ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 54412— 2019 (ISO/IEC TR 24741:2018)

Информационные технологии

БИОМЕТРИЯ

Общие положения и примеры применения

(ISO/IEC TR 24741:2018, Information technology — Biometrics — Overview and application, MOD)

Издание официальное

Москва
Стандартинформ
2019

Предисловие

1 ПОДГОТОВЛЕН Акционерным обществом «Всероссийский научно-исследовательский институт сертификации» (АО «ВНИИС») и Некоммерческим партнерством «Русское общество содействия развитию биометрических технологий, систем и коммуникаций» (Некоммерческое партнерство «Русское биометрическое общество») на основе собственного перевода на русский язык англоязычной версии документа, указанного в пункте 4, при консультативной поддержке Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)» (МГТУ им. Н.Э. Баумана)

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 19 ноября 2019 г. № 1184-ст

4 Настоящий стандарт является модифицированным по отношению к международному документу ISO/IEC TR 24741:2018 «Информационные технологии. Биометрия. Обзор и применение» (ISO/IEC TR 24741:2018 «Information technology — Biometrics — Overview and application», MOD) путем изменения отдельных фраз (слов, значений показателей, ссылок), которые выделены в тексте курсивом. Внесение указанных технических отклонений направлено на учет потребностей национальной экономики Российской Федерации.

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2012 (пункт 3.5).

Сведения о соответствии ссылочных национальных и межгосударственных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном документе, приведены в дополнительном приложении ДА.

Сопоставление структуры настоящего стандарта со структурой примененного в нем международного документа приведено в дополнительном приложении ДБ

5 ВЗАМЕН ГОСТ Р 54412—2011/ISO/IEC/TR 24741:2007

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 статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

Биометрическое распознавание представляет собой автоматическое распознавание индивидов, основанное на их биологических и поведенческих характеристиках. Данная сфера является составной частью более широкой области науки об идентификации человека. К технологиям распознавания человека относят распознавание по отпечаткам пальцев, изображению лица, геометрии кисти руки, голосу, радужной оболочке глаза (РОГ), сосудистому руслу, ДНК и т. д.

Некоторые технологии (например, распознавание по РОГ) в большей степени основаны на биологических характеристиках, а некоторые (например, распознавание по динамике подписи) — на поведенческих характеристиках, но в то же время во всех техниках распознавания присутствуют как биологические, так и поведенческие элементы. Не существует полноценных поведенческих или биологических биометрических систем.

Биометрическое распознавание часто называют биометрией, несмотря на то что этот более современный термин ранее употреблялся в контексте статистического анализа общих биологических данных. Термин «биометрия», так же как и термин «генетика», часто воспринимается как моноструктура. Впервые термин «биометрия» появился около 1980 г. в словаре физической и информационной безопасности, заменив термин «автоматическая идентификация личности», который существовал в 70-х гг. XX в. Биометрические системы распознают личности посредством распознавания тел. Для осознания характерных для данных технологий функциональных возможностей и ограничений существенное значение имеет отличие между личностью и телом. В общем случае биометрия представляет собой распознавание поведения человека и биологических структур при помощи компьютерных технологий и больше связана с вычислительной техникой и анализом статистических эталонов, чем с науками о поведении и биологией.

В настоящее время биометрия применяется для распознавания личности во многих сферах деятельности, таких как контроль физического доступа и доступа к компьютеру, в правоохранительных органах, при голосовании, пересечении границы, в кредитно-финансовой сфере, в системе социального обеспечения и при выдаче водительских прав.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

БИОМЕТРИЯ

Общие положения и примеры применения

Information technology. Biometrics. General provisions and examples of application

Дата введения — 2020—06—01

1 Область применения

В настоящем стандарте описаны история биометрии, функции биометрии, различные современные биометрические технологии (например, распознавание по отпечаткам пальцев и изображению лица), а также типовая архитектура биометрических систем и системных процессов, которые позволяют автоматизировать распознавание с использованием этих технологий.

В настоящем стандарте также содержится информация о применении биометрии в различных сферах, например при пограничном контроле, в правоохранительных органах и при выдаче водительских прав, а также о социальных и юридических аспектах, которые, как правило, учитываются в биометрических системах, и о стандартах, лежащих в основе их использования.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ ISO/IEC 2382-37 Информационные технологии. Словарь. Часть 37. Биометрия

ГОСТ Р 58293 (ИСО/МЭК 19785-1:2015) Информационные технологии. Единая структура форматов обмена биометрическими данными. Часть 1. Спецификация элементов данных

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую ссылку этого стандарта с учетом всех внесенных в данную версию изменений. Если изменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте отсутствуют термины и определения.

Издание официальное

4 Введение и основные понятия

4.1 Что такое биометрические технологии?

В соответствии с *ГОСТ ISO/IEC 2382-37* биометрия — это автоматическое распознавание индивидов, основанное на их биологических и поведенческих характеристиках.

Примечание — Всеобъемлющий термин «биометрия» означает применение к биологии современных методов статистики. В настоящем стандарте под биометрией понимаются автоматизированные технологии, предназначенные для анализа человеческих характеристик в целях распознавания; общее применение статистики к биологическим системам является отдельной дисциплиной.

Под термином «биометрическая характеристика» понимают биологическую и поведенческую характеристику индивида, которая может быть использована в качестве отличительных повторяющихся биометрических признаков для биометрического распознавания. Таким образом, биометрические технологии связаны с физическими частями человеческого тела или поведенческими чертами людей, а также с распознаванием индивидов, основанным на одной или на обеих этих частях или чертах. Более полное объяснение различных биометрических технологий приведено в разделе 6.

Примечание — В *ГОСТ ISO/IEC 2382-37* рекомендовано переводить термин «biometric» как «биометрический», а не «биометрика» для обозначения биометрической характеристики или биометрической модальности.

Совершенная биометрическая характеристика для всех применений обладает следующими свойствами:

- отличительность: разная для всех субъектов;
- повторяемость: одинаковая для каждого субъекта в течение длительного периода времени (несколько лет);
- доступность: легко предъявить устройству сбора биометрических данных/биометрическому сканеру;
- универсальность: наблюдаемая у всех людей;
- приемлемость: субъект готов использовать эту биометрическую характеристику в данном приложении.

Ни одна биометрическая характеристика не обладает всеми вышеперечисленными свойствами, и на практике приходится идти на компромисс по каждому пункту:

- существуют большие сходства между разными индивидами;
- биометрические характеристики меняются с течением времени;
- некоторые физические ограничения препятствуют биометрическому предъявлению;
- не все люди имеют все биометрические характеристики;
- приемлемость зависит от сознания субъекта.

Следовательно, задача широкого внедрения биометрических технологий заключается в разработке надежных систем для взаимодействия с людьми с учетом особенностей их поведения.

4.2 Что делают биометрические системы?

Начиная с 1970 г. установлено, что для некоторых приложений существует три принципа автоматического распознавания личности [1]:

а) что вы знаете или помните (например, ФИО, данные паспорта, дата рождения и т. д.);

б) чем вы владеете (например, электронно-цифровая подпись, идентификационная карта, токен и т. д.);

с) личная биометрическая характеристика.

Первоначальным контекстом этой концепции было безопасное управление доступом к компьютерным данным. Исходные предположения заключались в том, что лица, уполномоченные осуществлять доступ к защищенным данным, будут кооперативно предъявлять положительные заявления (например, «я уполномочен осуществить доступ к данным в системе») и могут рассчитывать на защиту своих персональных идентификационных номеров (ПИН-кодов) и паролей. В таких приложениях биометрические технологии действительно конкурируют с ПИН-кодами, паролями и токенами, но получают меньшее признание. Например, для большинства веб-систем управления доступом требуется идентификатор пользователя и соответствующий пароль, а не биометрия. В подобных приложениях пароли были более распространены, чем биометрия, потому что они легко заменяются, могут варьироваться в зависимости от приложений, не требуют специального оборудования для сбора данных, могут быть созданы с различными уровнями безопасности и точно повторяются под сознательным контролем.

Однако во многих приложениях ПИН-коды, пароли и токены не могут логически соответствовать требованиям безопасности. Например, ПИН-коды, пароли и токены не могут быть логически применены в приложениях, где зарегистрированные индивиды имеют мало мотивации для защиты своих счетов от использования другими лицами, например в парках развлечений. Аналогичным образом в тех приложениях, в которых предъявляются отрицательные заявления (например, «я не зарегистрирован в системе как *Иван*»), ПИН-коды, пароли и токены не могут логически соответствовать требованиям демонстрации истинности заявления.

В биометрических системах распознавание людей происходит путем наблюдения за физическими и поведенческими характеристиками их тел. Биометрические характеристики не так просто передать, забыть или украсть в отличие от ПИН-кодов, паролей и токенов, поэтому их можно использовать в тех приложениях, для которых эти методы аутентификации неуместны. Биометрия может быть объединена с ПИН-кодами и токенами в рамках многофакторных систем для дополнительной безопасности.

Хотя биометрические технологии не могут непосредственно идентифицировать людей, они могут связывать тела с записями атрибутов, которые называют «идентичности». Следовательно, биометрическое распознавание может стать частью системы управления идентификацией.

Биометрическое распознавание использовано в двух основных классах приложений:

- в одном применено биометрическое сравнение для проверки биометрического «удостоверения личности»;
- в другом осуществлен поиск в базе данных биометрических характеристик заранее известных индивидов, для того чтобы найти и возвратить идентификатор, относящийся к одному индивиду.

Первый класс приложений называют «биометрическая верификация», а второй — «биометрическая идентификация». Биометрические системы могут быть также использованы для «кластеризации» характеристик, обозначая совместно те, которые поступают из одного и того же телесного источника, даже если телесный источник не может быть приписан какому-либо заранее известному индивиду. Такие системы находят все большее применение в правоохранительных органах.

Системы биометрической верификации подтверждают заявления (тестовые гипотезы), относящиеся к источнику записи биометрических данных в базе данных. Заявление может быть сделано лицом, представляющим биометрическую выборку (например, «я являюсь источником записи биометрических данных в базе данных»), или заявление об источнике может быть сделано другим субъектом в системе («она является источником записи биометрических данных в базе данных»). Заявления могут быть положительными («я являюсь источником биометрической записи в базе данных»; «эти два биометрических образца взяты от одного и того же телесного источника») или отрицательными («я не являюсь источником записи биометрических данных в базе данных»). Заявления могут быть определенными («я являюсь источником записи биометрических данных в базе данных») или неопределенными («я не являюсь источником записи биометрических данных в базе данных»). Заявление может представлять собой любую комбинацию определенных или неопределенных, положительных или отрицательных заявлений, заявлений от первого или от третьего лица.

Согласно *ГОСТ ISO/IEC 2382-37* запись биометрических данных индивида в базе данных называется биометрическим контрольным шаблоном, а биометрический образец, используемый для сравнения с сохраненным биометрическим контрольным шаблоном, — биометрической пробой. Можно искать совпадение между биометрической пробой индивида и определенным биометрическим контрольным шаблоном, хранящимся в базе данных, или совокупность биометрических контрольных шаблонов в базе данных, совпадающих с представленной биометрической пробой, и возвращать идентификатор любого совпавшего биометрического контрольного шаблона. В обоих случаях необходимо установить порог, указывающий, насколько близким должно быть сравнение, прежде чем можно будет заключить, что биометрическая проба и биометрический контрольный шаблон зарегистрированы от одного и того же телесного источника (совпадение). При этом могут быть допущены следующие ошибки: либо ложное несовпадение, в том случае когда совпадение не объявляется, а биометрическая проба и биометрический контрольный шаблон действительно зарегистрированы от одного телесного источника, или ложное совпадение, когда совпадение объявляется, а биометрическая проба и биометрический контрольный шаблон зарегистрированы от различных телесных источников. О доле таких ошибок судят по общему количеству сравнений, вероятности ложного совпадения (ВЛС) и вероятности ложного несовпадения (ВЛНС) для данной технологии и совокупности в данной среде приложения.

Системы, требующие положительного заявления для конкретного зарегистрированного биометрического контрольного шаблона, рассматривают биометрический контрольный шаблон как атрибут записи о регистрации. Эти системы подтверждают, что биометрический контрольный шаблон в заявленной записи о регистрации совпадает с образцом биометрической пробы, представленным субъектом. Некоторые системы, например социального обеспечения и выдачи водительских прав, подтверждают отрицательные заявления об отсутствии записи биометрических данных в базе данных, рассматривая биометрический контрольный шаблон в качестве идентификатора записи или указателя. Эти системы осуществляют поиск в базе данных биометрических указателей, для того чтобы найти один, соответствующий представленной биометрической пробе (в этом случае речь идет о биометрической идентификации). Однако факт нахождения идентификатора (или указателя) в списке идентификаторов также подтверждает неопределенное заявление о регистрации в базе данных, а отсутствие указателя — отрицательное заявление о регистрации. Следовательно, различие между биометрическими системами идентификации и верификации не всегда четкое, и эти термины не являются взаимоисключающими.

В простейших системах подтверждение положительного заявления о конкретной записи регистрации может потребовать сравнения представленной биометрической пробы с единственным биометрическим контрольным шаблоном в одной заявленной записи.

Например, субъект может заявить о том, что он является источником биометрических данных отпечатков пальцев, хранящихся на иммиграционной карте. Для того чтобы подтвердить это заявление, субъект вставляет карту в считыватель карт, который считывает запись биометрического контрольного шаблона, а затем помещает палец на устройство считывания отпечатков пальцев. В системе осуществляется сравнение биометрических характеристик отпечатка пальца, полученных с устройства считывания отпечатков пальцев, с характеристиками биометрического контрольного шаблона, записанными на карте. В соответствии с установленными порогами система может сделать вывод о том, что субъект действительно является источником биометрического контрольного шаблона, хранящегося на карте, и поэтому ему должны быть предоставлены права и привилегии, связанные с картой. При этом предполагается, что карта не была подделана. С помощью биометрической верификации можно определить только то, что человек предъявил биометрические характеристики, которые близки к совпадению с теми, что записаны на карте.

Простая биометрическая идентификация может потребовать сравнения представленного биометрического образца со всеми биометрическими контрольными шаблонами, хранящимися в базе данных. Штат Калифорния требует от заявителей на получение социальных пособий подтверждения отрицательного заявления, касающегося отсутствия ранее зарегистрированной личности в системе, с помощью отпечатков пальцев с обоих указательных пальцев. В зависимости от конкретной стратегии автоматического поиска, поиск отпечатков пальцев может осуществляться по всей базе данных зарегистрированных получателей пособий, для того чтобы убедиться в том, что в системе отсутствуют совпадающие отпечатки пальцев, или, возможно, только по части базы данных, соответствующей субъектам того же пола, что и заявитель. При совпадении отпечатков пальцев запись регистрации, указывающая на эти отпечатки пальцев, возвращается к системному администратору для подтверждения отклонения заявления об отсутствии ранее регистрации.

Количество сравнений и вероятности того, что эти сравнения приведут к совпадению (определят, что биометрическая проба и биометрический контрольный шаблон имеют одинаковый телесный источник), будут зависеть как от заявления, так и от архитектуры системы. Риски безопасности, связанные с неправильными результатами, также зависят от функций системы. Следовательно, некоторые системы очень чувствительны к ложным совпадениям (ложноположительный результат), а другие — к ложным несовпадениям (ложноотрицательный результат) для любого сравнения. В зависимости от заявления ложноположительный или ложноотрицательный результат может привести либо к ложному принятию, либо к ложному отклонению заявления.

5 История

На неавтоматизированном уровне биометрические характеристики применялись веками. Части тела и особенности поведения людей для распознавания использовались с незапамятных времен и продолжают использоваться в настоящее время. Отпечатки пальцев применялись еще в древнем Китае; люди часто помнят и узнают других людей по их лицам, голосам, а подпись является общепринятым методом идентификации в банковской системе, при легитимизации документов и во многих других сферах деятельности.

Современное учение о распознавании личности, основанное на физических измерениях, многим обязано служащему полиции Альфонсу Бертильону, который начал свою работу в конце 70-х гг. XIX в. [2]. Система Бертильона включала в себя измерение несколько величин: рост, вес, длина и ширина головы, ширина щек, длина туловища, стоп, ушей, предплечья, средних пальцев и мизинцев. Также в систему входили категории цвета и узора РОГ. До 80-х гг. XIX в. система Бертильона применялась во Франции для идентификации рецидивистов. Некоторое время спустя система стала использоваться в США для идентификации заключенных вплоть до 20-х гг. XX в.

