ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Информационные технологии

БИОМЕТРИЯ

Обучающая программа по биометрии

ISO/IEC TR 24741:2007
Information technology — Biometrics tutorial
(IDT)

Издание официальное

Москва
Стандартинформ
2012

gost.e-ecolog.ru

Предисловие

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

Сведения о стандарте

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 21 сентября 2011 г. № 326-ст

4 Настоящий стандарт идентичен международному документу ИСО/МЭК ТО 24741:2007 «Информационные технологии. Обучающая программа по биометрии» (ISO/IEC TR 24741:2007 «Information technology – Biometrics tutorial»)

5 ВВЕДЕН ВПЕРВЫЕ

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

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

© Стандартинформ, 2012

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

Содержание

1 Область применения . . . 1
2 Введение и общий обзор . . . 1
2.1 Понятие «биометрическая технология» . . . 1
2.2 История развития . . . 2
3 Обзор технологий . . . 3
3.1 Технологии, построенные на анализе изображения глаза . . . 3
3.1.1 Характеристики изображения РОГ . . . 3
3.1.2 Характеристики сетчатки глаза . . . 4
3.2 Технологии, построенные на анализе изображения лица . . . 4
3.3 Технологии, построенные на анализе гребней отпечатка пальца . . . 4
3.3.1 Сканирование папиллярного узора . . . 4
3.3.2 Верификация изображения отпечатка пальца . . . 5
3.3.3 Идентификация изображения отпечатка пальца . . . 5
3.3.4 Технологии, построенные на анализе изображения ладоней . . . 5
3.4 Технологии, построенные на анализе геометрии контура кисти руки . . . 6
3.5 Технологии, построенные на анализе геометрии контура пальца . . . 6
3.6 Технологии, построенные на анализе динамики подписи . . . 6
3.7 Технологии, построенные на анализе голоса . . . 7
3.8 Технологии, построенные на анализе рисунка вен . . . 7
3.9 Технологии, построенные на анализе динамики работы на клавиатуре . . . 8
3.10 Биометрические технологии в будущем . . . 8
3.10.1 Запах . . . 8
3.10.2 Анализ ДНК . . . 8
3.10.3 Форма ушей . . . 8
3.10.4 Асимметрия тела . . . 8
4 Обобщенная биометрическая система . . . 9
4.1 Принципиальная схема обобщенной биометрической системы . . . 9
4.2 Принципиальные компоненты обобщенной биометрической системы . . . 10
4.2.1 Подсистема захвата данных . . . 10
4.2.2 Подсистема передачи данных . . . 10
4.2.3 Подсистема обработки данных . . . 11
4.2.4 Подсистема хранения данных . . . 12
4.2.5 Подсистема сравнения . . . 13
4.2.6 Подсистема принятия решения . . . 13
4.2.7 Подсистема управления . . . 14
4.2.8 Интерфейс . . . 15
4.3 Функции обобщенной биометрической системы . . . 15
4.3.1 Регистрация . . . 15
4.3.2 Распознавание . . . 15
4.3.2.1 Верификация . . . 15
4.3.2.2 Идентификация . . . 16
5 Основные концепции . . . 16
6 Стандарты на биометрические технические интерфейсы . . . 18
6.1 Блоки биометрических данных и записи биометрических данных . . . 18
6.2 Единая структура форматов обмена биометрическими данными (ЕСФОБД) . . . 19
6.3 Стандарт БиоАПИ . . . 19
6.3.1 Биометрический программный интерфейс: спецификация биометрического программного интерфейса (ИСО/МЭК 19784-1) . . . 19
6.4 Стандарт протокола межсетевого обмена БиоАПИ . . . 20
7 Эксплуатационные испытания . . . 20
7.1 Общие сведения . . . 20
7.2 Виды эксплуатационных испытаний . . . 21
8 Биометрия и информационная безопасность . . . 22

