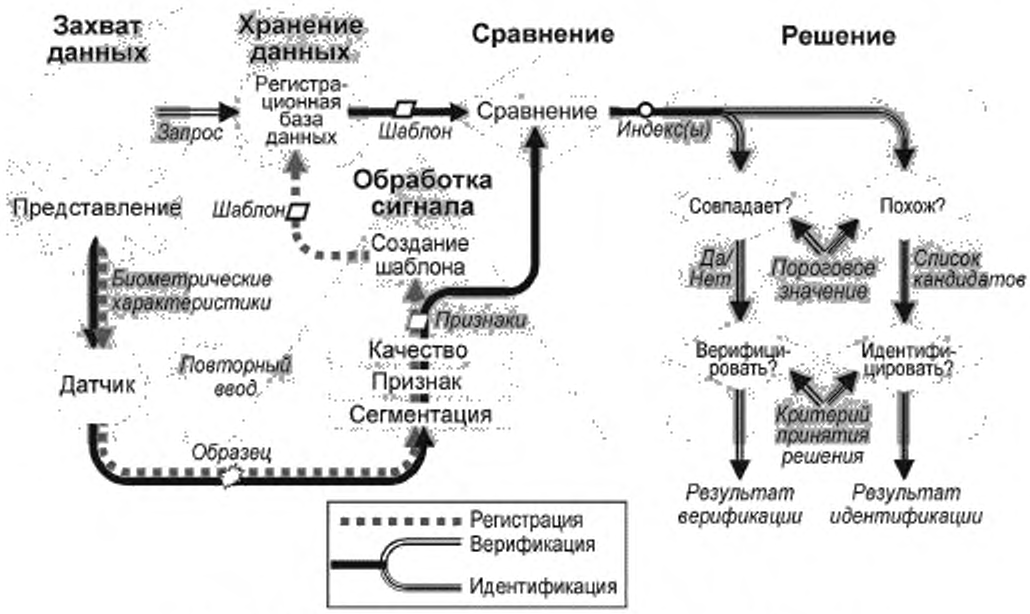

Рисунок 1 — Компоненты унифицированной биометрической системы

5.2 Концептуальные компоненты унифицированной биометрической системы

5.2.1 Подсистема захвата данных

Подсистема захвата данных получает с датчика биометрические характеристики субъекта в виде изображения или сигнала и выводит изображение/сигнал в виде биометрического образца.

5.2.2 Подсистема передачи данных (на схеме не представлена)

Подсистема передачи (которая не всегда представлена или явно присутствует в биометрической системе) осуществляет передачу биометрических образцов, признаков и/или шаблонов между различными подсистемами. Биометрические образцы, данные или шаблоны передаются в стандартном формате обмена биометрическими данными. Биометрический образец может быть подвергнут сжатию и/или шифрованию перед отправкой и распакован (разжат) и/или дешифрован перед использованием. В процессе передачи биометрический образец может изменяться из-за помех в канале передачи данных или из-за потерь при сжатии и распаковке. Для обеспечения подлинности, целостности и конфиденциальности записанных и передаваемых биометрических данных рекомендуется использовать криптографические методы защиты информации.

5.2.3 Подсистема обработки сигнала

Подсистема обработки сигнала извлекает отличительные признаки из биометрического образца. Эта обработка может включать локализацию сигнала, содержащего биометрические характеристики субъекта, внутри полученного образца (этот процесс именуется сегментацией), извлечение признаков и контроль качества, гарантирующий, что извлеченные свойства могут считаться отличительными и повторяющимися. Если на этапе контроля качества полученные образцы отвергаются, то требуется получить другие образцы от подсистемы захвата данных.

В процессе регистрации подсистема обработки сигнала создает шаблон на основе извлеченных биометрических признаков. Для прохождения регистрации могут потребоваться несколько представлений биометрических характеристик регистрируемого субъекта. В некоторых случаях шаблон состоит только из отличительных признаков.

5.2.4 Подсистема хранения данных

Шаблоны хранятся в регистрационной базе данных, поддерживаемой системой хранения данных. Каждый шаблон связан с подробной информацией о зарегистрированном лице. Следует заметить, что прежде чем шаблоны будут сохранены в регистрационной базе данных, они могут быть представлены в

соответствии с форматом обмена. Шаблоны могут храниться на самом устройстве захвата биометрического образца, на переносном носителе, например смарт-карте, на локальном персональном компьютере, локальном сервере или в центральной базе данных.

5.2.5 Подсистема сравнения данных

Подсистема сравнения данных выполняет сопоставление отличительных признаков с одним или более шаблонами и выдает подсистеме принятия решений индексы совпадения. Индексы совпадения указывают степень похожести сравниваемых признаков и шаблонов. В некоторых случаях отличительные свойства и хранимый шаблон могут иметь одинаковую форму. При выполнении верификации субъекта на единственный запрос выдается один единственный индекс совпадения. При выполнении идентификации множество или все шаблоны могут сравниваться с запросными отличительными признаками и индекс совпадения будет выдаваться на каждое сравнение.