Несмотря на то что исследования отпечатков пальцев начались еще в конце 50-х гг. XIX в., эти знания оставались неизвестными в западном мире до 80-х гг. XIX в. [3], [4], до тех пор пока не стали пропагандироваться сэром Фрэнсисом Гальтоном в научных работах (1888 г.) [5] и Марком Твеном в литературе (1893 г.) [6]. Работы Ф. Гальтона также включали в себя технологию идентификации личности по характеристикам лица.

К середине 20-х гг. XX в. дактилоскопия полностью вытеснила систему Бертильона в Бюро расследований США (вскоре сменившееся Федеральным бюро расследований, ФБР). Впрочем, исследования новых методов идентификации личности продолжались только в научном мире. Анализ почерка как метод признан в 1929 г. [7], а идентификация личности по сетчатке глаза — в 1935 г. [8]. Однако к этому времени ни один из данных методов не был автоматизирован.

Эксперименты в области автоматического распознавания диктора с использованием аналоговых фильтров начались в 40-х гг. XX в. [9] и начале 50-х гг. XX в. [10]. В 1960-х гг. во время набирающей скорость революции в вычислительной технике распознавание образцов голоса [11] и отпечатков пальцев [12] считалось первоочередным применением автоматической обработки сигнала. В 1963 г. начал формироваться широкий и разнообразный рынок систем с использованием автоматического распознавания личности по отпечаткам пальцев, которые в перспективе могли бы применяться в кредитных системах, в системах промышленной и военной безопасности и для защиты персональных данных [13]. Вскоре начались исследования по распознаванию лица с использованием вычислительной техники [14], [15]. В 70-х гг. XX в. зарегистрированы первые действующие системы идентификации по отпечатку пальца и геометрии контура кисти руки, доложены результаты официальных испытаний биометрических систем [16], проанализированы характеристики приборов, входящих в состав биометрических систем [17], [18], и опубликованы рекомендации государства по проведению испытаний [19].

Параллельно с развитием технологии идентификации по геометрии контура кисти руки в 60-е и 70-е гг. прошлого столетия быстрыми темпами развивалась дактилоскопическая биометрия. В течение этого времени многие организации с целью содействия сотрудникам правоохранительных органов подключились к разработке технологии автоматической идентификации по отпечаткам пальцев, потому что сравнение отпечатков пальцев с существующими в досье преступников происходило в лабораториях вручную, требовало большого штата и отнимало слишком много человеко-часов. В различных системах идентификации по отпечаткам пальцев, разработанных в 60-х и 70-х гг. XX в. для ФБР, уровень автоматизации был уже значительно выше, но все эти системы были рассчитаны только на сравнение отпечатков пальцев с участием подготовленных экспертов. Автоматизированные дактилоскопические информационные системы (АДИС) впервые были применены в конце 70-х гг. прошлого столетия, из них следует отметить АДИС Канадской королевской конной полиции, применявшуюся начиная с 1977 г. С тех пор роль биометрии в правоохранительных органах значительно возросла, а АДИС применяют в подавляющем большинстве правоохранительных подразделений по всему миру. Сегодня АДИС может приобретать и гражданское население.

В Российской Федерации с 2006 г. применяется система автоматизированных банков данных дактилоскопической информации (АДИС-МВД). Оператором АДИС-МВД является Министерство внутренних дел Российской Федерации. Данная система осуществляет формирование и ведение на базе органов внутренних дел информационных дактилоскопических массивов, полученных в процессе проведения государственной дактилоскопической регистрации, и информации о следах рук неустановленных лиц, изъятых с мест преступлений, а также обеспечивает информационное обеспечение правоохранительных органов при использовании функций по предупреждению, пресечению, выявлению, раскрытию и расследованию преступлений, предупреждению и выявлению административных правонарушений, розыску пропавших без вести, установлению по неопознанным трупам личности человека, установлению личности граждан Российской Федерации, иностранных граждан и лиц без гражданства, граждан, не способных по состоянию здоровья или возрасту сообщить данные о своей личности [20].

В 80-х гг. XX в. системы сканирования и распознавания отпечатков пальцев, а также системы распознавания диктора стали устанавливаться на персональные компьютеры для контроля доступа субъектов к хранящейся на них информации. Системы распознавания личности по РОГ, основанные на концепции, которая запатентована в 80-х гг. XX в. [21], стали доступны в середине 90-х гг. [22]. В настоящее время существует более десяти различных подходов, использующихся в доступных для приобретения систем, включающих в себя распознавание личности по геометрии контура кисти руки и пальца, паттернам РОГ и отпечатка пальца, изображениям лица, голосу, динамике подписи, работы на клавиатуре, паттернам вен руки/пальца.

Современные системы биометрической верификации по голосу во многом обязаны технологическим достижениям 60-х гг. XX в., в то время как биометрические технологии, основанные на распознавании РОГ, вен пальца и лица, являются сравнительно новыми технологиями. Во всем мире исследования университетов и поставщиков биометрических услуг для улучшения работы уже существующих биометрических технологий считаются намного важнее, чем развитие новых и более разнообразных технологий. Самой сложной частью процесса является выведение системы на рынок и подтверждение ее эксплуатационных характеристик. Для превращения лабораторной технологии в полноценно работающую систему требуется время. Впрочем, такие системы уже сейчас применяются в самых разных сферах и успешно доказывают свою работоспособность.

6 Обзор биометрических технологий

6.1 Технологии, построенные на анализе изображения глаза

6.1.1 Распознавание радужной оболочки глаза

Технология распознавания РОГ доступна в широком числе коммерческих приложений, а также успешно используется при пересечении границы, в программах лояльности и при контроле доступа. Распознавание РОГ успешно используется в приложениях контроля доступа без необходимости получения запроса идентификации или удостоверения личности от субъекта данных. Субъекту данных может быть разрешен доступ к системе путем его поиска во всей базе данных зарегистрированных лиц. Технологии различаются в зависимости от производителя; в некоторых системах получают изображения одного глаза, а в некоторых — обоих глаз одновременно. В настоящий момент существуют технологии, которые позволяют получать изображения РОГ с расстояния более 1 м или изображения РОГ людей, проходящих через терминал.

В большинстве реализаций изображение РОГ в оттенках серого получают в инфракрасном (ИК) спектре для повышения детализации изображений глаз всех цветов. Для обеспечения сужения зрачка в целях увеличения площади РОГ получение изображения должно быть осуществлено в хорошо освещенном помещении. Контактные линзы без рисунка и очки несущественно влияют на сбор изображений РОГ. Солнечные очки, однако, не должны применяться, так как они могут повлиять на процесс сбора изображений РОГ. Компьютерные алгоритмы разворачивают эти изображения, для того чтобы сформировать прямоугольную матрицу пикселей, по которым фильтр меньшего размера размещается в нескольких местах. Фильтр представляет собой гладкую волну с частотой и направлением. В каждом месте размещения фильтра фаза такой же частоты и направления на изображении РОГ наблюдается относительно фильтра и используется для создания паттернов 0s и 1s. 0s и 1s являются признаками РОГ и напрямую не представляют какие-либо видимые элементы РОГ, такие как углубления, нити, ямки. Признаки двух паттернов РОГ сравнивают путем подсчета процентов 0s и 1s, которые совпадают по длине этого двоичного вектора. Такой подсчет процентов может быть выполнен с помощью компьютера на битовом уровне с наибольшей эффективностью. Если $^2/_3$ из 0s и 1s совпадают, то считается, что паттерны собраны от одного и того же глаза. Значение $^2/_3$ представляет порог, который может изменяться для достижения баланса ложноположительных и ложноотрицательных результатов.

6.1.2 Распознавание сетчатки

Сетчатка — это светочувствительный слой нервов и кровеносных сосудов на внутренней оболочке глаза. В течение 80-х и 90-х гг. XX в. системы распознавания по сетчатке, которые формируют рисунок вен на сетчатке, были коммерчески доступными. Такие системы не исследовали изображения рисунка вен на сетчатке, а сканировали с помощью ИК-луча круговую область над сетчаткой и записывали интенсивность возвращенного света. В результате получался одномерный паттерн с большими значениями отраженного света на тех участках сетчатки, на которых отсутствуют кровеносные сосуды, и низкими значениями отраженного света на тех участках сетчатки, на которых кровеносные сосуды поглотили ИК-луч. Несмотря на слухи никакой информации о состоянии здоровья в этих паттернах не содержалось, а также никакой лазерный луч не использовался. Из-за требования использования ИК-луча низкой интенсивности для подсветки задней поверхности глаза субъекты данных должны были смотреть в сканер на очень близком расстоянии, т. е. в тесном контакте с устройством. На сегодняшний день устройства распознавания сетчатки не представлены на рынке.

6.2 Технологии, построенные на анализе изображения лица

Автоматическая идентификация личности с помощью анализа изображения лица является сложной процедурой, для которой требуются разнообразные алгоритмические подходы. Рядом биометрических разработчиков и исследовательских институтов разработаны системы распознавания лица, в которых для регистрации изображений лица в видимой, ближней ИК или дальней ИК (тепловизионной) области спектра используются цифровые фотографии или видеоизображение.

Алгоритмы, как правило, начинают процесс идентификации с повышения качества и нормализации изображения: обнаружения центров глаз, преобразования изображения лица до полной фронтальной ориентации, корректировки теней и т. д. На нормализованном изображении доступны к применению разнообразные методы обработки для извлечения абстрактных измерений из изображения путем размещения фильтров над всем изображением лица или его частями. Извлеченные признаки изображения лица являются абстрактными мерами, не связанными непосредственно с расстояниями между особыми точками на лице, такими как нос, рот и уши. Однако данные меры должны быть как стабильными (не сильно изменяющимися для каждого человека от изображения к изображению), так и отличительными (сильно различающимися между людьми).

При нынешнем уровне развития технология распознавания изображения лица может очень точно работать с высоким разрешением (более 100 пикселей между центрами глаз) и полным фронтальным изображением при хорошем освещении. Однако производительность снижается по мере уменьшения разрешения изображения или увеличения угла положения лица. Изменения освещения также вызывают снижение точности.

Трехмерные модели лица могут создаваться различными способами, такими как измерение расстояния лазером, проецирование сетки на лицо для определения искажений сетки из-за структуры лица, слияние нескольких изображений или использование информации о полутонах в отдельном изображении.

На тепловизионном изображении лица отображается количество тепла, вызванное притоком крови к лицу. Тепловизор регистрирует невидимый, вызванный теплом рисунок кровеносных сосудов, находящихся под кожей. Так как при сборе изображений лица ИК-камерами освещение не является необходимым, системы могут регистрировать изображения в темноте. Однако ИК-камеры являются более дорогими по сравнению с другими видами видеокамер, и системы распознавания лица, основанные на этой технологии, с 90-х гг. XX в. не представлены на рынке.

6.3 Технологии, построенные на анализе гребней отпечатка пальца и ладони

6.3.1 Построение изображения отпечатка пальца

Большинство систем распознавания отпечатков пальцев анализируют малые признаки папиллярных гребней на пальце, которые известны как минуции. Они определены как окончания гребней отпечатка пальца или бифуркации (разветвление гребней отпечатка пальца). Также могут быть проанализированы плотность изображения пальца или расстояние между гребнями.

Исторически сложилось так, что отпечатки пальцев собирались красковым методом путем оставления отпечатков пальцев, покрытых чернилами, на специальных картах. С появлением автоматического распознавания отпечатков пальцев эти карты были отсканированы на компьютер. В настоящий момент красковый метод сбора отпечатков пальцев устарел, отпечатки пальцев собираются в электронном виде путем размещения пальца на стеклянной поверхности, называемой рабочей поверхностью сканера отпечатков пальцев. Совсем недавно разработаны бесконтактные системы, которые используют лазер или стандартное освещение и при применении которых не требуется прикасаться к какой-либо поверхности.

Отпечатки пальцев, представляющие набор папиллярных гребней пальцев, могут варьироваться от экземпляра к экземпляру по многим причинам. Например, влажность пальцев, угол размещения, давление и повреждение гребня оказывают влияние на зарегистрированные изображения. Еще одним значимым фактором является то, каким образом субъект прикладывает палец к сканеру отпечатков пальцев, а именно — высота и угол наклона сканера отпечатков пальцев по отношению к субъекту данных. Поставщики принимают во внимание указанные выше проблемы, и таким образом сканеры отпечатков пальцев проектируются с учетом эргономических требований для оптимизации процесса получения отпечатка пальца.

Основным различием между контактными технологиями распознавания отпечатков пальцев на рынке является способ получения изображения отпечатка пальца. В большинстве крупных систем получения изображений отпечатков пальцев используют оптический метод или электронное сканирование изображений с листа бумаги. Другие методы получения изображений отпечатков пальцев связаны с использованием емкостных, тепловизионных и ультразвуковых устройств.

В контактных системах распознавания отпечатков пальцев оптический метод получения изображения основан на концепции нарушения принципа полного внутреннего отражения. Стеклянная рабочая поверхность сканера отпечатков пальцев освещена снизу под предельным углом, при котором происходит полное внутреннее отражение. При отсутствии касаний рабочей поверхности сканера отпечатков пальцев весь свет отражается и попадает на светочувствительный датчик камеры. При касании гребнем пальца рабочей поверхности сканера отпечатков пальцев принцип внутреннего отражения нарушается, т. е. лучи света не отражаются, а проходят сквозь палец. Следовательно, полученное изображение отпечатка пальца темное в тех местах, где есть гребни, и светлое в тех местах, где есть впадины, что повторяет рисунок, полученный с помощью традиционного краскового метода.

В емкостных датчиках отпечатков пальцев рабочая поверхность сканера отпечатков пальцев состоит из блока маленьких ячеек, размер каждой из которых меньше, чем ширина гребня отпечатка пальца. Измерение емкостного сопротивления ячеек в массиве показывает, где гребни пальцев соприкасаются с датчиком, генерируя изображение отпечатка пальца.

Тепловой метод заключается в использовании технологии кремниевого чипа для получения данных отпечатка пальца, в то время как субъект двигает пальцем по датчику. При этом регистрируются колебания температуры между гребнями и впадинами, которые затем преобразуются в черно-белое изображение.

Ультразвуковой метод построения изображения отпечатка пальца заключается в использовании звуковых волн, которые недоступны для человеческого слуха. Палец размещается на сканере отпечатков пальцев, и происходит измерение плотности образца отпечатка пальца с помощью акустических волн.

Отпечатки пальцев могут быть получены по одному или в комбинации двух или четырех пальцев. После получения изображений четырех пальцев (от указательного до мизинца) обеих рук получают изображения больших пальцев (по одному от каждой руки) для создания изображения всех десяти пальцев. В крупномасштабных системах идентификации людей регистрируют с помощью оптического метода получения изображений отпечатков нескольких пальцев в реальном времени, часто воспринимаемых как изображения четырех пальцев (от указательного до мизинца), описанные выше. АДИС правоохранительных органов, также известные как станции регистрации, собирают все десять отпечатков пальцев и зачастую в электронном виде. АДИС, применяемые в гражданских целях, не собирают все десять отпечатков пальцев и эффективно работают при наличии одного или двух отпечатков.

Независимо от используемой технологии построения изображений отпечатков пальцев сканер отпечатков пальцев формирует матрицу чисел, каждое из которых соответствует пикселю, представляющему отпечаток пальца. Стандартное разрешение для изображений отпечатков пальцев составляет 500 пикселей/дюйм. Числа в матрице, как правило, находятся в диапазоне от 0 (темный) до 255 (светлый), но некоторые неоптические сканеры на выходе могут давать только матрицу, состоящую из 0s и 1s.

6.3.2 Сравнение отпечатков пальцев

6.3.2.1 Есть много способов сравнить отпечатки пальцев численно (слово «численно» используется для того, чтобы исключить методы оптического сравнения, которые были разработаны в 60-х и 70-х гг. XX в. и не рассматриваются в настоящем стандарте). Основными численными подходами являются:

a) основанный на преобразовании;

b) локальная корреляция;

c) основанный на минуциях.

Данные подходы использованы в коммерческих системах, но подход, основанный на минуциях, является наиболее популярным.