9 Примеры областей применения . . . 23
9.1 Правоохранительные органы . . . 23
9.2 Гражданское применение . . . 23
9.2.1 Банковское применение . . . 24
9.2.2 Системы вознаграждений, льгот и соцобеспечения . . . 24
9.2.3 Контроль доступа к компьютерным системам . . . 24
9.2.4 Контроль иммиграции . . . 24
9.2.5 Идентификационные карты . . . 25
9.2.6 Контроль непосредственного доступа . . . 25
9.2.7 Применение в тюрьмах, следственных изоляторах и камерах предварительного заключения . . . 25
9.2.8 Телефонные системы . . . 25
9.2.9 Применения для регистрации времени, посещаемости и наблюдения . . . 25
9.2.10 Проверка граждан на криминальное прошлое . . . 25
10 Биометрия и конфиденциальность . . . 26
10.1 Общие положения . . . 26
10.2 Приемлемость биометрических технологий . . . 26
10.3 Защита от хищения персональных данных . . . 26
10.4 Конфиденциальность . . . 27
11 Заключение . . . 27
Приложение А(справочное) Краткая информация о биометрических стандартах . . . 28
А.1 Развитие биометрической стандартизации . . . 28
А.2 Области биометрической стандартизации и рабочие группы . . . 28
А.3 Стандарты уровня 1 (утверждены или находятся в процессе разработки) . . . 29
А.4 Стандарты уровня 2 (утверждены или находятся в процессе разработки) . . . 30
А.5 Стандарты уровня 3 (утверждены или находятся в процессе разработки) . . . 30
А.6 Стандарты уровня 4 (утверждены или находятся в процессе разработки) . . . 30
А.7 Стандарты уровня 5 (утверждены или находятся в процессе разработки) . . . 30
А.8 Стандарты уровня 6 (утверждены или находятся в процессе разработки) . . . 30
А.9 Стандарты уровня 7 (утверждены или находятся в процессе разработки) . . . 30
А.10 Словарь терминов (утверждены или находятся в процессе разработки) . . . 30
А.11 Краткая информация об используемых стандартах и технических отчетах . . . 30
А.11.1 Стандарты уровня 1 . . . 30
А.11.2 Стандарты уровня 2 . . . 35
А.11.3 Стандарты уровня 3 . . . 35
А.11.4 Стандарты уровня 4 . . . 36
А.11.5 Стандарт уровня 5 . . . 36
А.11.6 Стандарты уровня 6 . . . 37
А.11.7 Стандарты уровня 7 . . . 37
А.11.8 Стандарты словаря . . . 38
Приложение В(справочное) Термины и определения, используемые в биометрических стандартах . . . 39
В.1 Основные понятия . . . 39
В.2 Термины, связанные с данными . . . 39
В.3 Термины, связанные с захватом данных . . . 41
В.4 Термины, связанные с регистрацией . . . 41
В.5 Термины, связанные с процессами и системой . . . 42
В.6 Термины, связанные с личностью . . . 42
В.7 Термины, связанные с сопоставлением . . . 43
В.8 Термины, связанные с ЕСФОБД . . . 46
В.9 Термины, связанные с БиоАПИ . . . 46
В.10 Термины, связанные с приложениями . . . 47
В.11 Термины, связанные с эксплуатацией . . . 47
Библиография . . . 48

Введение

«Биометрическая аутентификация» представляет собой автоматическое распознавание человека на основе характерных биологических или поведенческих признаков. Данная область, в свою очередь, является частью более широкой области науки об идентификации человека.

К технологиям распознавания человека относят распознавание по отпечаткам пальцев, по геометрии лица, рук, по голосу и радужной оболочке глаза. При современном уровне технологического развития техника анализа ДНК не является полностью автоматической и подразумевает присутствие человека в качестве обработчика данных, поэтому термин «Биометрическая аутентификация» в этом случае неприменим (процесс не является автоматическим и быстрым, хотя в ближайшей перспективе может стать таковым).

Некоторые технологии (например, распознавание по радужной оболочке глаза) в большей степени основаны на биологических признаках, а некоторые (например, распознавание по динамике подписи) — на поведенческих признаках, но в то же время во всех техниках распознавания присутствуют как биологические, так и поведенческие элементы. Не существует полноценно «поведенческих» или «биологических» биометрических систем. «Биометрическую аутентификацию» часто называют «биометрией», несмотря на то, что этот более современный термин исторически употреблялся в контексте статистического анализа общих биологических данных.

Термин «биометрия» так же, как 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 годах XX века. Биометрические системы распознают «личности» посредством распознавания «тел». Для осознания характерных для данных технологий функциональных возможностей и ограничений существенно отличие между личностью и телом.