5.2.6 Подсистема принятия решений

Подсистема принятия решений использует индексы совпадения, сформированные одной или несколькими попытками, чтобы выдать итоговый результат для транзакции верификации или идентификации.

В процессе верификации сравнение биометрических признаков признается успешным, если индекс совпадения превышает установленное пороговое значение. Запрос на проверку наличия записи субъекта в регистрационной базе данных может быть выполнен в соответствии с методикой принятия решений, которая может предусматривать несколько попыток верификации.

В процессе идентификации идентификатор конечного пользователя или шаблон являются потенциальными кандидатами для субъекта, когда индекс совпадения превышает заданное пороговое значение, и/или когда индекс совпадения оказывается в числе заданного количества наибольших значений. Правила принятия решений могут допускать или требовать нескольких попыток для принятия решения об идентификации.

Примечание — Концептуально возможно рассматривать мульти-биометрические системы подобно моно-биометрическим, считая комплексные биометрические образцы/ шаблоны/ индексы за один образец/шаблон/ индекс и позволяя подсистеме принятия решений при необходимости оперировать совокупным индексом или совокупным решением.

5.2.7 Подсистема администрирования

Подсистема администрирования (на рисунке 1 не представлена) управляет общей методикой, поведением и использованием биометрической системы с учетом законодательных, юридических и общественных ограничений и требований. В частности, подсистема администрирования выполняет:

- обеспечение обратной связи с субъектом во время и/или после захвата данных;
- запрос дополнительной информации от субъекта;
- хранение и форматирование биометрических шаблонов и/или данных биометрического обмена;
- вынесение окончательного заключения на выходе из подсистемы принятия решений;
- задание пороговых значений;
- настройку параметров сбора данных для биометрической системы;
- контроль операционной среды и хранение других, небиометрических, данных;
- обеспечение надлежащих мер безопасности по защите персональной информации конечного пользователя;
- взаимодействие с приложением, использующим биометрическую систему.

5.2.8 Интерфейс*

Биометрическая система может взаимодействовать с внешними приложениями или системами через программный интерфейс приложений (ПИП), аппаратный интерфейс или интерфейс протокола.

5.3 Функции унифицированной биометрической системы

5.3.1 Биометрическая регистрация

При биометрической регистрации данные, полученные в результате взаимодействия субъекта с системой, обрабатываются и сохраняются в виде регистрационного шаблона для данного субъекта.

Биометрическая регистрация обычно включает в себя:

- получение образца;
- сегментацию и извлечение отличительных признаков,
- контроль качества (по результатам которого полученный образец или признаки могут быть отклонены как непригодные для создания шаблона, и может потребоваться получение дополнительных образцов);

* Интерфейс на рисунке 1 не представлен.

- создание шаблона, для чего могут потребоваться признаки, извлеченные из нескольких образцов, их преобразование в формат обмена биометрическими данными и его хранение;
- тестовая верификация или идентификация для подтверждения пригодности результата биометрической регистрации для дальнейшего использования;
- разрешение повторной попытки биометрической регистрации (в зависимости от принятых правил) в случае неудовлетворительных результатов.

5.3.2 Верификация

При верификации данные, полученные в результате взаимодействия субъекта с системой, обрабатываются с целью подтвердить наличие в системе данных субъекта (например — «я зарегистрирован как субъект X»). В результате верификации запрос будет отвергнут или подтвержден. Результат верификации считается неверным, если был принят ложный запрос (ложный допуск), либо если истинный запрос был отклонен (ложный недопуск). Некоторые биометрические системы позволяют одному конечному пользователю регистрировать более одного экземпляра биометрической характеристики (например система, использующая радужную оболочку глаза, может позволить конечным пользователям регистрировать изображения радужки обоих глаз, а система, использующая отпечатки пальцев, может регистрировать два и более пальцев, сохраняя их как резервные на случай травмы одного из пальцев).

Верификация обычно включает в себя:

- получение биометрического образца;
- сегментацию и извлечение отличительных признаков;
- контроль качества (по результатам которого полученный образец или признаки могут быть отклонены как непригодные для создания шаблона, и может потребоваться получение дополнительных образцов);
- сравнение признаков образца с шаблоном для подтверждения личности с выдачей индекса совпадения;
- выработку решения о совпадении с шаблоном на основании значения индекса совпадения, превышающего или нет пороговое значение;
- выработку верификационного решения на основании совпадений в результате одной или более попыток согласно правилам принятия решений.

Пример — В системе, допускающей при верификации до трех попыток сравнения с зарегистрированным шаблоном, ложный недопуск будет результатом любой комбинации сбоев в получении и ложных несовпадений в этих трех попытках. Ложный допуск произойдет, если образец получен, но совпал ошибочно с зарегистрированным образцом в любой из трех попыток.