6.3.2.2 Не существует двух одинаковых отпечатков пальцев, т. е. даже один и тот же палец, помещенный дважды на рабочую поверхность сканера отпечатков пальцев, будет оставлять два разных изображения структуры гребней. Ситуации, когда будут сравниваться два одинаковых отпечатка, даже если они получены с одного и того же пальца, не возникнет. Изменение отпечатков пальцев от одного и того же пальца называют вариативностью в пределах класса, которая имеет много причин:

a) рисунок гребней изменился из-за повреждения или ухудшения состояния кожи;

b) изменился уровень увлажненности пальца;

c) к рабочей поверхности биометрического сканера отпечатков пальцев приложено другое давление;

d) различная ориентация пальцев на рабочей поверхности биометрического сканера отпечатков пальцев по любой из трех осей;

e) изменения в устройстве построения изображения.

Учитывая данные обстоятельства, сравнение отпечатков пальцев происходит различными методами. В методах, основанных на преобразовании, как правило, задействованы двумерные преобразования Фурье и преобразования Хоу, применяемые к матрице пикселей, представляющей отпечаток пальца. Идея состоит в том, чтобы математически преобразовать изображение каким-то образом, а затем сравнить коэффициенты преобразованных изображений. В этом контексте признаками отпечатков пальцев являются коэффициенты преобразования. Был разработан стандарт для передачи и хранения отпечатков пальцев с использованием метода, основанного на преобразовании *(см. [23])*.

Методы, основанные на корреляции, учитывают, что отпечатки пальцев и их репрезентативные матрицы, полученные со сканера, не могут быть просто наложены из-за всех различий. Однако небольшие участки двух отпечатков пальцев при наложении могут быть коррелированы. Если геометрические отношения между центрами малых областей остаются примерно одинаковыми при наложении с целью максимизации корреляции между двумя изображениями, возможно, изображения относятся к одним и те же папиллярным гребням пальца.

Методы, основанные на минуциях, стремятся подражать тому, что делают судебно-медицинские эксперты. В этом контексте минуция гребня может быть двух типов: бифуркация или окончание. Минуции также имеют направление, связанное с гребнем в точке их возникновения. Математический алгоритм перемещается по изображению в поисках гребней, где они разделяются или заканчиваются, и составляет карту минуций. При сравнении двух отпечатков пальцев карты минуций располагают одну над другой и вращают/перемещают одну относительно другой. Если при этом получают некоторое количество минуций, совпавших по положению и направлению, то это считают совпадением.

6.3.3 Технологии, построенные на анализе изображения ладоней

Биометрия ладоней может быть поставлена в один ряд с биометрией отпечатков пальцев, особенно в технологии АДИС. Гребни, впадины и минуции есть как на отпечатках пальцев, так и на ладони. Они могут быть получены с использованием оптических методов так же, как и отпечатки пальцев. Данная область биометрической промышленности, в частности, ориентирована на правоохранительные органы, так как скрытые отпечатки ладоней так же крайне полезны при расследовании уголовных дел, как и отпечатки пальцев. Другая биометрия ладоней, основанная не на структуре папиллярных гребней, а на линиях ладони, разработана в лабораторных программах.

Характеристики биометрии ладоней преимущественно используются в идентификации «один ко многим», а процесс сбора биометрических данных по сути аналогичен оптическому методу регистрации отпечатков пальцев. Система регистрации отпечатка ладони собирает изображение ладони в тот момент, когда она находится на сканере. Скрытые и чернильные отпечатки ладоней также могут быть отсканированы и помещены в систему, как и в случае с АДИС.

6.4 Технологии, построенные на анализе геометрии контура кисти руки

Методы распознавания геометрии контура кисти руки широко использовались в приложениях контроля доступа с 80-х гг. XX в. При наиболее распространенном коммерческом подходе используется одно или несколько двумерных изображений контура кисти руки, которые обрабатывают с помощью проприетарного алгоритма для получения 9-байтного кода.

Субъект помещает кисть руки на отражающую рабочую поверхность сканера, выравнивая пальцы в соответствии со специально расположенными направляющими. Столик освещается ИК-светом и возвращает отраженный свет только там, где кисть руки не закрывает рабочую поверхность сканера, тем самым формируя изображение контура кисти руки. Зеркало отражает свет горизонтально через верхнюю часть кисти руки, формируя второе двумерное изображение контура обратной стороны кисти руки.

6.5 Технологии, построенные на анализе динамики подписи

Верификация динамики подписи (ВДП) основана на движениях кисти руки, производимых во время подписи. Важно отметить, что метод заключается не в анализе самой подписи, а в анализе процесса ее получения. Именно в этом отличие ВДП от анализа статичных подписей на бумаге. Технология разработана в 60-х гг. XX в. и является одной из старейших форм автоматического распознавания личности.

Данные о подписи могут быть получены при помощи чувствительного пера или электронного планшета. Суть первого метода заключается в наличии чувствительных элементов-датчиков внутри пера, а второй метод основан на том, что планшет регистрирует уникальные характеристики динамики подписи.

При помощи технологии ВДП можно извлечь и измерить ряд характеристик. Например, время, которое пишущий отводит на написание, скорость движения ручки и ускорение, силу, с которой пишущий держит ручку, и то, сколько раз ручка отрывалась от бумаги, — все эти показатели могут быть рассмотрены как уникальные поведенческие характеристики. Технология ВДП не основана на анализе статичного изображения, так что даже в том случае, если подпись скопирована, субъект подделки подписи должен знать о динамике ее изготовления.

Другим преимуществом биометрических технологий, построенных на анализе динамики подписи, является их распространенность в качестве метода подтверждения личности. Вместе с тем, технологии, построенные на анализе динамики подписи, применяются в тех ситуациях, когда необходимо наложить на человека юридические обязанности, например в случае подписания контракта. Вышеизложенные факторы привели к применению биометрии подписи в разных сферах деятельности — от проверки документов, предоставляющих право на социальное обеспечение, до управления документооборотом и использования электронной подписи.

6.6 Технологии, построенные на распознавании диктора

Распознавание диктора является биометрической технологией, построенной на анализе звучания голоса, которая отличается от распознавания диктора с похожей небиометрической технологией распознавания речи, используемой для распознавания слов при диктовке или автоматической обработке инструкций, переданных по телефону.

Звук человеческого голоса преимущественно является следствием резонанса, возникающего в речевом тракте. Особенности голоса определены длиной речевого тракта и формами ротовой и носовой полостей. В технологии измерения голоса может быть применен либо текстонезависимый, либо текстозависимый метод. Другими словами, при сборе образцов голоса можно использовать специально подготовленные вопросы, отвечая на которые субъект будет произносить определенный текст, сочетающий фразы, слова или цифры (текстозависимый метод), или может произносить любые фразы, слова или цифры без определенного задания (текстонезависимый метод).

Технологии распознавания диктора особенно полезны в приложениях, связанных с телефонами. Все люди разговаривают по телефону, поэтому биометрическая система может быть встроена в частную или общественную телефонную сеть. Однако на работу систем распознавания диктора влияют окружающие субъект шумы и помехи на линиях.

Субъект произносит в микрофон заранее подготовленную (текстозависимый метод) либо произвольную (текстонезависимый метод) фразу. Данный процесс обычно повторяют несколько раз во время регистрации, для того чтобы позволить системе сформировать подходящую модель голоса, основанную на биометрических признаках, таких как кепстральные коэффициенты, которые регистрируют резонансные характеристики голосового тракта.

6.7 Технологии, построенные на анализе рисунка сосудистого русла

Кровеносные сосуды (вены), которые находятся в подкожных областях человеческого тела, формируют уникальный рисунок для каждого человека. Более того, кровеносные сосуды находятся внутри человеческого тела, поэтому не могут быть легко получены другим человеком при помощи обычного фотоаппарата. Рисунок кровеносных сосудов может быть получен при помощи ИК-излучения, либо напрямую падающего на область, которая должна быть сфотографирована, либо проходящего через часть тела, изображение которой надо получить. Кровеносные сосуды поглощают ИК-излучение больше, чем окружающие их ткани, поэтому они выглядят более темными на полученном изображении. Рисунок кровеносных сосудов затем может быть извлечен и преобразован в контрольный биометрический шаблон или зарегистрированный биометрический образец для сравнения в биометрической системе.

В данной технологии выбирают такие части человеческого тела (ладонь, пальцы, запястье и тыльная сторона ладони), в которых присутствует уникальный рисунок кровеносных сосудов, следовательно, биометрический сканер может зарегистрировать эти данные.

6.8 Технологии, построенные на анализе динамики работы на клавиатуре

Динамика работы на клавиатуре является биометрической технологией, построенной на анализе ритма печати. Динамика работы на клавиатуре человека развивается со временем, так как он учится печатать на клавиатуре, тем самым развивая уникальные навыки печати. Алгоритмы должны учитывать тот факт, что субъекты могут отвлекаться или уставать от работы в течение дня, что заметно влияет на ритм печати.

6.9 Технологии, построенные на анализе запаха

Распознавание людей через их запах уже давно предлагается как технология, основанная на доказанных способностях собак в этой области. Хотя устройства еще коммерчески не реализованы, они находятся в стадии разработки. Устройство, чувствительное к запаху, формирует его на электронном датчике, содержащем белки, которые реагируют на специфические молекулы запаха. Изменения в пропорциях различных молекул могут быть достаточно значимыми для осуществления распознавания.

6.10 Технологии, построенные на анализе ДНК

Есть много типов полуавтоматического анализа ДНК, некоторые из них занимают всего 15 мин. Учитывая достаточное количество локусов, с помощью анализа ДНК невозможно только идентифицировать людей, так как при этом выявляются также наследственные связи. Поскольку для анализа ДНК требуется определенная форма ткани, крови или другого физического биологического образца, вероятнее всего, этот метод останется исключительно криминалистическим, а не конкурентоспособным методом на рынке контроля доступа.

6.11 Технологии, построенные на анализе кардиограммы

Физические различия между сердечной мышцей и кровеносными системами приводят к различению мелких деталей сердечного ритма, проявляющихся в электрических сигналах или кровотоке. Существует много исследований в этой области, некоторые из них реализованы в виде коммерческих продуктов.

6.12 Распознавание походки и изображения всего тела

Походка определяется как стиль или манера ходьбы. Системы распознавания походки записывают видеоизображение ходьбы человека и анализируют отличительные особенности формы и динамики силуэта и/или относительное положение и динамику суставов и конечностей.

7 Примеры областей применения

Области применения биометрических технологий весьма разнообразны и затрагивают государственные, коммерческие и персональные области, которые трудно отчетливо классифицировать. Поэтому настоящий раздел построен на основе функций приложения (например, время и посещаемость, автоматизированные платежи), а не областей реализации (например, банковское дело, здравоохранение), с учетом того факта, что одно биометрическое приложение может быть использовано в нескольких областях.

7.1 Физический контроль доступа

Некоторые из самых ранних областей применения автоматизированного распознавания людей были связаны с открытием дверей. Это применение охватывает в настоящий момент спортивно-оздоровительные центры, тематические парки и рабочие места и позволяет членам и работникам осуществлять вход с минимальным контролем со стороны. В 90-х гг. XX в. и в начале XXI в. геометрия контура кисти руки была основной биометрической модальностью, используемой для приложений с низким и умеренным уровнем безопасности, однако в последнее время технология распознавания отпечатков пальцев стала доминирующей. В 80-х и 90-х гг. XX в. некоторые приложения с высоким уровнем безопасности, предназначенные для государства и для бизнеса, использовали распознавание сетчатки глаза, но с тех пор на рынке стали доминировать технологии распознавания РОГ и нескольких отпечатков пальцев.

Парк развлечений «Disney World» в Орландо, штат Флорида, США, начал использовать геометрию пальцев (одна из форм геометрии контура кисти руки) в середине 90-х гг. XX в. в качестве многофакторного решения для контроля доступа владельцев сезонных абонементов. К середине 2000-х гг. система перешла на регистрацию отпечатков пальцев и была применена ко всем владельцам пропусков в «Disney World», для того чтобы предотвратить передачу пропусков посторонним лицам.

7.2 Логический контроль доступа

В 70-х гг. XX в. активно пропагандировалось использование биометрических данных для контроля доступа к компьютерным записям. К концу 80-х гг. XX в. на рынке появилось много систем распознавания отпечатков пальцев, сетчатки глаза и голоса. К концу 90-х гг. XX в. считыватели отпечатков пальцев стали встраивать в компьютерные клавиатуры и мобильные телефоны, но внедрение происходило медленно. Технология биометрического сравнения на идентификационной карте стала доступна в конце 2000-х гг. Данная технология заключалась в сохранении биометрического контрольного шаблона (как правило, отпечатка пальца) и в выполнении всех компьютерных вычислений, необходимых для распознавания на идентификационной карте, контролируемой субъектом данных. Считалось, что эта технология обеспечивает защиту персональных данных. Хотя субъект данных должен был представить биометрический образец на главный компьютер, но этот биометрический образец не сохранялся, а сразу же передавался на идентификационную карту для биометрического сравнения с ранее зарегистрированным биометрическим контрольным шаблоном.

Быстрое внедрение смартфонов в 2010-х гг. XXI в. позволило расширить концепцию технологии сравнения на идентификационной карте и использовать ее на мобильном телефоне, включая все аспекты, например сбор, хранение и сравнение биометрических данных под полным контролем субъекта биометрических данных. Приложения для голоса, лица, вен, склеры и отпечатков пальцев стали легкодоступны для разблокировки телефона и других приложений на телефоне без передачи биометрических данных из непосредственного владения субъекта данных.

7.3 Учет рабочего времени и посещаемости

Биометрические системы для учета рабочего времени и посещаемости датируются началом 90-х гг. XX в., и в настоящее время они используются малыми предприятиями, в различных областях промышленности и на государственном уровне. На рынке доступны различные устройства, основанные на получении данных отпечатков пальцев, геометрии руки и РОГ. В дополнение к отслеживанию времени с целью расчета заработной платы системы могут в любое время предоставить руководителям немедленный доступ к данным о том, какие сотрудники находятся на рабочем месте. Такая информация полезна в случае возникновения чрезвычайной ситуации.

7.4 Отчетность

Биометрическое распознавание может быть использовано в приложениях, требующих отчетности и неотказуемости. В некоторых больницах и аптеках используют биометрические данные как одно из требований для предоставления доступа к наркотикам. Сбор биометрических данных гарантирует, что выдача каждой дозы может быть однозначно отнесена на счет зарегистрированного лица таким образом, чтобы впоследствии от нее невозможно было отказаться.

7.5 Электронная подпись

Ряд банков выпустили приложения для смартфонов, использующие биометрические характеристики для авторизации покупок и переводов денежных средств.

7.6 Государственные/гражданские услуги

Электронные государственные услуги в ряде стран предоставляются гражданам и резидентам на основе использования биометрии. Крупнейшим таким приложением является уникальный идентификационный орган Индии (UIDAI). Резиденты Индии обращаются за номером «Aadhaar» на любом из тысячи сайтов для регистрации, предоставляя изображения радужной оболочки двух глаз, отпечатков пальцев и изображения лица. Изображения РОГ и отпечатков пальцев используют для исключения дублирования; при этом осуществляется поиск по всей базе данных, для того чтобы избежать выдачи нескольких номеров «Aadhaar» одному человеку. Выданный номер может быть применен с одной из биометрических характеристик (как правило, с отпечатков пальца) для многофакторного распознавания при распределении государственных льгот и услуг. Первоначальная цель системы заключалась в содействии развитию экономики за счет открытия банковских счетов для тех лиц, которые не имеют идентификационных документов или других государственных удостоверений личности.

Использование биометрии при голосовании сопряжено с многочисленными проблемами. Мексиканское правительство использовало изображения лиц наряду с биографической информацией для исключения дублирования регистраций избирателей на отдельных участках. Использование биометрии на национальном уровне в день выборов для соотнесения избирателей с регистрациями оказалось проблематичным из-за требований к пропускной способности и необходимости наличия механизмов обработки исключений для тех, кто не был распознан.

Австралийский департамент социальных служб использует распознавание диктора для проверки личности звонящих в офисы выдачи пособий «Centrelink». Биометрические контрольные шаблоны голоса индексируются по номеру телефона, так что входящий вызов с распознанного номера телефона необходимо сравнить только с очень небольшим количеством биометрических контрольных шаблонов для проверки личности вызывающего абонента. Эта система работает как в текстозависимом, так и в текстонезависимом режиме.