В общем случае биометрия представляет собой распознавание поведения человека и биологических структур при помощи компьютера 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 системе социального обеспечения и при выдаче водительских прав.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

БИОМЕТРИЯ

Обучающая программа по биометрии

Information technologies. Biometrics.
Biometrics tutorial

Дата введения — 2012—07—01

1 Область применения

Настоящий стандарт определяет структуру обучающей программы по биометрии. В обучающую программу включено описание архитектуры биометрических процессов и процессов как таковых. В приложениях настоящего стандарта представлены дополнительные сведения о национальных стандартах в области биометрии, термины и определения, применяющиеся в данных национальных стандартах в области биометрии.

2 Введение и общий обзор

2.1 Понятие «биометрическая технология»

Комплексный термин «биометрия» относится к количественному или статистическому анализу биологических характеристик. В этой связи мы заинтересованы во всех технологиях, которые предусматривают анализ характеристик человеческого организма для распознавания личности. Статистика применительно к биометрии обычно подразумевается в контексте биомедицины и является отдельной областью знаний. Наиболее распространенное определение биометрии применительно к задаче распознавания личности звучит следующим образом: биометрическая характеристика или признак (биометрический) — это уникальная, измеримая характеристика или признак, используемый для автоматического распознавания или верификации личности. Определение по ИСО/МЭК СТК 1/ПК 37 разделено на две части и в основном соответствует приведенному выше определению. Рекомендуется употреблять термин «биометрический» в качестве определения, в других случаях более уместным является употребление словосочетания «биометрическая характеристика» (как указано выше). Для употребления в качестве определения применяют термин:

биометрический — имеющий отношение к биометрии;

для употребления в качестве существительного применяют термин:

биометрия — автоматическое распознавание личности по поведенческим и биологическим характеристикам.

Таким образом, биометрические технологии связаны с физическими частями человеческого тела или индивидуальными признаками субъекта, и распознавание личности осуществляется либо на основе особенностей частей человеческого тела, либо на индивидуальных признаках субъекта, либо на том и другом одновременно. Следует отметить термин «автоматическое», указанный выше. На самом деле это значит, что биометрическая технология должна распознать или верифицировать субъекта быстро, автоматически и в режиме реального времени (более подробное определение различных биометрических технологий представлено в разделе 3). Наиболее распространенными физическими биометрическими характеристиками являются глаза, лицо, отпечатки пальцев, рука и голос, в то время как подпись, динамика работы с клави-

Издание официальное

атурой и походка являются наиболее распространенными поведенческими биометрическими характеристиками. Распознавание личности по ДНК на сегодняшний момент исключено, так как эта технология не является быстрым автоматическим процессом, но такое положение вещей может измениться уже через несколько лет.

2.2 История развития

На примитивном уровне биометрические характеристики применялись веками. Части нашего тела и особенности нашего поведения для распознавания использовались с незапамятных времен и продолжают использоваться в наши дни. Учение об отпечатках пальцев существовало еще в древнем Китае; мы часто помним и узнаем людей по их лицам, голосам, а подпись является общепринятым методом идентификации в банковской системе, 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 годов XIX века [3], [11]. Система Бертильона включала в себя измерение нескольких величин: рост, вес, длина и ширина головы, толщина щек, длина туловища, стоп, ушей, предплечья, средних пальцев и мизинцев. Также в систему входили категории цвета и узора радужной оболочки глаза (РОГ). До 80-х годов XIX века система Бертильона применялась во Франции для идентификации рецидивистов. Некоторое время спустя система стала применяться в США для идентификации заключенных и применялась до 20-х годов XX века. Несмотря на то, что исследования отпечатков пальцев британским управляющим колонией в Индии Уильямом Гершелем началось еще в конце 50-х годов XIX века, эти знания оставались неизвестными в западном мире до 80-х годов XIX века [13], [18], пока не стали пропагандироваться Сэром Фрэнсисом Гальтоном в научных работах (1888) [16] и Марком Твеном в литературе (1893) [47]. Работы Ф. Гальтона также включали в себя технологию идентификации личности по характеристикам лица.

К середине 20-х годов XX века дактилоскопия полностью вытеснила систему Бертильона в Бюро Расследований США (вскоре сменившимся Федеральным Бюро Расследований). Впрочем, исследования новых методов идентификации личности продолжались только в научном мире. Анализ почерка как метод был признан в 1929 году [36], а идентификация личности по сетчатке глаза — в 1935 году [44].