5.3.3 Идентификация

При идентификации данные, полученные в результате взаимодействия субъекта с системой, обрабатываются с целью поиска идентификатора, полученного при регистрации субъекта. Идентификация выдает рекомендательный список идентификаторов, который может быть пустым или содержать только один идентификатор. Идентификация считается верной, если идентификатор истинного зарегистрированного субъекта попадает в список кандидатов. Идентификация считается ошибочной, если идентификатор истинного зарегистрированного субъекта не попадает в рекомендательный список (ложноотрицательная идентификация), либо если в результате обработки запроса, составленного на незарегистрированного субъекта, создается непустой рекомендательный список (ложноположительная идентификация).

Процесс идентификация обычно предусматривает:

- получение биометрического образца;
- сегментация и извлечение отличительных признаков;
- контроль качества (по результатам которого полученный образец или признаки могут быть отклонены как непригодные для создания шаблона, и может потребоваться получение дополнительных образцов);
- сравнение с отдельными или со всеми шаблонами, имеющимися в регистрационной базе данных, в результате которого выдается индекс совпадения по каждому сравнению;
- выработку решений о том, является ли каждый совпавший шаблон потенциальным кандидатом для определения идентификатора пользователя на основании превышения значением индекса совпадения порогового значения и/или попадания значения индекса в заданное число наибольших значений, и выдачу списка кандидатов;
- решение об идентификации на основании анализа списков кандидатов, полученных после одной или более попыток, в соответствии с правилами принятия решений.

6 Взаимодействие биометрической системы и приложения

6.1 Общие положения

Приложение, которое включает в себя (помимо прочего) биометрическую систему, должно быть способным управлять признаками идентичности зарегистрированных лиц. На абстрактном уровне это можно описать с помощью понятия «жизненный цикл идентификации». Жизненный цикл идентификации (ИД) описывает взаимодействие:

- индивидуумов;
- удостоверяющих данных, дающих полномочия или подтверждающих личность;
- привилегий и ресурсов.

Обычна ситуация, когда индивидуум хочет получить и использовать некие (логические или физические) удостоверяющие данные, обеспечивающие ему доступ к привилегиям и/или ресурсам. Такие данные представляют собой нечто, дающее право на доверие, хорошую репутацию или полномочия.

К подобным данным относятся:

- документы;
- пластиковые карты;
- персональные идентификационные номера (ПИН);
- пароли.

Привилегия может представлять собой авторизацию, например — с целью доступа к определенным данным.

Пример обычного контроля доступа: сотрудник использует карточку контроля доступа для прохода в определенные помещения; применительно к паспортной системе — гражданин может обратиться за новым паспортом или визой, разрешающей ему пересекать границу страны, которую он хочет посетить.

Роль, которую играют биометрические системы в типичной системе прикладного назначения или системе безопасности, заключается в том, чтобы засвидетельствовать (через биометрическое решение), что субъект является тем, за кого себя выдает (верификация и положительная идентификация), или установить, что он не принадлежит к заранее установленной группе лиц (отрицательный запрос идентификационной информации или идентификация лиц, находящихся в розыске).

6.2 Жизненный цикл ИД

Жизненный цикл ИД в системе верификации включает четыре различных стадии или фазы с точки зрения управления. В некоторых приложениях часть фаз может присутствовать в слиянии с другими стадиями цикла. Но в общем случае любая из этих фаз может встречаться (физически или логически) отдельно от других.

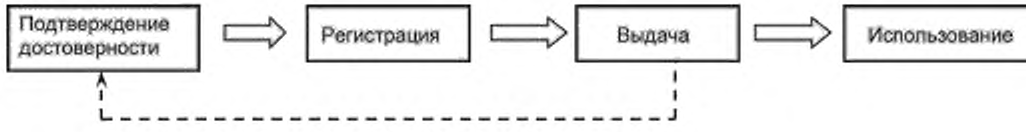

Рисунок 2 — Жизненный цикл ИД

Приложения обычно работают по принципу циклов итераций с точки зрения управления признаками идентичности в течение своего жизненного цикла.

6.2.1 Подтверждение достоверности

Подтверждение достоверности — процесс проверки физической идентичности, т.е. того факта, что человек действительно является тем, за кого себя выдает.

Пример — Проверка достоверности документов (например свидетельства о рождении, паспорта). Биометрические характеристики могут быть использованы для проверки анкетных данных и для того, чтобы проверить человека по его документам, и т.д. (см. далее).

6.2.2 Регистрация

Регистрация — процесс создания электронной записи, представляющей физическое лицо и сопутствующую ему информацию в логической структуре данных, поддерживаемых приложением. Обычно в рамках данного процесса создается уникальный идентификатор, представляющий физическое лицо. Кроме того, на этапе биометрической регистрации захватываются образцы биометрических данных.

Пример — Захват и сохранение персональных данных, прежде чем будет выдано новое водительское удостоверение.