В Российской Федерации с 2018 г. действует Единая биометрическая система, которая позволяет предоставлять новые цифровые коммерческие и государственные услуги для граждан в любое время и в любом месте с помощью биометрии. В настоящее время с помощью Единой биометрической системы граждане без личного присутствия могут открыть счет, вклад или получить кредит в банке. Биометрическая верификация происходит по двум биометрическим характеристикам — лицо и голос, которую можно выполнить с любого устройства. Также в Единой биометрической системе реализована подсистема обнаружения атаки на биометрическое предъявление, которая позволяет обнаружить подделку вместо «живого человека» и избежать подмены биометрического образца.

7.7 Охрана границы

7.7.1 Электронные паспорта и машисчитываемые проездные документы

В 90-х гг. XX в. Международная организация гражданской авиации (ИКАО, ICAO), отвечающая за установление международных стандартов на паспорта, приступила к осуществлению инициативы по созданию машиносчитываемых проездных документов (МПД, MRTD), а в 2003 г. установила, что изображения лиц, дополненные, по мере необходимости, изображениями отпечатков пальцев и РОГ, являются предпочтительной биометрической характеристикой для использования в МПД. Начиная с 2006 г. почти все развитые страны выпускают электронные паспорта, содержащие компьютерную микросхему, соответствующую спецификациям МПД ИКАО (MRTD ICAO). Изображение лица хранится на компьютерной микросхеме в виде файла JPEG. Некоторые страны расширили эти данные, включив в них биометрические контрольные шаблоны отпечатков пальцев. Это позволило использовать электронные паспорта с биометрическими автоматизированными системами паспортного контроля (АСПК), позволяющими пассажирам проходить транзитом через системы, в которых они ранее не были зарегистрированы.

7.7.2 Автоматизированные системы паспортного контроля (АСПК)

К середине 2000-х гг. XXI в. по меньшей мере 15 стран внедрили АСПК для некоторых международных пассажиров, заменив первичный линейный контроль биометрическими воротами. АСПК проверяет принадлежность проездного документа (как правило, паспорта) пассажиру путем сбора предъявленных им биометрических характеристик и сравнения их с теми, которые содержатся в МПД (изображение лица или, в некоторых паспортах, отпечатки пальцев), или с зарегистрированным биометрическим контрольным шаблоном, ранее созданным специально для этой АСПК и связанным с идентификационным документом. Если пассажир не распознан по биометрическому контрольному шаблону, то он направляется к сотруднику пограничной службы для дополнительной проверки.

Как правило, АСПК включают другие процедуры пограничного контроля, требуемые органами пограничного контроля, такие как проверка срока действия и подлинности проездного документа, а также поиск фамилии пассажира или номера идентификационного документа в контрольном списке. АСПК не предназначены для замены всех ручных операций, выполняемых при проведении пограничного контроля, и, как правило, они функционируют под человеческим надзором.

7.7.3 Визы

Большинство стран требуют, чтобы пассажиры из других стран получали визы в местных консульствах или аккредитованных визовых центрах до въезда. При некоторых процессах выдачи виз осуществляется сбор изображений лиц и отпечатков пальцев для сравнения с данными тех лиц, которым ранее было отказано в визе, и для сравнения с данными пассажиров по прибытии, для того чтобы предотвратить передачу визы другому лицу.

7.7.4 EURODAC

EURODAC — это база данных отпечатков пальцев просителей убежища Европейского союза (ЕС), которая функционирует с 2003 г. Отпечатки пальцев всех просителей убежища ЕС старше 14 лет сравнивают с отпечатками пальцев ранее зарегистрированных просителей убежища ЕС, а затем хранят в центральной системе EURODAC в течение 10 лет. Цель этой системы заключается в выявлении лиц, многократно ходатайствующих о предоставлении убежища в ЕС в течение этого десятилетнего периода.

7.8 Правоохранительные органы

Правоохранительные органы используют многие из крупнейших в мире биометрических систем. Две основные биометрические функции в правоохранительных органах включают идентификацию арестованных (обычно с помощью наборов отпечатков пальцев, а также, в некоторых случаях, с помощью изображений лица) и идентификацию данных криминалистической экспертизы (часто с помощью скрытых отпечатков пальцев или ДНК, оставленных на местах *преступления). В Российской Федерации отпечатки пальцев ищут по базе данных АДИС-МВД.* В США отпечатки пальцев ищут по базе данных NGI ФБР, которая в настоящее время содержит наборы отпечатков пальцев более чем 70 млн человек. Полицейские подразделения во всем мире используют технологию АДИС для определения источника отпечатков пальцев, оставленных на месте преступлений, и для идентификации арестованных. Базы данных правоохранительных органов также часто содержат отпечатки пальцев лиц, не связанных с преступной деятельностью, например сотрудников правоохранительных органов, военнослужащих или государственных служащих.

7.9 Проверки граждан

Многие виды государственной и частной занятости требуют проверки криминального прошлого заявителей. Эти проверки, как правило, осуществляют путем поиска отпечатков пальцев заявителя по базам данных отпечатков пальцев правоохранительных органов.

7.10 Кластеризация

Биометрия традиционно ассоциируется с идентификацией и верификацией, однако из определения биометрии как автоматизированных методов распознавания лиц вытекают и другие виды применений. Биометрические системы могут быть использованы для кластеризации биометрических образцов (например, изображений лиц) путем группировки биометрических образцов, которые, вероятно, были получены от одного и того же лица, без требования регистрации или распознавании лица.

Социальные сети начали группировать и отмечать лица отдельных людей. Эти люди могут быть связаны с кластерами других людей, появляющихся на тех же изображениях, что позволяет создавать карты социальных сетей.

Таким образом аудиозапись с голосами нескольких людей можно сегментировать и кластеризовать по сегментам речи, связанным с каждым человеком, даже если люди неизвестны.

8 Биометрическая система общего вида

8.1 Схема концептуального представления биометрической системы общего вида

Из-за большого разнообразия биометрических приложений и технологий можно сделать некое обобщение биометрических систем. Во всех биометрических системах присутствуют общие элементы.

Биометрические образцы субъекта регистрируют с помощью биометрических сканеров. Данные с биометрического сканера передают в устройство обработки, которое извлекает отличительные, но повторяющиеся характеристики биометрического образца (его биометрические признаки) и отбрасывает все прочие элементы. Выделенные таким образом биометрические признаки записывают в базу данных в виде биометрического контрольного шаблона или биометрического шаблона. В остальных случаях биометрический образец (без выделения биометрических признаков) может быть записан в базу данных в виде биометрического контрольного шаблона. Последующий биометрический запрос или биометрическую пробу сравнивают с отдельным биометрическим контрольным шаблоном, с несколькими биометрическими контрольными шаблонами или со всеми биометрическими контрольными шаблонами, хранящимися в базе данных. Решение о подтверждении биометрического заявления выносят на основании оценки степени схожести или различия биометрических признаков пробы и биометрических признаков, записанных в биометрическом контрольном шаблоне или биометрических контрольных шаблонах, с которыми данную биометрическую пробу сравнивают.

На рисунке 1 показаны информационные потоки биометрической системы общего вида, а также представлена структура биометрической системы общего вида, которая состоит из подсистем сбора данных, обработки сигнала, хранения данных, сравнения и принятия решения. На схеме также показаны процесс биометрической регистрации и работа систем биометрической верификации и идентификации. В следующих разделах настоящего стандарта каждая из перечисленных подсистем описана более подробно. Следует отметить, что в любой реально действующей биометрической системе некоторые из представленных концептуальных компонентов могут отсутствовать или не соответствовать в точности реальным физическим компонентам или программному обеспечению.

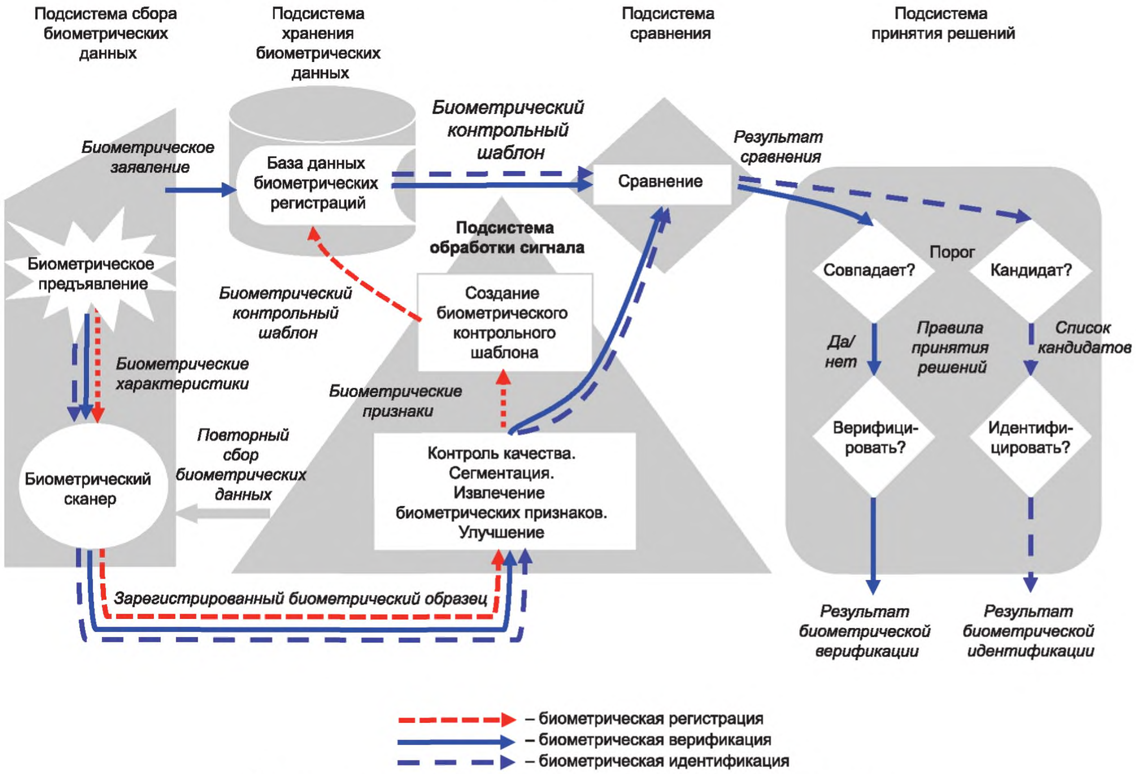


Рисунок 1 — Компоненты биометрической системы общего вида

8.2 Концептуальные компоненты биометрической системы общего вида

8.2.1 Подсистема сбора биометрических данных

Подсистема сбора биометрических данных получает с биометрического сканера биометрические характеристики субъекта в виде изображения или сигнала и выводит изображение/сигнал в виде зарегистрированного биометрического образца.

8.2.2 Подсистема передачи биометрических данных

Подсистема передачи биометрических данных, которая не всегда представлена или явно присутствует в биометрической системе, осуществляет передачу биометрических образцов, биометрических признаков и биометрических контрольных шаблонов между различными подсистемами биометрической системы. Зарегистрированный биометрический образец может быть подвержен сжатию и/или шифрованию перед передачей и распакован (разжат) и/или дешифрован перед использованием. В процессе передачи зарегистрированный биометрический образец может изменяться из-за помех в канале передачи данных или из-за потерь при сжатии и распаковке. Данные могут быть переданы с использованием стандартных форматов обмена биометрическими данными, а для обеспечения подлинности, целостности и конфиденциальности записанных и передаваемых биометрических данных рекомендуется использовать методы защиты информации.

8.2.3 Подсистема обработки сигнала

Обработка сигнала включает следующие процессы:

- улучшение, т. е. повышение качества и четкости зарегистрированного биометрического образца;
- сегментацию, т. е. локализацию сигнала, содержащего биометрические характеристики субъекта, внутри зарегистрированного биометрического образца;
- извлечение биометрических признаков, т. е. получение повторяющихся и отличительных показателей субъекта из зарегистрированного биометрического образца;
- контроль качества, т. е. оценку пригодности биометрических образцов, биометрических признаков, биометрических контрольных шаблонов и возможное влияние других процессов, например возвращение управления подсистеме сбора биометрических данных для последующего сбора биометрических образцов или изменение параметров сегментации, извлечения биометрических признаков или сравнения.

В процессе биометрической регистрации подсистема обработки сигнала создает биометрический контрольный шаблон. В некоторых случаях для процесса биометрической регистрации может потребоваться несколько предъявлений субъектом биометрических характеристик. Когда биометрический контрольный шаблон содержит только биометрические признаки, он именуется шаблоном. Когда биометрический контрольный шаблон содержит только биометрический образец, извлечение биометрических признаков из биометрического контрольного шаблона происходит сразу перед сравнением.

В случае биометрической верификации и идентификации подсистема обработки сигнала создает биометрическую пробу.

Порядок и итерация вышеупомянутых процессов должны быть определены в спецификации к каждой биометрической системе.

8.2.4 Подсистема хранения биометрических данных

Биометрические контрольные шаблоны хранят в базе данных биометрических регистраций, являющейся частью подсистемы хранения данных. Каждый биометрический контрольный шаблон должен быть связан с определенным зарегистрированным субъектом или процессом биометрической регистрации. Перед сохранением в базе данных биометрических регистраций биометрические шаблоны могут быть преобразованы в формат обмена биометрическими данными. Биометрические контрольные шаблоны могут хранить на самом устройстве сбора биометрических данных, на переносном носителе (например, смарт-карте), на персональном компьютере, на локальном сервере или в центральной базе данных.

8.2.5 Подсистема сравнения

Подсистема сравнения выполняет сравнение биометрических проб с одним или несколькими биометрическими контрольными шаблонами и выдает подсистеме принятия решений результат сравнения. Результаты сравнения определяют степени схожести или различия при сравнении биометрических проб с биометрическим(и) контрольным(и) шаблоном(ами).

При выполнении биометрической верификации субъекта на единственный запрос выдается единственный результат сравнения. При выполнении биометрической идентификации множество или все биометрические контрольные шаблоны могут сравниваться с биометрическими признаками, при этом результат сравнения будет выдаваться на каждое сравнение.

8.2.6 Подсистема принятия решений

Подсистема принятия решений использует результаты сравнения, сформированные одной или несколькими попытками, чтобы выдать итоговый результат для транзакции биометрической верификации или идентификации.

В случае биометрической верификации сравнение биометрической пробы и биометрического контрольного шаблона признают успешным (считая, что более высокие результаты соответствуют большему сходству), если результат сравнения превышает установленный порог. Биометрическое заявление может быть подтверждено согласно правилам принятия решений, которые могут предусматривать несколько попыток биометрической верификации.

В случае биометрической идентификации зарегистрированный биометрический контрольный шаблон является потенциальным кандидатом для субъекта (т. е. более высокие результаты соответствуют большему сходству), если результат сравнения превысил установленный порог и/или если результат сравнения является одним из самых высоких ранжированных значений, созданных во время сравнения по всей базе данных. Согласно правилам принятия решений может потребоваться несколько попыток идентификации перед принятием решения.

Примечание — Концептуально можно рассматривать мультибиометрические системы подобно монобиометрическим системам, считая комплексные зарегистрированные биометрические образцы/шаблоны/показатели за один биометрический образец/шаблон/показатель и позволяя подсистеме принятия решений, при необходимости, оперировать совокупным показателем или совокупным решением *(см. [24])*.

8.2.7 Подсистема администрирования

Подсистема администрирования управляет общими правилами, реализацией, конфигурацией и использованием биометрической системы с учетом законодательных, юридических и общественных ограничений и требований.

В частности, подсистема администрирования выполняет:

a) взаимодействие с субъектом, включая обеспечение обратной связи с субъектом в процессе и/или после сбора биометрических данных, и запрос дополнительной информации от субъекта;

b) хранение и форматирование биометрических контрольных шаблонов и/или данных биометрического обмена;

c) вынесение окончательного заключения на выходе на основе решения и/или результатов сравнения;

d) задание пороговых значений;

e) настройку параметров сбора биометрических данных для биометрической системы;

f) контроль операционной среды и хранение небиометрических данных;

g) обеспечение соответствующих гарантий конфиденциальности и безопасности данных субъекта;

h) взаимодействие с приложением, использующим биометрическую систему.

8.2.8 Интерфейс

Биометрическая система может взаимодействовать с внешними приложениями или системами через интерфейс веб-служб, программный интерфейс приложений, аппаратный интерфейс или интерфейс протоколов.

8.3 Функции биометрической системы общего вида

8.3.1 Биометрическая регистрация

При биометрической регистрации данные, полученные в результате взаимодействия субъекта с биометрической системой, обрабатывают и хранят в виде контрольного шаблона биометрической регистрации для данного индивида.