Однако ни одна из описанных выше технологий не являлась «автоматической», поэтому ни одна из них не отвечает определению «биометрическая аутентификация», используемому в настоящем стандарте. Автоматические технологии требуют автоматического и преимущественно быстрого вычисления. Эксперименты в области автоматического распознавания голоса с использованием аналоговых фильтров [38] начались в 40-х годах XX века и начале 50-х годов XX века [10]. В 1960-х годах во время набирающей скорость революции в вычислительной технике распознавание паттернов голоса [39] и отпечатков пальцев [46] считалось первоочередным применением автоматической обработки сигнала. В 1963 году 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». Вскоре начались исследования по распознаванию лица с использованием вычислительной техники [6], [17]. В 70-х годах XX века были зарегистрированы первые действующие системы идентификации по отпечатку пальца и геометрии контура кисти руки (например, система «Identimat»), доложены результаты официальных испытаний биометрических систем [52], проанализированы характеристики приборов, входящих в состав биометрических систем [14], [27], и опубликованы результаты тестирования [28].

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

В 80-х годах XX века системы сканирования и распознавания отпечатков пальцев, а также системы распознавания голоса стали устанавливаться на персональные компьютеры для контроля доступа субъектов к хранящейся на них информации. Системы распознавания личности по РОГ, основанные на концепции, которая была запатентована в 80-х годах XX века [15], стали доступны только в середине 90-х годов [12]. На сегодняшний день существует более десяти различных подходов, использующихся в доступных для приобретения систем, включающих в себя распознавания личности по геометрии контура кисти руки и пальца, паттернам РОГ и отпечатка пальца, изображениям лица, голосу, динамике подписи, работы на клавиатуре, паттернам вен руки.

Современные системы верификации по голосу многим обязаны технологическим достижениям 70-х годов XX века, в то время как технологии верификации по подписи и распознавания по лицу сравнительно новые технологии. Переход от исследований и развития к области коммерции продолжается и сегодня. 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 того, чтобы добиться полноценной работы системы, требуется время. Впрочем, такие системы уже сейчас применяются в самых разнообразных сферах и успешно доказывают свою работоспособность.

3 Обзор технологий

На сегодняшний день биометрические системы представлены многообразием видов и размеров. Биометрические системы представлены оборудованием, программным обеспечением, комплектующими, комплектами разработчика программного обеспечения и законченными решениями. Поставщики выводят такие системы на рынок и продают напрямую или через различные системы сбыта, например, специализирующиеся на системной интеграции, стратегическом партнерстве или через фирмы-посредники, которые вносят добавленную стоимость. Все биометрические системы работают по одним и тем же принципам: захват данных, извлечение данных и сопоставление данных. Так как до сих пор биометрические технологии строятся на анализе различных частей человеческого тела, то работа каждой технологии и системы различается. В данном разделе рассматривается функционирование каждой биометрической технологии в рамках четырех стадий: захват данных, извлечение данных, сопоставление данных и принятие решения.

3.1 Технологии, построенные на анализе изображения глаза

В настоящее время биометрические технологии, построенные на анализе глаза, характеризуются высочайшей точностью и способны найти различия даже между близнецами. Эти технологии могут быть разделены на две отдельные технологии, анализирующие биометрические характеристики РОГ и сетчатки глаза.

3.1.1 Характеристики изображения РОГ

РОГ представляет собой цветное кольцо текстурированной материи вокруг зрачка. Каждая РОГ имеет уникальную структуру, особый комплекс паттернов. Она представляет собой комбинацию особых характеристик, таких как лакуны, углубления, нити, ямки, радиальные кольца и жилки. Считается, что искусственное воспроизведение РОГ невозможно из-за ее уникальных свойств, поскольку не существует двух одинаковых РОГ. РОГ тесно связана с человеческим мозгом, поэтому считается, что ее нельзя использовать для биометрического распознавания после смерти. По этой причине невозможно создать искусственную РОГ и, скорее всего, при использовании трупного материала РОГ не удастся «обмануть» биометрическую систему. Это означает, что идентификация мертвого тела с использованием зарегистрированных данных РОГ невозможна, в то время как код ДНК успешно применяется и после смерти субъекта при условии отсутствия влияния жары и соленой воды.

В большинстве систем полутоновое изображение РОГ получают в ближнем инфракрасном (ИК) диапазоне с целью максимизировать детали в случае темных глаз, некоторые системы способны захватывать данные о РОГ также и в цвете. Данная процедура должна проходить при хорошем освещении. Контактные линзы без рисунка не мешают захвату данных, а наличие солнечных очков и очков с линзами не допускается, так как это может повлиять на процесс захвата данных.