Биометрическая подсистема обычно используется органами управления (юридическими, профессиональными и т.д.), которые могут устанавливать жесткие связи между биометрическим образцом и набором информации, релевантной (т.е. значимой) для данной структуры. Эти жесткие связи первоначально устанавливаются в рамках биометрической регистрации, когда биометрические данные добавляются к уже подтвержденным личностным данным. Органы управления имеют возможность устанавливать подобные жесткие связи с использованием любого механизма обеспечения безопасности, таких как шифрование записей, касающихся конечных пользователей.

6.2.3 Выдача

Выдача — процесс предоставления привилегий человеку и выдачи ему неких удостоверяющих данных, дающих ему право доступа к этим привилегиям.

Пример 1 — Предоставление человеку прав физического доступа вместе с картой контроля доступа.

Пример 2 — Выдача паспорта человеку, дающего ему право пересекать границы.

Пример 3 — Выдача пароля человеку для доступа к конфиденциальной информации.

Процесс выдачи может включать биометрические технологии, например для того, чтобы проверить, что человек, желающий получить удостоверяющий документ, действительно тот, кто должен его получить, т.е. его биометрические данные совпадают с теми, что записаны в удостоверяющем его личность документе.

6.2.4 Использование

После получения прав, физическое лицо использует удостоверяющие данные в рамках взаимодействия с приложением для доступа к привилегиям, что подразумевает авторизацию определенного характера.

Пример 1 — Физический доступ на территорию с ограниченным доступом посредством использования токена, содержащего биометрические данные.

Пример 2 — Пересечение границы с использованием машиносчитываемого проездного документа, содержащего биометрические данные.

В процессе использования биометрических технологий можно проверить целостность информации, полученной во время биометрической регистрации, и подтвердить строгое соответствие между конечным пользователем и связанной с ним информацией в зависимости от уровня доверия к органу управления, проводившему биометрическую регистрацию.

6.3 Субъект и конечный пользователь

В настоящем разделе рассматриваются два аспекта личности субъекта: идентификатор (относящийся к логической записи личности), посредством которого личность распознается приложением, и процесс подтверждения достоверности, который дополнительно свидетельствует о том, что данный человек является лицом, связанным с идентификатором.

6.3.1 Пример контроля доступа

В качестве примера должны быть рассмотрены все этапы регистрации нового конечного пользователя в приложении, таком как, например, система контроля доступа на предприятии.

Подтверждение достоверности

Администратор приложения устанавливает личность субъекта, используя как небиометрические, так и биометрические средства. Подтвердить достоверность можно, как правило, с помощью документов, таких как свидетельство о рождении, паспорт и т.д. Данный этап может также включать поиск по биометрической базе данных, чтобы проверить, не был ли этот человек ранее зарегистрирован в базе данных. Это достигается посредством негативной идентификации. Данный этап может также включать проверку по другим имеющимся данным, например по досье в правоохранительных органах или по базе данных всех конечных пользователей, зарегистрированных в системе на данный момент.

Регистрация

Если идентичность субъекта подтверждена, система контроля доступа признает его новым конечным пользователем и присваивает ему уникальный идентификатор, по которому она его будет распознавать. Примером идентификатора может служить идентификационный номер в системе контроля доступа. В ходе процесса регистрации будут получены также биометрические данные субъекта,

а биометрическая система создаст запись в соответствии с форматом обмена биометрическими данными (ДБО-запись), которая будет соотноситься с личностью конечного пользователя через его идентификатор. Эта запись будет связана с идентификатором либо путем сохранения их физически в одном и том же месте в базе данных приложения или в базе данных ДБО-записей, либо путем связывания их с использованием шифрования или механизма цифровой подписи при создании записи конечного пользователя. На этом регистрация субъекта в качестве нового конечного пользователя системы завершается.

6.3.2 Пример проездных документов

Второй пример показывает этапы получения гражданином нового проездного документа, например биометрического паспорта.

Подтверждение достоверности

В этом конкретном примере процесс подтверждения достоверности сведений может растянуться на более продолжительное время, чем в примере с системой контроля доступа (6.3.1), так как часто требуется обращение к другим базам данных, чтобы получить свидетельства социальной благонадежности гражданина, и, возможно, его освидетельствование уполномоченными органами. Кроме того, в случае продления срока действия документа, позитивная биометрическая верификация может использоваться для проверки подлинности личности.

Регистрация

Если идентичность субъекта подтверждена, администратор признает его действительным конечным пользователем и присваивает ему уникальный идентификатор, по которому система будет его распознавать. Примером идентификатора может быть номер паспорта. В процессе регистрации будут получены также биометрические данные субъекта, и биометрическая система создаст запись в соответствии с форматом обмена биометрическими данными (ДБО-запись), которая будет соотноситься с личностью конечного пользователя через его идентификатор. Данная запись будет связана с идентификатором либо путем сохранения их физически в одном и том же месте в базе данных приложения или в базе данных ДБО-записей, либо путем связывания их с использованием шифрования (см. рисунок 2) или механизма цифровой подписи при создании записи конечного пользователя. Регистрация субъекта в качестве нового пользователя системы завершена. Администратор может также выдать субъекту уникальный номер транзакции, который позволит ему забрать паспорт после выпуска. Данный номер может совпадать или не совпадать с идентификатором, с которым оказался связанным данный субъект в рамках приложения.