При биометрической регистрации выполняют следующие операции:

a) получение биометрических образцов;

b) восстановление или улучшение биометрических образцов;

c) сегментацию;

d) извлечение биометрических признаков;

e) контроль качества (по результатам которого биометрический образец или биометрические признаки могут быть отклонены как непригодные для создания биометрического контрольного шаблона и может потребоваться получение дополнительных биометрических образцов);

f) сравнение с существующими биометрическими контрольными шаблонами, для того чтобы убедиться в том, что субъект еще не зарегистрирован (при наличии требований системных правил);

g) создание биометрического контрольного шаблона, для чего могут потребоваться биометрические признаки нескольких биометрических образцов, их преобразование в формат обмена биометрическими данными;

h) хранение;

i) тестовую биометрическую верификацию или идентификацию для подтверждения пригодности результата биометрической регистрации при дальнейшем использовании;

j) разрешение повторной попытки биометрической регистрации, если результаты первоначальной биометрической регистрации признаны неудовлетворительными (в зависимости от правил биометрической регистрации).

8.3.2 Биометрическая верификация положительного биометрического заявления

В приложениях, таких как контроль доступа, при верификации биометрические данные, полученные в результате взаимодействия субъекта с системой, обрабатывают с целью подтверждения наличия в системе данных субъекта (например, «я зарегистрирован как субъект *X*»). Следует отметить, что некоторые биометрические системы позволяют субъекту регистрировать несколько биометрических характеристик. Например, в системе биометрической идентификации по РОГ субъекты могут зарегистрировать изображения радужных оболочек обоих глаз, а в системе биометрической идентификации по отпечаткам пальцев — другие пальцы, если основной палец окажется травмированным.

При биометрической верификации определенного положительного биометрического заявления выполняют следующие операции:

a) получение биометрических образцов;

b) восстановление или улучшение биометрических образцов;

c) сегментацию;

d) извлечение биометрических признаков;

e) контроль качества (по результатам которого биометрический образец или биометрические признаки могут быть отклонены как непригодные для сравнения и может потребоваться получение дополнительных биометрических образцов);

f) создание биометрической пробы (что может потребовать биометрические признаки нескольких образцов), возможное преобразование в формат обмена биометрическими данными;

g) сравнение биометрической пробы с биометрическим контрольным шаблоном для подтверждения личности с выдачей результата сравнения;

h) определение совпадений биометрических признаков пробы и биометрического контрольного шаблона, основанное на превышении результатом сравнения установленного порога (т. е. более высокие результаты соответствуют большему сходству);

i) принятие решения по биометрической верификации на основании результата сравнения в одной или нескольких попытках согласно правилам принятия решений.

Пример — В системе, допускающей при верификации не более трех попыток распознавания, ложный недопуск будет результатом любой комбинации сбоев в процессе получения данных или ложных несовпадений в процессе сравнения в этих трех попытках. Ложный допуск произойдет, если биометрический образец получен, но совпал ошибочно с зарегистрированным биометрическим контрольным шаблоном в любой из трех попыток.

Функция биометрической верификации либо примет, либо отклонит определенное положительное биометрическое заявление. Результат решения системы биометрической верификации считается ошибочным, если принято ложное заявление (ложный допуск) или отклонено истинное заявление (ложный недопуск). В этом приложении ложный допуск происходит, если представленный биометрический образец ошибочно совпал с биометрическим контрольным шаблоном, который не создавался субъектом данных. Ложный недопуск происходит, если представленный биометрический образец не совпадает с биометрическим контрольным шаблоном, действительно созданным субъектом данных.

Биометрическая верификация неопределенного положительного биометрического заявления также вполне возможна с помощью биометрической системы. В 90-х гг. XX в. такие приложения именовались «верификация без ПИН-кода», так как ПИН-код или другой идентификатор не требовался для установления того, что субъект данных действительно был зарегистрирован в базе данных. С конца

90-х гг. XX в. системы распознавания РОГ были использованы в этом качестве для контроля допуска. Процесс соответствует указанным выше перечислениям a)—f). Однако шаги по перечислениям g)—i) несколько отличаются, когда заявление является неопределенным, а именно:

g) сравнение биометрической пробы со всеми биометрическими контрольными шаблонами, дающее результат для каждого сравнения;

h) определение совпадений биометрических признаков пробы и любого биометрического контрольного шаблона, основанное на превышении результатом сравнения установленного порога (т. е. более высокие результаты соответствуют большему сходству);

i) принятие решения на основании результатов сравнения в одной или нескольких попытках согласно правилам принятия решений.

8.3.3 Биометрическая идентификация

При биометрической идентификации данные, полученные в результате взаимодействия субъекта с биометрической системой, обрабатывают с целью поиска совпадающих биометрических контрольных шаблонов в базе данных биометрических регистраций. По результатам биометрической идентификации создается список кандидатов. Список кандидатов может быть пустым, содержать только один идентификатор или более. Биометрическая идентификация признана успешной, если субъект прошел биометрическую регистрацию, а его идентификатор присутствует в списке кандидатов. Биометрическая идентификация признана ошибочной, если идентификатор зарегистрированного субъекта не попадает в список кандидатов (ложноотрицательная биометрическая идентификация) либо в результате обработки запроса от незарегистрированного субъекта создается непустой список кандидатов (ложноположительная биометрическая идентификация).

При биометрической идентификации выполняют следующие операции:

a) получение биометрических образцов;

b) восстановление или улучшение биометрических образцов;

c) сегментацию;

d) извлечение биометрических признаков;

e) контроль качества (по результатам которого биометрический образец или биометрические признаки могут быть отклонены как непригодные для сравнения и может потребоваться получение дополнительных биометрических образцов);

f) создание биометрической пробы (что может потребовать биометрические признаки нескольких образцов), возможное преобразование в формат обмена биометрическими данными;

g) сравнение с отдельными или со всеми биометрическими контрольными шаблонами, имеющимися в базе данных биометрических регистраций, выдачу результата сравнения для каждого сравнения;

h) проверку условия, является ли каждый сравниваемый контрольный шаблон потенциальным идентификатором кандидата для данного пользователя, основанную на превышении результатом сравнения установленного порога и/или его принадлежности к диапазону максимальных значений, а также дальнейшее формирование списка кандидатов;

i) принятие решения на основании списков кандидатов из одной или нескольких попыток согласно правилам принятия решений.

9 Эксплуатационные испытания

9.1 Общие положения

Биометрические устройства и системы могут быть подвергнуты различным испытаниям. Испытания могут включать в себя оценку:

a) эксплуатационных характеристик (в терминах вероятностей ошибок и производительности);

b) надежности, доступности и удобства эксплуатации;

c) степени защищенности;

d) безопасности;

e) приемлемости системы для пользователя;

f) влияния человеческих факторов;

g) коэффициента эффективности затрат;

h) соблюдения законодательства, в том числе касающегося конфиденциальности и прозрачности использования зарегистрированных биометрических данных индивида.

В течение последних трех десятилетий оценка эксплуатационных характеристик является наиболее распространенной формой испытаний. Эксплуатационные испытания обычно проводят с целью прогноза эксплуатационных характеристик системы для целевой выборки и в целевых условиях применения, но исторически сложилось так, что экстраполяция результатов испытаний в тестовых условиях на практике вызывает много трудностей. Для того чтобы результаты испытаний лучше соответствовали эксплуатационным характеристикам систем при практической эксплуатации, разработаны стандарты, устанавливающие процедуры проведения испытаний (*см. [25]*).

Эксплуатационные испытания могут проводиться на замкнутом множестве либо на открытом множестве. Испытания не могут выявить эксплуатационные характеристики системы, если она использована субъектами, которые не зарегистрированы в системе. В процессе испытания на замкнутом множестве возвращается ранг истинного совпадения, когда входной биометрический образец сравнивают со всеми зарегистрированными биометрическими контрольными шаблонами. В процессе испытания на замкнутом множестве вычисляют вероятность того, что истинный биометрический контрольный шаблон найден во время поиска по базе данных размера N с рангом k или выше. При любом испытании данная вероятность зависит от размера базы данных, уменьшаясь с увеличением размера базы данных.

При проведении испытания на открытом множестве не требуется, чтобы все входные биометрические образцы имели соответствующий зарегистрированный в базе данных биометрический контрольный шаблон, при этом все результаты сравнения сопоставляют с порогом. По результатам испытаний на открытом множестве строят функцию порога, вероятности отсутствия совпадения при сравнении биометрической пробы и биометрического контрольного шаблона от одного источника (вероятность ложного несовпадения) и вероятности совпадения биометрической пробы и биометрического контрольного шаблона от разных источников (вероятность ложного совпадения).

Примеры испытаний как на открытом множестве, так и на замкнутом множестве описаны в литературе, но так как большинство приложений предполагает потенциальное существование «самозванцев», то результаты испытаний на открытом множестве крайне важны для разработчиков системы или аналитиков с практической точки зрения.

Как правило, в процессе проведения испытаний на открытом множестве определяют следующие характеристики: вероятность отказа биометрической регистрации, вероятность отказа получения биометрических данных, вероятность ложного допуска, вероятность ложного недопуска, пропускная способность. Вероятность отказа биометрической регистрации определяют как долю зарегистрированных транзакций, при которых биометрическая регистрация не может быть завершена вследствие ошибки биометрической системы или человеческой ошибки. Вероятность отказа получения биометрических данных определяют как долю процессов получения биометрических данных от всех зарегистрированных субъектов, которые не были приняты биометрической системой. Вероятность ложного недопуска определяют как долю всех транзакций биометрической верификации с истинными биометрическими заявлениями, которые были ошибочно отвергнуты биометрической системой. Вероятность ложного допуска определяют как долю всех транзакций биометрической верификации с ложными биометрическими заявлениями, которые ошибочно приняты биометрической системой. Так как вероятности ложного допуска/недопуска (или вероятности ложного совпадения/несовпадения) представляют собой противоположные показатели, они могут быть изображены одновременно на кривой компромиссного определения ошибки (КОО). Пропускная способность системы представляет собой число субъектов, которое биометрическая система может обработать за 1 мин, и определена с учетом как времени взаимодействия человека и устройства, так и времени обработки биометрических данных.

9.2 Виды эксплуатационных испытаний

Ниже приведено описание трех видов эксплуатационных испытаний: технологического, сценарного и оперативного [26].

Технологическое испытание, целью которого является сравнение нескольких алгоритмов распознавания одинаковых биометрических модальностей (например, отпечатков пальцев) с использованием стандартизованной базы данных биометрических образцов, собранной с помощью биометрического сканера, соответствующего стандартам (т. е. «универсального» сканера). Технологические испытания проводятся для систем:

- верификации диктора [27];
- распознавания по лицу [28]—[33];

- распознавания по отпечаткам пальцев [34]—[41];
- распознавания по РОГ [42], [43].

Сценарное испытание, целью которого является оценка эксплуатационных характеристик всей биометрической системы, осуществляемая при использовании реальных взаимодействующих с системой субъектов и в условиях, моделирующих реальное применение биометрической системы. Каждая испытуемая биометрическая система имеет свой биометрический сканер для сбора биометрических данных, в результате чего могут быть небольшие различия в получаемых исходных данных. Сценарные испытания проведены на больших выборках, но в открытых источниках публикуется малая часть результатов сценарных испытаний [44]—[46].

Оперативное испытание, целью которого является определение эксплуатационных характеристик всей биометрической системы при использовании целевой выборки и в определенных условиях применения. В общем случае из-за неизвестных и недокументированных различий в условиях окружающей среды, имевших место в процессе проведения испытания, добиться воспроизводимости результатов оперативных испытаний невозможно. Кроме того, трудно установить истинную информацию (т. е. найти тех, кто предоставляет «достоверные» биометрические характеристики). Так как вероятности ошибок в значительной степени зависят от используемой операционной системы, в открытых источниках публикуется малая часть результатов оперативных испытаний [47].

Все биометрические технологии распознавания предусматривают взаимодействие субъекта с устройством сбора биометрических данных. В общем случае технологическое испытание направлено на снижение влияния взаимодействия биометрической системы с субъектом, в то время как при проведении сценарного и оперативного испытаний оказываемое влияние должно быть учтено и оценено. Вероятности ошибок сравнения, отказа биометрической регистрации и получения биометрических данных и показатели пропускной способности определены взаимодействием биометрической системы с субъектом, что, в свою очередь, зависит от особенностей условий сбора биометрических данных. Дисциплина, изучающая человеческие факторы при сборе биометрических данных, находится на стадии становления.

Результаты эксплуатационных испытаний могут варьироваться в зависимости:
- от типа испытания (технологического, сценарного или оперативного);
- состава корпуса данных для испытаний и контроля качества данных *(см. [48])*;
- условий применения (которые могут повлиять на относительную разницу между сопоставляемой биометрической пробой и биометрическим контрольным шаблоном, затрудняя процесс определения результата сравнения *(см. [49])*;
- правил принятия решений (например, сколько попыток допускается).

Эти проблемы могут затруднить сравнение результатов испытания и прогнозирование реальных эксплуатационных характеристик биометрической системы.

10 Биометрические технические интерфейсы

10.1 Блоки биометрических данных и записи биометрических данных

В биометрических стандартах существуют две основные концепции биометрических технических интерфейсов.

Первая концепция основана на блоках биометрических данных (ББД). ББД представляет собой блок данных с определенным форматом, который содержит один биометрический образец или биометрический контрольный шаблон или более, такой как изображение отпечатка пальца, запись о минуциях пальца (соединение или бифуркация гребней и впадин), изображение РОГ и т. д.

Для различных биометрических технологий существуют стандарты форматов обмена биометрическими данными *(см. [50])*, каждый из которых определяет один формат ББД или более (например, форматы компактных смарт-карт наравне с обычными форматами). У каждого формата ББД есть идентификатор формата ББД, позволяющий расшифровать или обработать формат, о котором у системы имеется информация.

Вторая концепция основана на записи биометрической информации (ЗБИ). ЗБИ — это ББД, но с дополнительными метаданными: дата сбора, дата истечения срока хранения, данные об устройстве сбора, информация о том, закодированы или не закодированы данные. Некоторые форматы ЗБИ установлены как части продолжающейся работы в данной области на базе как количества информации, включенной в ЗБИ, так и компактности используемой схемы кодирования *(см. [51])*. К тому же у форматов ЗБИ имеется идентификатор, который в данном случае именуется идентификатором формата ведущей организации ЕСФОБД.

ЗБИ является блоком, применяемым в большинстве стандартов для хранения и обмена между модулями программного обеспечения и компьютерными системами, например используя сервисы биометрической идентификации (BIAS) и интерфейсы BioAPI (в рамках системы) или протокол межсетевого обмена (ПМО) (между системами).

Архитектуры BioAPI и ЗБИ имеют важное значение в любой работе, включающей в себя обмен биометрической информацией (ББД, ЗБИ) в рамках системы или между системами.

10.2 Сервисные архитектуры

Сервис-ориентированная архитектура (SOA) — это шаблон проектирования программного обеспечения, основанный на отдельных частях программного обеспечения, называемых сервисами. Сервисы — это независимые программные продукты, предназначенные для выполнения определенной функции и содержащие набор возможностей для реализации этой функции. Сервис, как правило, подразумевает заключение контрактов на услуги, которые представляют собой технические описания сервисов, предназначенных для использования во время выполнения [например, определение языка описания веб-служб (WSDL) и определение схемы XML]. Сервисы сходны с программными интерфейсами (API). Шаблон проектирования SOA обеспечивает агрегирование сервисов посредством объединений сервисов, результатом которого является автоматизированная поддержка любого бизнес-процесса, требующего функциональности объединения сервисов.

Биометрические программные сервисы предназначены для обеспечения общего набора биометрических и идентификационных функций и связанных с ними определений, приведенных для облегчения сбора, хранения, использования и раскрытия биографических и биометрических данных в различных бизнес-контекстах и областях. Эти сервисы, как правило, не содержат логики, специфичной и уникальной для конкретной бизнес-операции, так как такая логика более уместна на уровне логики приложения. Вероятнее всего, сервисы содержат логику, необходимую для применения биометрических сервисов независимо от условий эксплуатации.

В настоящее время существует два стандарта, которые определяют биометрические сервисы:

a) биометрические устройства WS (WS-BD), описанные в [52], в которых определен ряд примитивных и агрегированных сервисов для интеграции биометрических сенсорных устройств в биометрические системы, имеющие компонент получения биометрических данных;

b) BIAS *(см. [53])*, который определяет ряд примитивных и агрегированных сервисов по обеспечению биометрической идентификации. По сути, эти сервисы обеспечивают хранение и извлечение биографических и биометрических данных, собранных у индивида, когда биометрические данные получают с помощью биометрического сканера.