Уникальные признаки РОГ извлекаются из захваченного образца при помощи блока извлечения признаков. Далее эти признаки РОГ преобразовываются в уникальный математический код и сохраняются в виде шаблона (биометрического эталона) для конкретного субъекта.

3.1.2 Характеристики сетчатки глаза

Сетчатка глаза представляет собой слой кровеносных сосудов, находящихся на внутренней оболочке глаза. Аналогично РОГ сетчатка глаза формирует уникальный рисунок, и считается, что ее невозможно применять для биометрической идентификации после смерти субъекта.

Необходимо провести точную регистрацию, включающую в себя расположение глаза на одной оси с оптической осью системы захвата данных для получения оптимального считывания. Глаз позиционируется перед системой захвата данных так, чтобы расстояние варьировалось от восьми сантиметров до одного метра. Человек должен через окулярную трубку проследить за серией отметок и расположить их на одной оси. После этой процедуры сканер фокусирует глаз в достаточной степени для того, чтобы захватить рисунок сетчатки глаза.

Уникальное расположение кровеносных сосудов сетчатки глаза фиксируется блоком извлечения признаков. Далее эти признаки преобразовываются в уникальный математический код и сохраняются в виде шаблона (биометрического эталона) для конкретного субъекта.

3.2 Технологии, построенные на анализе изображения лица

Основным элементом в распознавании людей является лицо. Автоматическая идентификация личности с помощью анализа лица является сложной процедурой, для которой требуются сложные методы искусственного интеллекта и машинного обучения. Рядом биометрических компаний и исследовательских институтов разработаны системы распознавания лица, в которых для регистрации биометрических данных используется стандартное видеоизображение или тепловизионное изображение (термограмма) лица. На результаты сравнения лиц, которое проводится в биометрических системах, могут повлиять такие факторы, как возрастные изменения внешности человека, растительность на лице, наличие очков и положение головы. Для проведения корректного сопоставления новых биометрических образцов с ранее зарегистрированными шаблонами необходимо использовать машинное обучение.

В методах распознавания лица, основанных на видеоизображении, используется изображение лица или серия изображений лиц, захватываемых видеокамерой. Точность расположения лица субъекта и условия освещения могут повлиять на работу системы. Обычно захватывается изображение лица целиком, на котором затем могут проставляться контрольные точки лица. Например, расположение глаз, рта и ноздрей может быть таким, что будет создан уникальный шаблон. Трехмерные модели лица могут создаваться разными способами, такими как проецирование ИК-сетки («структурированного света»), слияние нескольких изображений или использование информации о полутонах в отдельном изображении. На тепловизионном изображении лица отображается количество тепла, вызванное притоком крови к лицу. Тепловизор захватывает невидимый, вызванный теплом рисунок кровеносных сосудов, находящихся под кожей. Так как при захвате изображений лица ИК-камерами освещение не является необходимым, системы могут захватывать изображения в темноте. Однако ИК-камеры являются более дорогими по сравнению с другими видами видеокамер.

С помощью специальных алгоритмов или нейтронной сети в ядре распознавания биометрической системы изображение лица преобразуется в шаблон, а далее — в уникальный математический код. Этот код сохраняется в виде шаблона (биометрического эталона) для конкретного субъекта.

3.3 Технологии, построенные на анализе гребней отпечатка пальца

3.3.1 Сканирование папиллярного узора

Биометрия изображения отпечатков пальцев является точным методом биометрической идентификации и верификации. Большинство АСДИ сопоставления «один-ко-многим» анализируют мелкие уникальные отметки на отпечатке пальца, называемые минуциями. Их можно определить как окончания гребней на отпечатке пальца или бифуркации (ветви, произведенные гребнями на отпечатке пальца). Некоторые системы распознавания отпечатков пальцев также анализируют мелкие потовые поры на пальце, которые аналогично минуциям расположены уникально, создавая возможность отличить отпечаток пальца одного человека от другого. Также могут быть проанализированы плотность изображения пальца или расстояние между гребнями.

На отпечатки пальцев могут влиять некоторые условия. Например, при сборе данных грязные, сухие или потрескавшиеся подушечки пальцев значительно снижают качество захватываемого изображения отпечатка пальца. На качество изображения отпечатка пальца могут повлиять также возраст, пол и национальность субъекта. Еще одним значительным фактором является то, каким образом субъект прикладывает палец к биометрическому сканеру. Изображение отпечатка пальца может быть неудовлетворительного

качества, если палец слишком сильно прижат к поверхности биометрического сканера. Поставщики принимают указанные выше проблемы во внимание, и таким образом биометрические сканеры проектируются с учетом эргономических требований для оптимизации процесса получения отпечатка пальца.