Выдача

Субъект может забрать свои новые проездные документы по уведомлению, или по номеру транзакции, если таковой был выдан ему при регистрации. Могут быть использованы биометрические характеристики для подтверждения того, что субъект, получающий паспорт, является именно тем лицом, чьи биометрические данные записаны в паспорте.

Оба примера демонстрируют в конечном итоге связь биометрических данных и идентификационного номера (ИД-номера). Именно этот ИД-номер (идентификатор), т.е. логическая запись личности, распознается приложением, а не физическая личность.

6.4 Биометрическое решение в сравнении с авторизацией

Данный раздел дает дальнейшие разъяснения относительно различий между решением (верификацией или идентификацией), вырабатываемым биометрической системой, и получением привилегий в форме авторизации в рамках приложения. Если от биометрической системы требуется подтвердить личность или идентифицировать ее, приложение работает с решением и привилегиями (авторизацией).

Решение — результат работы биометрической системы, основанный на сравнительном анализе биометрических данных субъекта, полученных из биометрического образца, и либо шаблона (в случае верификации), либо некоего набора шаблонов (в случае идентификации).

Примечание — Вид представляемых результатов зависит от конкретного приложения: проход разрешен/запрещен, индекс совпадения, список и др.

Привилегии (авторизация) являются результатом процесса, в основе которого лежит решение и информация, соотносимая с определенными биометрическими данными, полученными при регистрации. На этом этапе целостность информации, уровень доверительности, обеспечиваемый органом управления, оперирующем данной информацией, соответствующие права и полномочия и т.д. являются существенными для обеспечения достоверности авторизации.

Будет полезным рассмотреть, что происходит в процессе использования, т.е. когда индивидуум хочет получить доступ (6.3.1) или пересечь границу (6.3.2).

Биометрическое решение может использовать положительную идентификацию или верификацию. В случае, когда ДБО-запись (запись в соответствии с форматом обмена биометрическими данными) связана с идентификатором с использованием шифрования, выполняют следующие шаги.

Субъект обращается к приложению с запросом, заявляя тем самым, что является зарегистрированным пользователем системы. Согласно сценарию процедуры контроля доступа, это можно сделать, например, посредством ввода имени пользователя, соответствующего конечному пользователю, или представив системе токен, с которого считывается указатель на запись конечного пользователя или непосредственно сама такая запись. Согласно сценарию проездных документов, паспорт может содержать устройство идентификации или чип, содержащий запись конечного пользователя, которая считывается специальным считывателем непосредственно с паспорта:

- приложение проверяет (путем передачи записи в биометрическую систему или путем поиска по биометрической системе), что запись конечного пользователя, им заявленная, действительно существует в биометрической системе, после чего система выдает ДБО-запись и идентификатор, созданные в системе при регистрации конечного пользователя. На этом этапе либо приложение, либо биометрическая система (либо и то и другое) могут проверить достоверность записи конечного пользователя, используя для этого, например, цифровую подпись;
- от субъекта потребуется доказать, что идентификатор действительно принадлежит ему, путем предоставления биометрического образца с помощью соответствующего биометрического устройства. Выполнив обычные шаги верификации (5.3.2), биометрическая система выдает решение о соответствии данного субъекта идентификатору;
- положительное биометрическое решение предполагает, что субъект соответствует ДБО, которые связаны с идентификатором в составе записи конечного пользователя. Тем самым подразумевается, что субъект связан с идентификатором в составе записи конечного пользователя. Этот идентификатор затем передается приложению (рисунок 3), где конечный пользователь авторизуется в соответствии с его правами в данном приложении. По сценарию процедуры контроля доступа субъект получает доступ в систему, а по сценарию выездных документов — ему разрешается пересечь границу.

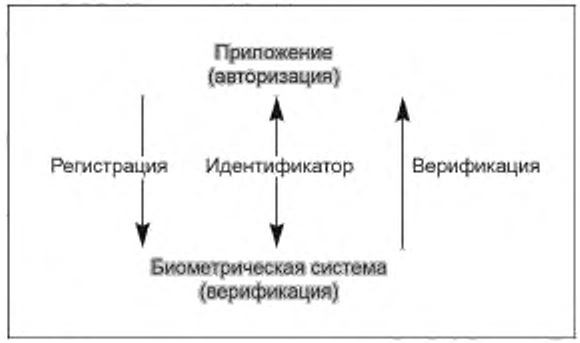

Рисунок 3 — Взаимосвязь идентификатора с биометрической системой при верификации конечного пользователя и с приложением при авторизации

Такое разделение между процедурами верификации субъекта (решением биометрической системы) и наделением привилегиями конечного пользователя, например авторизацией, внутри приложения открывает возможность успешной интеграции биометрических систем в типичные приложения. Оно обеспечивает явную изоляцию процесса принятия решений в биометрической системе от прав и привилегий, которые даны конечному пользователю в приложении. Это особенно важно при решении таких задач, как аннулирование прав и привилегий конечного пользователя, или в случае, когда один человек выступает в роли нескольких конечных пользователей в приложении (например как обычный конечный пользователь и как администратор). Использование шифрования или другого подобного механизма привязки также уменьшает риск утечки данных.