10.3 Единая структура форматов обмена биометрическими данными (ЕСФОБД)

ГОСТ Р 58293 предназначен для обеспечения взаимодействия приложений, применяемых в области биометрии, путем установления стандартных структур ЗБИ (ББД с метаданными) и набора абстрактных элементов данных и значений, которые могут быть использованы для формирования части заголовка ЗБИ, соответствующей ЕСФОБД.

ЗБИ представляет собой данные, записанные в соответствии с форматом ведущей организации ЕСФОБД (см. ниже). Это ББД для хранения в базе данных или обмена между системами или частями систем. ЗБИ всегда состоит не менее чем из двух частей: стандартного биометрического заголовка (СБЗ) и по меньшей мере одного ББД. ЗБИ может содержать также и третью часть, именуемую блоком защиты информации (БЗИ). ЕСФОБД не устанавливает требований к содержанию и способу записи ББД, за исключением того, что его размер в битах должен быть кратным восьми, установлены стандартизованные форматы ББД для ряда биометрических технологий *(см. [50])*.

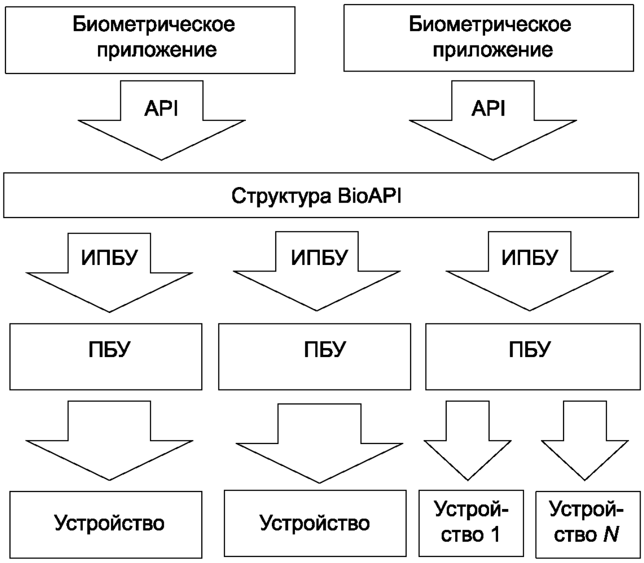
Основным назначением ЕСФОБД является установление элементов данных и их абстрактных значений с определенной семантикой, которые являются общепринятыми параметрами и применяются как части СБЗ в ЗБИ.

Конкретный формат ведущей организации ЕСФОБД устанавливает требования для определенной области использования. Формат ведущей организации ЕСФОБД представляет собой полноразрядную спецификацию кодирования, которая может использовать некоторые или все абстрактные значения некоторых или всех элементов данных ЕСФОБД, определенных в настоящем стандарте. Допускается также применять дополнительные абстрактные значения, установленные форматом ведущей организации ЕСФОБД, вместе с одним ББД или более.

10.4 Стандарт BioAPI

Стандарт BioAPI *(см. [54])* предоставляет архитектуру реализации, которая поддерживает биометрические приложения с использованием программных (и аппаратных) модулей от нескольких поставщиков.

Основная концепция заключена в приложениях (от множества поставщиков), которые взаимодействуют со структурой BioAPI (от одного поставщика, но с определенными интерфейсами), которая, в свою очередь, взаимодействует с поставщиками биометрических услуг (ПБУ) (от множества поставщиков) для выполнения биометрических функций. Архитектура BioAPI представлена на рисунке 2.



ИПБУ — интерфейс поставщика биометрической услуги

Рисунок 2 — Архитектура BioAPI

Взаимодействие между разными компонентами осуществляется посредством передачи ЗБИ.

ПБУ может выполнять сбор, сопоставление, архивацию или обработку ЗБИ.

В последнем издании, посвященном архитектуре BioAPI, ПБУ может состоять из кода одного поставщика, взаимодействующего с блоком BioAPI, предоставленным другим поставщиком, — в основном это аппаратное устройство и драйверы к нему. Таким образом, работа поставщиков аппаратных устройств, необходимая для того, чтобы стать частью биометрической системы, сведена к минимуму.

10.5 Стандарт протокола межсетевого обмена BioAPI

Стандарт протокола межсетевого обмена BioAPI *(см. [55])* предоставляет собой линейный битовый контакт, обеспечивающий взаимодействие приложения в одной системе BioAPI с ПБУ удаленной системы BioAPI. Данное расширение архитектуры BioAPI формирует часть подсистемы передачи, описанной в 8.2.2 (см. рисунок 3).

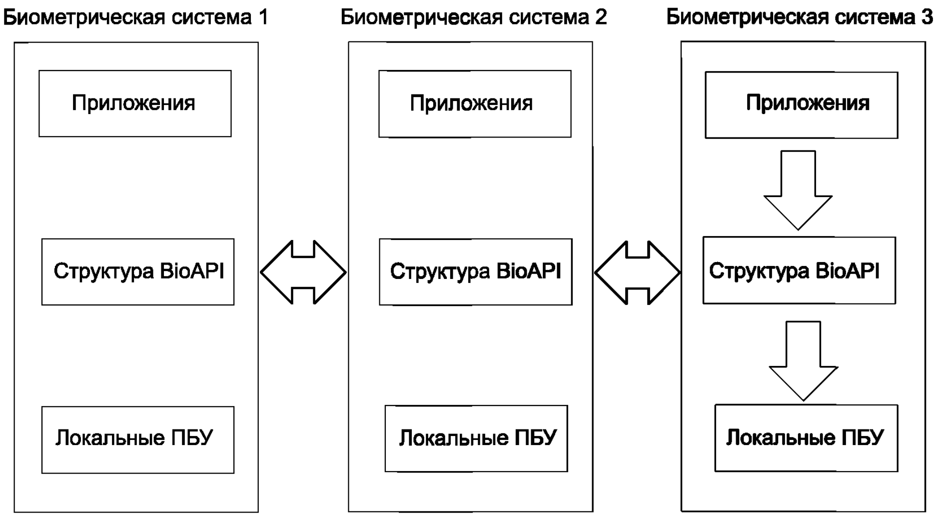


Рисунок 3 — Применение протокола межсетевого обмена для контакта между биометрическими системами

11 Биометрия и информационная безопасность

11.1 Общие положения

На данный момент очевидно, что биометрия может играть важную роль в информационной безопасности, потому что тесно связана с субъектом, так как биометрические характеристики сложнее забыть, раскрыть или потерять, чем токены, ПИН-код или пароль. Применение биометрии может служить дополнительным свидетельством того, что авторизационные данные предъявлены именно тем субъектом, которому они были выданы. Однако биометрические технологии не становятся панацеей, избавляющей от необходимости использования ПИН-кодов, паролей и токенов при решении проблем безопасности.

При разработке системы биометрической верификации положительных биометрических заявлений необходимо решить, будет ли биометрический контрольный шаблон находиться у самого субъекта на токене (в этом случае в такой обработанной форме, как биометрический шаблон, или в той же форме, которая была получена первоначально, например в форме изображения) либо биометрический контрольный шаблон будет сохранен централизованно в базе данных, соединенной с пунктом обслуживания коммуникационной системы (см. 10.5). В первом случае происходит лучшее обеспечение конфиденциальности данных *[56]*, а в случае централизованного сохранения возникают следующие вопросы:

a) будет ли полученный биометрический образец передан центральной системе, или центральная система передаст биометрический контрольный шаблон на пункт обслуживания для обработки. В любом случае потребуется надежная форма кодирования для защиты информации в процессе передачи;

b) если биометрический образец из пункта обслуживания передан в центральный пункт, то будет ли он иметь необработанный вид или уже преобразованный в биометрические признаки. В том случае, если преобразование в биометрические признаки происходит перед передачей, на каждом пункте обслуживания потребуются вычислительные возможности и информация об алгоритме извлечения признаков, но пропускная способность передачи при этом снизится;

c) каким образом будет происходить дешифровка зашифрованных данных в том случае, когда это необходимо для сравнения;

d) каким образом субъект может проверить легитимность пункта обслуживания и быть уверенным в том, что после передачи биометрические данные не сохраняются.

Несмотря на то что вышеуказанные вопросы не являются непреодолимыми, они подтверждают тот факт, что биометрия не решает всех проблем безопасности.

11.2 Безопасность биометрических данных

Требования в отношении использования биометрических данных для проверки заявления индивида для авторизации тщательно документируют.

Во-первых, биометрические данные лица должны быть конфиденциальными и не подлежат несанкционированному доступу, использованию и изменению или разглашению посторонним лицам. Это является важным соображением как для передачи, так и для хранения биометрических данных.

Во-вторых, целостность биометрических данных в различных подсистемах обработки в биометрической системе также имеет решающее значение. Например, если целостность данных нарушена, что приводит к созданию недостоверного биометрического контрольного шаблона, результаты последующей биометрической верификации и идентификации также не заслуживают доверия.

В-третьих, если биометрический контрольный шаблон физического лица является предметом кражи личных данных и, следовательно, поставлен под угрозу, сохранение биометрических характеристик, на основе которых получен биометрический контрольный шаблон, означает, что очень трудно отозвать украденный биометрический контрольный шаблон и зарегистрировать новый. Поэтому рассматриваются методы снижения риска компрометации биометрических контрольных шаблонов, включая положения об отзывных/возобновляемых биометрических контрольных шаблонах.

Конфиденциальность, целостность, возобновляемость и отзываемость биометрических данных достигается за счет применения криптографических методов (*см. [57]*).

Для обеспечения конфиденциальности хранимых данных могут быть использованы различные формы криптографических алгоритмов шифрования (шифров). Алгоритмы шифрования применяются к биометрическим данным для получения зашифрованных данных и разработаны таким образом, что зашифрованные данные не предоставляют информации о биометрических данных. Существует соответствующий алгоритм расшифровки, который преобразует зашифрованные данные в исходную форму. Шифры работают совместно с ключами. Если ключ является идентичным и для шифрования, и для дешифрования, шифр симметричен. Если они отличаются, шифр асимметричен. Инфраструктура открытых ключей для шифрования биографических и биометрических данных изображений лиц в электронных паспортах использует асимметричные шифры.

Для обеспечения целостности передаваемых биометрических данных используют алгоритмы проверки подлинности кода аутентификации сообщения (МАС) для проверки того, что биометрические данные не подвергались несанкционированному изменению. Эти алгоритмы обеспечивают целостность и подлинность передаваемого сообщения, обнаруживая изменения в сообщении, а также подтверждая его происхождение. Так как МАС не обеспечивает неотказуемость там, где это требуется, используют схемы цифровой подписи.

Существуют также методы обработки данных, обеспечивающие как конфиденциальность, так и защиту целостности. Они, как правило, включают в себя либо конкретную комбинацию шифрования и вычислений МАС, либо использование алгоритма шифрования особым образом. Определены шесть методов для аутентифицированного шифрования со следующими показателями безопасности (*см. [58]*):

- конфиденциальность данных — защита от несанкционированного раскрытия данных;
- целостность данных — защита, позволяющая получателю данных убедиться в том, что данные не были изменены;
- аутентификация источника данных — защита, позволяющая получателю данных проверить личность источника данных.

Данные методы требуют от отправителя и получателя защищенных данных совместного использования секретного ключа.

Возобновляемые и отзываемые биометрические контрольные шаблоны создаются с помощью концепции псевдоидентичностей (PI). PI являются анонимными и возобновляемыми строками биометрической проверки идентичности в определенном контексте (*см. [59]*). PI получается из биометрических характеристик субъекта данных. Признаки, извлеченные из зарегистрированного биометрического образца субъекта данных, обрабатываются псевдонимным идентифицированным кодировщиком, который генерирует псевдонимный идентификатор и вспомогательные данные (AD), обеспечивая формирование возобновляемого биометрического контрольного шаблона (RBR). После того как этот биометрический контрольный шаблон создан, он может быть сохранен, а зарегистрированный биометрический образец и извлеченные биометрические признаки отбрасываются. Для последующих процессов биометрической верификации биометрические признаки извлекают из зарегистрированного биометрического образца, а затем применяют псевдоидентификационный рекодер для формирования PI, основанной на извлеченных биометрических признаках, и компонента AD RBR. PI биометрического контрольного шаблона и PI биометрической пробы сравнивают. При равных условиях они будут совпадать только в том случае, если будут предъявлены правильные биометрические характеристики и использованы правильные AD.

В дополнение к включению сравнения биометрической пробы и биометрического контрольного шаблона компонент AD RBR может быть использован для выполнения ряда задач, в том числе создания:

- нескольких независимых PI из одного и того же зарегистрированного биометрического образца для обеспечения достаточного числа вариантов биометрических характеристик индивида и, следовательно, возможности создания возобновляемого биометрического контрольного шаблона в рамках одного и того же контекста приложения;
- независимых PI из одного и того же зарегистрированного биометрического образца с минимальной общей информацией между PI для предотвращения биометрических сравнений и связей между приложениями, в которых они использованы.

В зависимости от требований безопасности для биометрической системы RBR может быть использован или не использован. В последнем случае применяют обобщенную модель биометрической системы (см. рисунок 1). Если RBR используют, то обобщенная модель имеет вид, представленный на рисунке 4 (адаптировано из *[57]*).

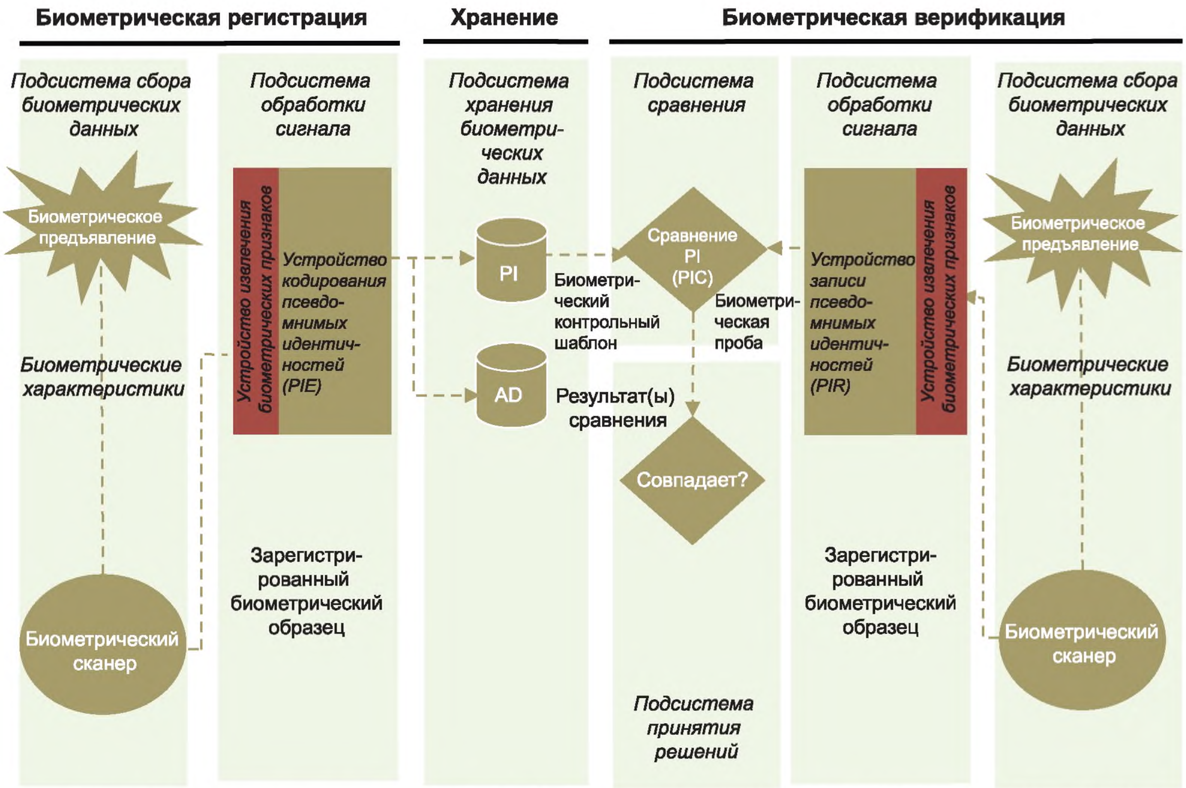


Рисунок 4 — Обобщенная модель биометрической системы, использующей возобновляемые биометрические контрольные шаблоны

Обобщенная модель и модели RBR могут быть реализованы различными способами в зависимости от того, где хранится биометрический контрольный шаблон, где проводится сравнение биометрического контрольного шаблона с биометрической пробой и, в случае реализации RBR, где хранятся компоненты PI и AD. В этом контексте возможные топологии включают (см. *[57]*):

- модель А — хранение на сервере и сравнение на сервере;
- модель В — хранение на токене и сравнение на сервере;
- модель С — хранение на сервере и сравнение на стороне клиента;

- модель D — хранение на стороне клиента и сравнение на стороне клиента;
- модель E — хранение на токене и сравнение на стороне клиента;
- модель F — хранение на токене и сравнение на токене;
- модель G — хранение распределено на токене и сервере, сравнение — на сервере;
- модель H — хранение распределено на токене и на стороне клиента, сравнение — на стороне клиента.