7 Средства сопряжения биометрической системы и приложения

Цель данного раздела — определение возможных способов сопряжения биометрической системы и приложения.

Существуют следующие варианты интерфейсов:

- программный интерфейс приложений (ПИП);
- интерфейс протокола;
- аппаратный интерфейс электронного устройства ввода/вывода.

7.1 Программный интерфейс приложений (ПИП)

Как определено соответствующими стандартами в сфере информационных технологий, ПИП — программный интерфейс, который может быть использован для взаимодействия и сопряжения приложения и биометрической системы. Такая форма интерфейса может, но не обязательно, находиться на том же самом физическом компьютере, на котором запущены приложение и биометрическая система. Это наиболее часто встречающаяся форма интерфейса, поддерживаемая, в том числе, и спецификациями БиоАПИ. Интерфейс стандарта ПИП — это интерфейс низкого уровня, который, как правило, обеспечивает исчерпывающий характер функциональных возможностей взаимодействия приложения и биометрической системы.

7.2 Интерфейс протокола

Интерфейс протокола используют для сопряжения систем, которые выдают данные в специфическом стандартизированном формате либо в каком-то проприетарном (пользовательском) формате, и биометрической системы, которая может использовать такой интерфейс для получения, например, идентификатора пользователя из строки данных. Типичный пример интерфейса такого типа — биометрические системы, которые получают идентификатор по Wiegand-протоколу со считывателя системы контроля доступа и извлекают идентификатор из строки данных (см. SIA AC-01-1996.10, Access Control Standard Protocol for the 26-bit Wiegand TM Reader Interface).

7.3 Аппаратный интерфейс электронного устройства ввода/вывода

Такая форма интерфейса обычно используется для инициализации биометрического сравнения или для подачи сигнала в ответ на выход результата биометрического сравнения. Он не может передавать идентификатор от приложения биометрической системе, также как и приложение не может запросить информацию у биометрической системы, используя этот тип интерфейса. Типичный пример интерфейса электронного устройства ввода/вывода: приложение посредством такого интерфейса запускает процесс идентификации разыскиваемых лиц по биометрической системе. В таком сценарии биометрическая система должна быть сконфигурирована таким образом, чтобы процесс поиска лиц, находящихся в розыске, запускался, когда приложение изменяет состояние аппаратного интерфейса. Изменение состояния интерфейса означает, что приложение хочет запустить какую-либо биометрическую функцию. Соответствующее физическое устройство может быть подключено к любому компьютеру, используемому для обработки данных, либо может быть использовано в составе периферийных устройств. Например, к компьютеру, на котором запущено приложение, подсоединена камера с контактным сенсорным датчиком, так что каждый раз, когда датчик меняет свое состояние, запускается процесс распознавания изображения лица по списку разыскиваемых лиц, хранимому в биометрической системе.

Обратная связь по результатам идентификации обеспечивается биометрической системой, поскольку в рамках интерфейса не существует никаких других средств, которые можно было бы использовать для передачи данных между приложением и биометрической системой. Так биометрическая система может изменять состояние контакта в зависимости от результата биометрического сравнения. Например, интерфейс между биометрической системой и панелью контроля доступа может формировать сигнал о том, что биометрическое сравнение выполнено успешно или неуспешно. При обнаружении сигнала об изменении состояния интерфейса приложение контроля доступа может сформировать решение в соответствии со своими собственными внутренними правилами.

8 Разработка биометрических профилей на базе биометрических стандартов

8.1 Взаимосвязь базовых биометрических стандартов и их использование в биометрических профилях

Цель данного раздела – описание и разъяснение взаимосвязей, которые существуют между базовыми стандартами в области биометрии, и общее описание применения базовых биометрических стандартов при разработке биометрических профилей, которые используются для обеспечения функционального взаимодействия и обмена данными между биометрическими приложениями и системами.

На рисунке 4 представлены три класса стандартов, которые могут понадобиться для успешного внедрения профиля приложения. Каждый класс представляет собой совокупность базовых биометрических стандартов в определенной области. Вводя в действие биометрический профиль, необходимо иметь представление о взаимосвязях, которые существуют между соответствующими базовыми биометрическими стандартами. Следует отметить, что, хотя и поощряется использование базовых стандартов всех классов для обеспечения лучшего взаимодействия, но в некоторых случаях может оказаться желательным использование не всех классов для биометрической системы. Более того, необходимо помнить, что некоторые базовые стандарты могут принадлежать не к одному только классу, то есть может иметь место наложение функций различных классов стандартов.

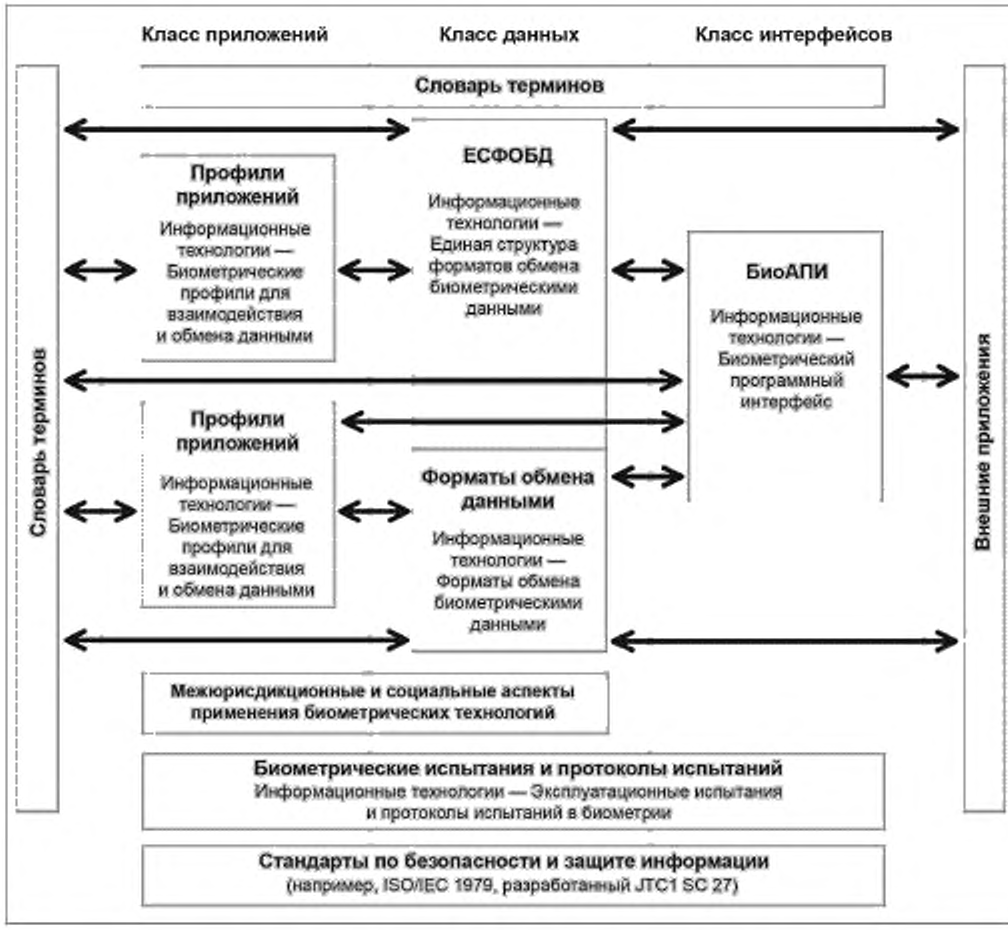

Рисунок 4 — Взаимосвязь базовых биометрических стандартов

8.2 Группы стандартов

8.2.1 Класс приложений

Класс приложений — главный класс всех базовых биометрических стандартов, определяющих конкретное приложение или сценарий использования биометрической системы. Данный класс является базовым для профилей приложений вместе с базовыми стандартами по терминологии, межюрисдикционным и социальным аспектам, по биометрическим испытаниям и протоколам испытаний, а также со стандартами по безопасности и защите информации. Данный класс базовых стандартов обслуживает область приложения внутри стандартизованной биометрической системы. Для нестандартизированных в части приложений систем данный класс может оказаться избыточным, так как в части, касающейся внешних приложений, можно использовать только класс (или классы) стандартов, определяющих структуру и формат данных и/или интерфейс.

8.2.2 Класс данных

Класс данных — главный класс всех базовых биометрических стандартов, определяющих конкретную систему или структуру данных для биометрической системы. Данный класс включает все стандарты на форматы обмена данными и стандарты ЕСФОБД. Данный класс тесно взаимодействует с базовыми стандартами по терминологии, межюрисдикционным и социальным аспектам, по биометрическим испытаниям и протоколам испытаний, а также со стандартами по безопасности и защите информации. Класс данных может быть использован для внешних приложений или применительно к интерфейсам, данный класс может быть использован прямо или опосредованно каким-либо стандартом, относящимся к классу приложений или интерфейсов.

8.2.3 Класс интерфейсов

Класс интерфейсов — главный класс всех базовых биометрических стандартов, определяющих конкретный интерфейс или методологию связей для биометрической системы. Данный класс тесно взаимодействует с базовыми стандартами по терминологии, межюрисдикционным и социальным аспектам, по биометрическим испытаниям и протоколам испытаний, а также со стандартами по безопасности и защите информации. К данному классу относятся стандарты, востребованные биометрическими системами, использующими стандартизированные интерфейсы как высокого, так и низкого уровня. Класс интерфейсов может быть использован как для внешних приложений, так и прменительно к интерфейсам, в некоторых случаях — исключая использование каких-либо иных стандартов.