Каждая модель имеет свои преимущества и недостатки в отношении безопасности и конфиденциальности.

11.3 Атаки на биометрическое предъявление (спуфинг)

Несмотря на методы защиты биометрических данных, еще с 70-х гг. XX в. хорошо известно, что биометрические устройства можно обмануть с помощью подделок (*см. [61]—[63]*). «Спуфинг» — это термин, который широко используется в литературе для описания способа подделки биометрических характеристик другого лица с целью быть распознанным в качестве этого лица. Термин «атака на биометрическое предъявление» указывает на то, что может быть сделано с биометрическим предъявлением с целью нарушения запланированной деятельности биометрической системы (*см. [63]*).

Выделяют два основных типа атаки на биометрическое предъявление:

- когда лицо намеревается быть распознанным в качестве иного лица, которым оно не является;
- когда лицо намеревается не быть распознанным в качестве определенного лица, известного системе, и таким образом скрывает свои биометрические характеристики.

В обоих случаях это лицо именуют «самозванец».

Для того чтобы быть признанным биометрической системой в качестве другого лица, самозванец может совершить атаку на биометрический сканер, принуждая другое лицо предъявить свои биометрические характеристики или имитируя другое лицо. В случае принудительной атаки биометрические характеристики субъекта биометрических данных передаются биометрическому сканеру без его разрешения. Это может быть выполнено силовым или другим способом. При атаке имитацией лицо изменяет свои биологические или физические характеристики, например внешний вид, для того чтобы соответствовать зарегистрированному субъекту данных. Индивид может также скрывать или маскировать свои биометрические характеристики, для того чтобы избежать распознавания. Например, в системе распознавания лиц маскировка может быть осуществлена за счет кепки и солнечных очков для сокрытия лица. Индивид может также искажать свои биометрические характеристики, например, нанося клей на пальцы или надевая контактные линзы или линзы с рисунком. Подделать биометрические характеристики другого лица сложнее, чем маскировать собственные биометрические характеристики, но тем не менее это вполне возможно.

Способы мошенничества в сфере биометрии лица, отпечатков пальцев и РОГ описываются во многих исследованиях (см. [29], *[65]—[69]*). Испытания на обнаружение атаки на биометрическое предъявление (испытания на возможность быть введенным мошенником в заблуждение) возможны в нескольких биометрических технологиях, например: в случае систем распознавания диктора мошенничество можно значительно затруднить, если при авторизации субъекту будет необходимо произнести цифры, которые в случайном порядке выбираются компьютером; систем распознавания по РОГ можно проверять наличие колебаний зрачка; систем распознавания по отпечаткам пальцев можно проверять кровоток. Вероятность мошенничества может быть снижена посредством применения совокупности множества биометрических характеристик (например, отпечатки десяти пальцев или РОГ и лицо) наряду с работой обученных операторов.

11.4 Целостность процесса биометрической регистрации

Использование биометрии не исключает необходимости в надлежащем подтверждении информации, удостоверяющей личность заявителя, или в авторизациях. Биометрическая система может не только не верифицировать истинность самой зарегистрированной идентификационной информации, но и не устанавливать автоматически с полной достоверностью связь с внешней идентификационной информацией. Определение «истинности» идентификационной информации субъекта при необходимости происходит в процессе биометрической регистрации по достоверным внешним документам, таким как свидетельство о рождении, паспорт, идентификационная карта или водительское удостоверение. Биометрические характеристики связывают субъект с зарегистрированной идентификационной информацией и соответствующими авторизациями, которые достоверны настолько, насколько достоверен исходный процесс определения.

Однако не всем системам необходима информация о настоящем имени или идентификационных данных субъекта. Биометрические характеристики могут быть использованы в качестве псевдоанонимной идентификационной информации, тем самым впоследствии значительно увеличивая уровень безопасности конфиденциальных данных в системах авторизации.

Все биометрические характеристики со временем изменяются вследствие старения тела, травм или заболеваний субъекта. В силу этих обстоятельств может потребоваться повторная биометрическая регистрация. Если системе требуется «истинная» идентификационная информация или полная идентификационная информация, то для перерегистрации в ней потребуется предоставление достоверных удостоверяющих документов. Как для биометрической регистрации, так и для перерегистрации необходимо присутствие субъекта, регистрацию которого проводят. В противном случае не представляется возможным достоверно определить то, что зарегистрированная биометрическая характеристика принадлежит телу именно того субъекта, который ее предоставляет. Механизмы обновления зарегистрированного биометрического шаблона могут быть также использованы для периодического обновления зарегистрированных биометрических контрольных шаблонов на основе биометрических образцов, полученных в транзакциях после биометрической регистрации. Целью обновления биометрического шаблона является автоматическая адаптация биометрического контрольного шаблона с течением времени. При этом учитывают различия в биометрических данных, предоставляемых в каждом случае, в том числе по причине старения, для того чтобы свести к минимуму воздействие таких различий на эксплуатационные характеристики распознавания.

12 Биометрия и конфиденциальность

12.1 Общие положения

Распознавание при близком осмотре тела причиняет дискомфорт тем людям, которые могут считать, что биометрия нарушает их конфиденциальность. Конфиденциальность — это юридически и культурно обусловленная концепция, которая чрезвычайно важна и может напрямую повлиять на успех развертывания любой биометрической системы.

Понятие «конфиденциальность» в разных культурах интерпретируется совершенно по-разному. Официальное определение конфиденциальности в каждой стране имеет свое объяснение (*см. [69]*). Классическим определением конфиденциальности является «естественное право быть оставленным в покое» (*см. [70]*), но современное определение конфиденциальности включает в себя также термин «конфиденциальность информации»: обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя (*см. [71]*), и право информационного самоопределения как право знать, кто получает информацию о субъекте, когда и с какой целью. Еще одним недавно установленным правом является защищенность субъекта от кражи его идентификационной информации или право на быструю и достоверную идентификацию в условиях аварии или несчастного случая.

Широкое распространение веб-технологий и мобильных технологий приводит к тому, что все больше людей совершают электронные операции по социальным и экономическим причинам с использованием личной информации, которую они обязаны предоставлять, включая биометрические данные. При этом многих беспокоят вопросы защиты такой информации, ее применения, механизмов контроля в месте доступа, использования, раскрытия и удаления.

Различные национальные и международные правовые и нормативные документы, касающиеся конфиденциальности персональных данных, основаны на ряде принципов, включая информирование физических лиц о следующем (*см. [72]*):

- когда и с какой целью (в каком объеме) проводят сбор персональных данных;
- кто запрашивает данные и в чем причина запроса, для того чтобы помочь решить, следует ли предоставлять и осуществлять контроль над всеми или частью таких персональных данных;
- каким сторонам могут быть раскрыты предоставленные персональные данные и при каких обстоятельствах;
- как физические лица могут получить доступ к своим персональным данным для проверки их точности и запроса изменений;
- как персональные данные будут защищены от несанкционированного доступа, изменения, использования и раскрытия;

- как долго будут храниться предоставленные персональные данные, включая стороны, которым персональные данные были раскрыты, прежде чем они будут окончательно удалены.

Примечание — В некоторых юрисдикциях биометрическая информация считается конфиденциальной персональной информацией, по отношению к которой установлены более жесткие обязательства для организаций, использующих биометрические данные, например: *Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»*, Директива Европейского союза 2016/680 об обработке персональных данных и обновление от 2014 г. к закону о конфиденциальности 1988 г. Австралии.

Целью этих документов является защита личных прав лиц, чьи данные обрабатываются, а также защита субъектов данных, а не просто защита данных. Применение биометрической системы означает в большинстве случаев использование персональных данных, таким образом, гарантирован режим конфиденциальности национальных законов. В зависимости от того, каким образом развернута система, использование биометрических данных может угрожать или защищать конфиденциальность субъекта данных. Возможность защиты особенно актуальна ввиду особых свойств биометрических характеристик, которые на протяжении всей жизни связаны с субъектом, в отличие от ПИН-кодов и паролей, которые лишь косвенно и слабо связаны с человеком. Поэтому при использовании биометрических технологий другие типы персональных данных могут быть лучше защищены от кражи и неправомерного применения в отличие от традиционных технологий. Таким образом, биометрия может быть как объектом, подлежащим охране, так и инструментом повышения степени защиты.

Основные меры защиты конфиденциальности, которые обычно применяют в биометрии, следующие:

- пропорциональность применения собранных биометрических данных;
- приемлемость в популяции кандидатов используемых биометрических данных с учетом культурных и религиозных особенностей, чувствительных к конфиденциальности;
- конфиденциальность биометрических данных, предоставленных индивидом;
- целостность биометрических данных, предоставленных индивидом;
- необратимость биометрических данных, полученных из биометрических образцов, предоставленных индивидом;
- несвязанность биометрических данных в контекстах, выходящих за рамки разрешений, согласованных при предоставлении биометрических образцов индивидом;
- возобновляемость биометрического контрольного шаблона, созданного на основе биометрических образцов, предоставленных индивидом, если они будут скомпрометированы.

При реализации этих мер защиты руководствуются рядом общих принципов, благодаря которым повышается конфиденциальность данных (см. *[73]*):

- ограничение на хранение и использование персональных данных;
- применение шифрования при использовании персональных данных;
- уничтожение необработанных данных в максимально сжатые сроки;
- анонимизация персональных данных, при возможности;
- отказ от использования центральных баз данных, если они не требуются;
- предоставление субъектам контроля над своими персональными данными;
- использование средств оценки и сертификации для проверки того, что заявка обеспечивает гарантию надлежащего уровня доверия.

Биометрия может быть также применена в качестве технологии усиления конфиденциальности информации. Принцип усиления конфиденциальности применим к биометрии с двух точек зрения: первая заключается в том, что при внедрении и применении биометрии должен соблюдаться корректный режим конфиденциальности с целью ее усиления; вторая — в том, что биометрия сама по себе может быть методом усиления конфиденциальности. Основной вопрос, касающийся концепции технологии усиления конфиденциальности и применения биометрии по принципу пропорциональности, — требуется или не требуется идентификация процессов традиционной информационной системы. В большинстве случаев необходимость в знании персональной идентификационной информации субъекта для предоставления ему прав доступа отсутствует. Однако существуют ситуации, в которых субъект, предоставляющий персональные данные, должен раскрыть свою личность для осуществления биометрической верификации.

12.2 Соразмерное применение биометрии

Во всех биометрических приложениях должен применяться принцип соразмерности. Это означает, что используемые биометрические данные должны быть адекватными, актуальными и нечрезмерными с точки зрения целей, для которых они собираются и обрабатываются. На практике это означает, что биометрическое приложение применено для связи биометрического контрольного шаблона с необходимыми и достаточными атрибутами личности лица для присвоения прав или разрешений, на которые имеет право конкретное лицо в контексте приложения. Такое присвоение происходит после проверки биометрического заявления, сделанного соответствующим лицом. Вместе с тем, имеют место случаи применения, особенно в контексте защиты границ, мошенничества и судебной экспертизы, когда отдельные лица должны в соответствии с законодательными нормами подвергаться процессам идентификации, и они могут содействовать или не содействовать этому процессу. Кроме того, в праве или авторизации может быть отказано, если в результате процесса идентификации по оценкам регулирующего органа существует неприемлемый риск для сообщества в случае предоставления данного права или авторизации. Таким образом, к основной цели процесса идентификации должно всегда применяться понятие соразмерности (*см. [74]*).

12.3 Приемлемость биометрических технологий

Приемлемость биометрических технологий тесно связана с личными предпочтениями, ценностями и нормами, на которые влияют исторические, социальные и культурные предпосылки, поэтому существуют различные значения и нормы предпочтений в различных географических районах и группах населения, что приводит к различиям в приемлемости биометрических технологий.

Для некоторых биометрических технологий необходим физический контакт субъекта с системой (например, в случае биометрического сканера, регистрирующего отпечаток пальца), что не отличается от применения обычной клавиатуры для ввода ПИН-кода. Для других биометрических систем требуется освещение глаза субъекта, например при регистрации изображения сетчатки. Многие технологии крайне неинтрузивны, такие как распознавание субъекта по изображению лица или РОГ. Для ряда культур считается недопустимым показывать лицо перед камерой, в других — отпечаток ладони связан с библейским «знаком зверя». Для того чтобы приспосабливаться к культурным традициям, необходимо создавать большое количество различных биометрических технологий.

Можно с успехом оспаривать тот факт (*см. [75], [76]*), что тело не тождественно субъекту, которому оно принадлежит. В то время как ПИН-коды и пароли идентифицируют личность, биометрия идентифицирует тело. Биометрические характеристики могли бы связать различные психологические портреты личности, которые люди демонстрируют при общении в рамках социальных структур. Биометрические данные, если они будут собираться повсеместно без надлежащего контроля, могут способствовать соотнесению данных, например трудовых книжек субъектов с их историями болезни. Объединение подобных данных о субъекте может быть проведено на законных основаниях, однако источники биометрических данных должны оставаться анонимными, и ни один субъект не должен быть идентифицирован. Аналогичные средства безопасности необходимы при повсеместном распространении биометрических технологий.

12.4 Конфиденциальность биометрических данных

Хищение и подделка персональной идентификационной информации являются серьезными и все более обостряющимися проблемами. На сегодняшний день существует большое количество способов избежать деятельности субъекта под разными цифровыми идентичностями с целью обеспечения безопасности персональной конфиденциальной информации, а также прав и привилегий субъекта, включая возможности скрываться под его цифровой идентичностью. Поэтому важное требование конфиденциальности заключается в том, что биометрические данные, хранящиеся в составе личности записи данных или иным образом, останутся в тайне.

Конфиденциальность биометрических данных [38], как правило, достигается с помощью:

- хранения биометрических контрольных шаблонов (или их частей) на персональном токене или карте вместо использования централизованных баз данных для предотвращения угроз конфиденциальности в результате нарушения безопасности централизованной базы данных (например, когда злоумышленник получает незаконный доступ к централизованной базе данных и публикует ее содержимое);
- шифрования биометрических контрольных шаблонов с использованием ключа, известного только оператору приложения и/или субъекту данных.

12.5 Целостность биометрических данных

В процессе принятия решений после оценки результатов биометрического сравнения лицу могут разрешить или отказать в предоставлении соответствующих прав и разрешений, и для оператора биометрической системы, контролирующих органов и соответствующего лица важно, чтобы биометрические данные всегда сохранялись в целостности. Решения, основанные на недостоверных биометрических данных, могут лишить человека его прав и полномочий и привести к ненужному вмешательству в его личную и частную жизнь.

Согласно 11.2 использование алгоритмов МАС или алгоритмов цифровой подписи может обеспечить целостность биометрических данных.

12.6 Необратимость биометрических данных

Вполне возможно, что наблюдатель за биометрической информацией, в частности за необработанной биометрической информацией, которая может содержаться в зарегистрированном биометрическом образце, может истолковать ее как означающую, что человек имеет определенные медицинские заболевания или принадлежит к определенной расе или религии, что считается персональной и конфиденциальной информацией.

При создании биометрических шаблонов из зарегистрированных биометрических образцов для целей создания биометрического контрольного шаблона или биометрического сравнения алгоритмы извлечения биометрических признаков выполняют сокращение данных и удаление избыточности, тем самым увеличивая сложность использования извлеченных биометрических признаков для получения медицинских или этнических данных. Эти подходы к минимизации данных направлены на снижение риска утечки информации из биометрических данных. Тем не менее по крайней мере до 2007 г. не проводилось систематических исследований в отношении дополнительной информации в биометрических шаблонах и степени, в которой такая информация, как состояние здоровья, все еще может быть получена (*см. [74]*). Известно, что знание обученного собственного пространства РСА в сочетании с собственными значениями РСА для индивида позволяет реконструировать лицо индивида (*см. [77]*). Информация о минуциях отпечатков пальцев также может быть получена из биометрических шаблонов и использована для создания искусственных отпечатков пальцев (*см. [78]*).