8.3 Использование базовых биометрических стандартов для разработки биометрических профилей

Биометрические профили представляют собой значимый уровень стандартизации, который призван облегчить обеспечение биометрической совместимости. Биометрические профили предписывают, какие базовые стандарты следует применять, и какие опции и диапазоны возможных значений, описанные в данных базовых стандартах, необходимы и достаточны, чтобы обеспечить биометрическое взаимодействие для определенного набора функций приложения.

Первая задача, которую выполняет биометрический профиль, — определение и задание биометрических функций для своего применения. Типичными биометрическими функциями являются: регистрация, верификация и идентификация (5.3). В контексте заданных биометрических функций биометрический профиль определяет и устанавливает свои прикладные функции. Например, если областью применения биометрического профиля является управление пассажиропотоком при пересечении государственной границы, то функции управления включали бы: контроль, предшествующий приезду, контроль прибытия, пребывания, отбытия, а также сверку/управление базой данных. На основании конкретного перечня биометрических функций и прикладных функций биометрический профиль устанавливает, какие необязательные требования одного или нескольких базовых биометрических стандартов будут обязательными для данного биометрического профиля. Рисунок 5 иллюстрирует использование различных групп базовых стандартов для разработки биометрических профилей.

Для обеспечения взаимодействия между системами в любом конкретном прикладном профиле определенные режимы и/или процессы могут быть прописаны как обязательные. В зависимости от профиля приложения, может потребоваться использование определенного режима (формата обмена данными) или может быть использован некий набор режимов (в рамках определенного режима можно использовать более одного формата обмена данными).

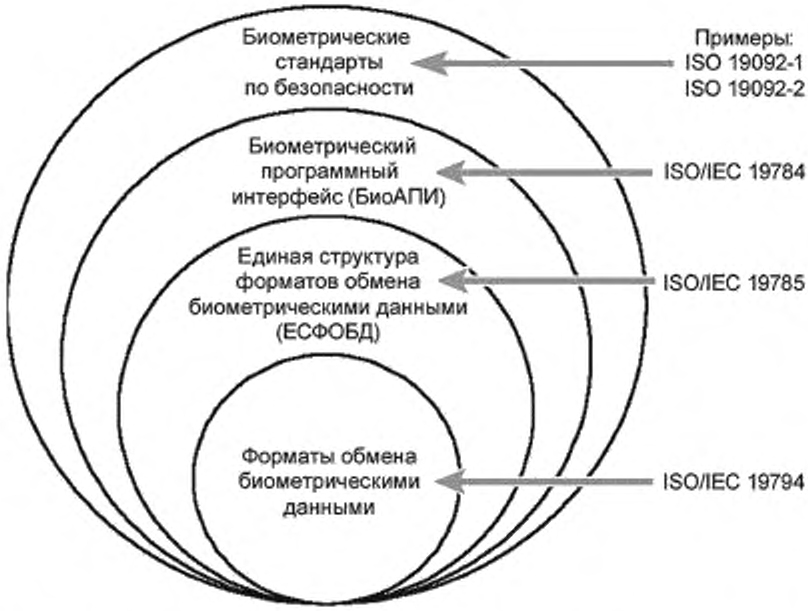

Рисунок 5 — Основные базовые стандарты для разработки биометрических профилей

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов межгосударственным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего межгосударственного стандарта
ISO/IEC 19794-1:2006	IDT	ГОСТ ISO/IEC 19794-1—2015 «Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 1. Структура»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: - IDT — идентичные стандарты.		

Библиография

[1]	ISO/IEC 7816-11:2004	Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods
[2]	ISO/IEC 19784-1:2006	Information technology — Biometric application programming interface — Part 1: BioAPI specification
[3]	ISO 19092:2008	Financial services — Biometrics — Security framework
[4]	ISO/IEC 19795-1:2006	Information technology — Biometric performance testing and reporting — Part 1: Principles and framework
[5]	ISO/IEC TR 24714-1	Cross-jurisdictional and societal aspects of implementation of biometric technologies — Part 1: Guide to the accessibility, privacy and health and safety issues in the deployment of biometric systems for commercial application
[6]	ISO/IEC 19785-1:2006	Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification
[7]	NISTIR 6887 (GSC-IS)	Government Smart Card Interoperability Specification
[8]	SIA AC-01-1996.10	Access Control Standard Protocol for the 26-bit Wiegand TM Reader Interface

УДК 004.93'1:006.89:006.354 МКС 35.040 IDT

Ключевые слова: информационные технологии, профили биометрические, обмен данными, общая архитектура, биометрическая система

Редактор *Л.В. Коретникова*
Технический редактор *И.Е. Черепкова*
Корректор *С.И. Фирсова*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 10.10.2018. Подписано в печать 30.10.2018. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 2,79. Уч.-изд. л. 2,51.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ» для комплектования Федерального информационного фонда стандартов, 117418 Москва, Нахимовский пр-т, д. 31. к. 2.

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

gost.e-ecolog.ru