В последнее время значительное число исследований направлено на методы, которые усложняют вычислительные операции по извлечению биометрических признаков из хранимых биометрических шаблонов. Современные методы (*см. [57]*), позволяющие этого достигнуть, включают:

- шифрование с использованием ключа, известного только оператору системы и/или субъекту данных, предотвращает доступ внешних наблюдателей к биометрическим данным;
- использование PI и необратимых преобразований для обеспечения средств предотвращения доступа к биометрическим характеристикам субъекта данных.

12.7 Несвязанность биометрической информации

Использование биометрических данных для целей, отличных от целей, сообщаемых физическому лицу во время сбора биометрических данных, представляет для этого лица различные риски. Например, биометрические данные могут быть использованы для выявления связей в информации, имеющейся у различных организаций, которые не подпадают под сферу применения, для которой данные первоначально собраны. Это может привести к тому, что какое-либо лицо окажется в неблагоприятном положении, например отказ в предоставлении кредита на основе кредитной информации, полученной из фондов данных финансовых организаций *(например, бюро кредитных историй)* с использованием биометрической информации в качестве связующего механизма.

Для снижения рисков для индивида, связанных с попытками несанкционированного подключения, могут быть использованы различные механизмы (*см. [57]*) как отдельно, так и в сочетании, в том числе:

- шифрование биометрических контрольных шаблонов с использованием различных (секретных) ключей или механизмов в разных приложениях;
- независимые PI, созданные на основе биометрических контрольных шаблонов (диверсификация);
- логическое или физическое разделение записи данных биометрической регистрации и соответствующей записи данных биометрического контрольного шаблона или компонентов PI и AD, где используются RBR;
- использование несовместимых алгоритмов извлечения биометрических признаков или форматов обмена биометрическими данными между приложениями.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных национальных и межгосударственных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном документе

Таблица ДА.1

Обозначение ссылочного национального, межгосударственного стандарта	Степень соответствия	Обозначение и наименование соответствующего международного документа
ГОСТ ISO/IEC 2382-37—2016	IDT	ISO/IEC 2382-37:2012 «Информационные технологии. Словарь. Часть 37. Биометрия»
ГОСТ Р 58293 (ИСО/МЭК 19785-1:2015)	MOD	ISO/IEC 19785-1:2015 «Информационные технологии. Единая структура форматов обмена биометрическими данными. Часть 1. Спецификация элементов данных»
Примечание — В настоящей таблице использованы следующие условные обозначения степени соответствия стандартов: - IDT — идентичный стандарт; - MOD — модифицированный стандарт.		

Приложение ДБ
(справочное)

Сопоставление структуры настоящего стандарта со структурой примененного в нем международного документа

Таблица ДБ.1

Структура настоящего стандарта	Структура международного документа ISO/IEC TR 24741:2018
Приложение ДА Сведения о соответствии ссылочных национальных и межгосударственных стандартов международным стандартам, использованных в качестве ссылочных в примененном международном документе	—
Приложение ДБ Сопоставление структуры настоящего стандарта со структурой примененного в нем международного стандарта	—
Примечание — Сопоставление структуры стандартов приведено начиная с приложения ДА, так как предыдущие разделы стандартов идентичны.	

Библиография

[1] IBM. 1970. The Considerations of Data Security in a Computer Environment, Technical Report G520-2169, White Plains, NY

[2] Bertillon A. 1889. Alphonse Bertillon's Instructions For Taking Descriptions For The Identification Of Criminals And Others, By Means Of Anthropometric Indications, translated by Gallus Muller. Whitefish: Kessinger Publishing

[3] Faulds H. 1880. On the Skin Furrows of the Hand, Nature, 22, 605

[4] Herschel W.J. 1880. Skin Furrows of the Hand, Nature, 23, 76

[5] Fejfar A. 1978. Combining techniques to improve security in automated entry control, Carnahan Conference on Crime Countermeasures

[6] Twain M. 1893. Pudd'nhead Wilson, The Century, serialized 47(2) — 48(2), New York: The Century Company

[7] Osborn S. 1929. Questioned Documents. Chicago: Nelson-Hall

[8] Simon C., & Goldstein I. 1935. A new scientific method of identification. New York State Journal of Medicine, 35, 901—906

[9] Potter R.K., Kopp G.A., Green H.C. 1947. Visible Speech, New York: van Nostran Co

[10] Chang S.H., Pihl G.E., Essignmann M.W 1951. Representations of Speech Sounds and Some of Their Statistical Properties, Proc. Institute of Radio Engineers, 147

[11] Pruzansky S. 1963. Pattern-matching procedure for automatic talker recognition, Journal of the Acoustical Society of America, 26, 403—406

[12] Trauring M. 1963a. On the automatic comparison of finger ridge patterns, Nature, 197, 938—940

[13] Trauring M. 1963b. Automatic comparison of finger ridge patterns, Hughes Research Laboratory Report, 190, Malibu

[14] Bledsoe W.W. 1966. Man-machine facial Recognition: Report on a large-scale experiment, Technical Report PRI22, Panoramic Research Inc, Palo Alto, CA

[15] Goldstein A.J., Harmon L.D., Lesk A.B. 1971. Identification of human faces, Proc. Institute of Electrical and Electronic Engineers, 59, 748—760

[16] Wegstein J. 1970. Automated Fingerprint Identification, Technical Note 538, National Bureau of Standards

[17] Messner W.K., Cleciwa C.A., Kibbler G.O.T.H., Parlee W.L. 1974. Research and Development of Personal Identity Verification Systems, Proceedings 1974 Carnahan and International Crime Countermeasures Conference, University of Kentucky

[18] Fejfar A. 1978. Combining techniques to improve security in automated entry control, Carnahan Conference on Crime Countermeasures

[19] Meissner P. 1977. Guidelines on evaluation of techniques for automated personal identification, National Bureau of Standards, FIPS PUB 48

[20] https://mvd.ru/upload/site1/folder_page/001/930/393/ADIS.pdf

[21] Flom L., & Safir A. 1987. Iris recognition system, U.S. Patent 4,641,349

[22] Daugman J. 1993. High confidence visual recognition of persons by a test of statistical independence, IEEE Trans. on Pattern Analysis and Machine Intelligence 15, 1148—1161

[23] ISO/IEC 19794-3:2006, Information technology — Biometric data interchange formats — Part 3: Finger pattern spectral data

[24] ISO/IEC 24722:2007, Information technology — Biometrics — Multimodal and other multibiometric fusion

[25] ISO/IEC 19795-1:2006, Information technology — Biometric performance testing and reporting — Part 1: Principles and framework

[26] Phillips P.J., Martin A., Wilson C.L., Przybocki M. 2000. An introduction to evaluating biometric systems, Computer, 33, 56—63

[27] National Institute of Standards And Technology Multimodal Information Group (1996—2012). Speaker Recognition Evaluation

[28] National Institute Of Standards And Technology (1993—1997). Facial Recognition Technology (FERET) Database Evaluation

[29] Blackburn D., Bone M., Grother P., Phillips P.J. 2001. Facial Recognition Vendor Test 2000: Evaluation Report

[30] Phillips P., Grother P., Micheals R., Blackburn D., Tabassi E., Bone J. 2003. Face recognition vendor test 2002: Evaluation report, National Institute of Standards and Technology, Tech. Report, NISTIR 6965

[31] Phillips P.J., Scruggs W.T., O'toole A.J., Flynn P.J., Bowyer K.W., Schott C.L., Sharpe M. 2007. FRVT 2006 and ICE 2006 Large-scale results. National Institute of Standards and Technology, Tech. Report NISTIR 7408

[32] Grother P., Quinn G.W., Phillips P.J 2010. Evaluation of 2-D still-image face recognition algorithms. National Institute of Standards and Technology, Tech. Report, NISTIR 7709

[33] Grother P., & Ngan M 2014. Face recognition vendor test (FRVT): Performance of face identification algorithms. National Institute of Standards and Technology, Tech. Report, NISTIR 8009

[34] Maio D., Maltoni D., Cappelli R., Wayman J.L., Jain A.K. 2002. FVC2000: Fingerprint verification competition. IEEE Trans. on Pattern Analysis and Machine Intelligence. 24, pp. 402—412

[35] Maio D., Maltoni D., Cappelli R., Wayman J.L., Jain A.K. 2002. FVC2002: Second fingerprint verification competition. Proceedings of the 16*th* International Conference on Pattern Recognition (ICPR'02) volume 3, pp. 811—814

[36] Cappelli R., Maio D., Maltoni D., Wayman J.L., Jain A.K. 2006. Performance evaluation of fingerprint verification systems. IEEE Trans. on Pattern Analysis and Machine Intelligence. 28, pp. 3—18

[37] Cappelli R., Ferrara M., Franco A., Maltoni D. 2007. Fingerprint verification competition 2006, Biometric Technology Today, vol. 15, no. 7—8, pp. 7—9

[38] Wilson C.L., Grother P.J., Michaels R.J., Otto S.C., Watson C.I., Hicklin R.A., Korves H., Ulery B., Zoepfl M. 2004. Fingerprint vendor technology evaluation 2003: Summary of results and analysis report. National Institute of Standards and Technology, Tech. Report NISTIR 7123

[39] Watson C., Fiumara G., Tabassi E., Cheng S.L., Flanagan P., Salamon W. 2014. Fingerprint vendor technology evaluation 2012: Evaluation of fingerprint matching algorithms, National Institute of Standards and Technology, Tech Report, NISTIR 8034

[40] Watson C.I., & Wilson C.L 2005. Effect of Image Size and Compression on One-to-One Fingerprint Matching. National Institute of Standards and Technology, Tech Report, NISTIR 7201

[41] Grother P.J., Mccabe R., Watson C.I., Indovina M.D., Salamon W.J., Flanagan P.A., Tabassi E., Newton E.M., Wilson C.L 2006. MINEX Performance and Interoperability of the INCITS 378 Fingerprint Template. National Institute of Standards and Technology, Tech. Report, NISTIR 7296

[42] International Biometric Group. 2005. Independent testing of iris recognition technology (ITIRT)

[43] Phillips P.J., Scruggs W.T., O'toole A.J., Flynn P.J., Bowyer K.W., Schott C.L., Sharpe M. 2007. FRVT 2006 and ICE 2006 Large-scale results. National Institute of Standards and Technology, Tech. Report NISTIR 7408

[44] Rodriguez J.R., Bouchier F., Ruehie M. 1993. Performance Evaluation of Biometric Identification Devices, Report SAND93-1930, Sandia National Laboratory Albuquerque

[45] Bouchier F., Ahrens J., Wells G. 1996. Laboratory evaluation of the Iriscan prototype biometric identifier. Technical report SAND96-1033, Sandia National Laboratories

[46] Mansfield A.J., Kelly G., Chandler D., Kane J. 2000. Biometric product testing final report

[47] Wayman J.L. 2000. Evaluation of the INSPASS Hand Geometry Data. In Wayman J.L. (Ed.), U.S. National Biometric Test Center Collected Works: 1997—2000, San Jose: San Jose State University

[*48*] ISO/IEC 29794-1:2016, Information technology — Biometric sample quality — Part 1: Framework

[*49*] ISO/IEC/TR 29198:2013, Information technology — Biometrics — Characterization and measurement of difficulty for fingerprint databases for technology evaluation

[*50*] ISO/IEC 19794-1:2011, Information technology — Biometric data interchange formats — Part 1: Framework

[*51*] ISO/IEC 19785-3:2007, Information technology — Common Biometric Exchange Formats Framework — Part 3: Patron format specifications

[52] Michaels R.J., Mangold K., Aronoff M., Kwong K., Marshall K. 2012. Specification for WS-Biometric Devices (WS-BD), Version 1, National Institute of Standards and Technology, Tech. Report, NISTSP 500—288

[53] ISO/IEC 30108-1:2016, Information technology — Biometric Identity Assurance Services — Part 1: BIAS services

[54] ISO/IEC 19784-1:2006, Information technology — Biometric application programming interface — Part 1: BioAPI specification

[55] ISO/IEC 24708:2008, Information technology — Biometrics — BioAPI Interworking Protocol

[56] Kent S.T, & Millett L.I. 2003. Who goes there? Authentication through the lens of privacy, Washington, D.C.: National Academies Press

[57] ISO/IEC 24745:2011, Information technology — Security techniques — Biometric information protection

[58] ISO/IEC 19772:2009, Information technology — Security techniques — Authenticated encryption

[59] Breebart J., Busch C., Grave J., Kindt E. 2008. A reference architecture for biometric template protection based on pseudo identities. In: BIOSIG 2008. Proceedings of the Special Interest Group on Biometrics and Electronic Signatures. Editor: Brömme, A. Bonn: Gesellschaft für Informatik, 2008, pp. 25—37

[60] Lummis R.C., & Rosenberg A 1972. Test of an ASV method with intensively trained professional mimics, Journal of the Acoustical. Society of America 51, 131

[61] Raphael D.E., & Young J.R. 1974. Automated Personal Identification, Palo Alto: SRI International

[62] Meissner P. 1977. Guidelines on evaluation of techniques for automated personal identification, National Bureau of Standards, FIPS PUB 48

[63] ISO/IEC 30107-1:2016, Information technology — Biometric presentation attack detection — Part 1: Framework

[64] Van Der Putte T.,& Keuning J. 2000. Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned, IFIP TC8/WG.8., Fourth Working Group Conference on Smart Card Research and Advanced Applications, 289—303

[65] Matsumoto T., Matsumoto H., Yamada K., Hoshino S. 2002. Impact of Artificial 'Gummy' Fingers on Fingerprint Systems, Proceedings SPIE, 4677

[66] Thalheim L., Krissler J., Ziegler P. 2002. Biometric Access Protection Devices and their Programs Put to the Test, C'T Magazine 11

[67] Bundesamt für Sicherheit in der Informationstechnik. 2004. An investigation into the performance of facial recognition systems relative to their planned use in photo identification documents — BioP I: Public final report. Available online at https:// www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/BioP/BioPfinalreportpdf.pdf?__blob=publicationFile (Date of Access 25 Jul 2016)

[68] Bundesamt für Sicherheit in der Informationstechnik. 2005. Untersuchung der Leistungsfähigkeit von biometrischen Verifikationssystemen — BioP II Öffentlicher Abschlussbericht https://www.bsi.bund.de/DE/Publikationen/Studien/BioPII/BioPII.html (Date of Access 25 Jul 2016)

[69] Alderman E., & Kennedy C. 1995. The Right to Privacy. New York: Vintage Books

[70] Warren S., & Brandeis L. 1890. The Right to Privacy, Harvard Law Review, 4, 193—220

[71] Westin A. 1967. Privacy and Freedom, Boston: Atheneum

[72] Robinson N., Graux H., Botterman M., Valeri L. 2009. Review of the European Data Protection Directive. Rand Europe

[73] ISO/IEC 24714-1:2008, Biometrics — Jurisdictional and societal considerations for commercial applications — Part 1: General guidance

[74] Kindt E., & Müller L. eds. 2007. Biometrics in identity management, Report D3.10, Future of Identity in the Information Society (FIDIS)

[75] Locke J 1690. An essay concerning human understanding, Book 2, Chapter 27

[76] Baker L.R. 2000. Persons and Bodies: A Constitution View. Cambridge: Cambridge University Press

[77] Adler A. 2003. Sample images can be independently restored from face recognition templates. Proc. Canadian Conference on Electrical and Computer Engineering 2003, pp. 1163—1166

[78] Hill C.J. 2001. Risk of masquerade arising from the storage of biometrics. Australian National University, 2001, p. 116

УДК 004.93'1:006.89:006.354 ОКС 35.040

Ключевые слова: информационные технологии, биометрия, общие положения

БЗ 12—2019/75

Редактор *Л.С. Зимилова*
Технический редактор *И.Е. Черепкова*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 21.11.2019. Подписано в печать 20.12.2019. Формат $60 \times 84^{1}/_{8}$. Гарнитура Ариал.
Усл. печ. л. 5,12. Уч.-изд. л. 4,61.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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