Основным различием между различными дактилоскопическими техниками, существующими на рынке, является способ захвата изображения отпечатка пальца. В системах верификации «один-к-одному» применяются четыре основные техники захвата данных: оптическая, тактильная, или термальная, емкостная и ультразвуковая. В большинстве систем сопоставления «один-ко-многим» при захвате изображения отпечатка пальца используется оптический метод или электронное сканирование изображений с листа бумаги.

3.3.2 Верификация изображения отпечатка пальца

Техника получения изображения оптическим методом включает в себя использование пучка света, преломляемого призмой. Субъект прикладывает палец к стеклянной поверхности биометрического сканера, которая называется планшетом. Свет попадает на отпечаток пальца, и захватывается оттиск.

В тактильной, или термальной, технике для получения данных об отпечатке пальца используется сложный силиконовый чип. Субъект прикладывает палец к датчику-чипу, чувствительному к теплу или давлению, оказываемому пальцем. Данные об отпечатке пальца захватываются.

Емкостные силиконовые датчики измеряют электрический заряд и выдают электрический сигнал в тот момент, когда палец оказывается на поверхности датчика. Основным элементом емкостной техники, так же как в тактильной или термальной технике, является датчик-чип. Емкостная техника заключается в анализе низших и высших точек гребней и впадин в отпечатке пальца. Электрический сигнал подается в тот момент, когда гребни отпечатка пальца контактируют с датчиком. Углубления не генерируют сигнал. Именно благодаря такому непостоянству электрического заряда воспроизводится изображение отпечатка пальца.

Захват изображения отпечатка пальца ультразвуковым методом основан на использовании звуковых волн, которые находятся вне диапазона слышимости человеческого уха. Палец прикладывают к биометрическому сканеру, и акустические волны измеряют плотность рисунка отпечатка пальца.

Блок извлечения признаков выделяет признаки отпечатка пальца. Уникальный математический код отпечатка сохраняется в виде шаблона (биометрического эталона) для конкретного субъекта.

3.3.3 Идентификация изображения отпечатка пальца

При идентификации «один-ко-многим» субъекты регистрируются при помощи оптического прямого сканирования, описанного выше для верификации изображения отпечатка пальца. АСДИ системы правоохранительных органов, также известные как станции регистрации, захватывают все десять отпечатков. Версия систем АСДИ, применяемая в гражданских целях, не захватывает все десять отпечатков пальцев и эффективно работает при наличии одного или двух отпечатков. Скрытые отпечатки (полученные на месте преступления или чернильные изображения на бумаге) также могут быть захвачены системой АСДИ при помощи планшетного сканера.

В случае АСДИ процесс биннинга отпечатков пальцев оптимизирует процесс выделения. Данные о минуциях извлекаются и сохраняются в виде шаблона (биометрического эталона) для конкретного субъекта.

Новый образец, захваченный либо устройством прямого считывания папиллярного узора, либо техникой сканирования скрытых или чернильных отпечатков, сопоставляется с имеющимися контрольными шаблонами в базе данных. Если использовался биннинг, то сопоставление будет проводиться с бином, содержащим идентичные признаки, а также с новым отпечатком.

3.3.4 Технологии, построенные на анализе изображения ладоней

Биометрия ладоней может быть поставлена в один ряд с биометрией отпечатков пальцев, особенно в технологии АСДИ. Гребни, впадины и минуции есть как на отпечатках пальцев, так и на ладони. Признаки ладони чаще всего анализируются при помощи техники оптического захвата. Данная область биометрической промышленности, в частности, ориентирована на правоохранительные органы, так как скрытые отпечатки ладоней так же крайне полезны в раскрытии преступлений, как и отпечатки пальцев. Однако поставщики обращают внимание на рынок контроля доступа и надеются заняться разработкой версий своей продукции применительно к гражданской сфере.

Характеристики биометрии ладоней преимущественно используются в идентификации «один-к-одному», а процесс захвата по сути аналогичен оптической технике, предназначенной для регистрации отпечат-

ков пальцев. Система регистрации отпечатка ладони захватывает ладонь в тот момент, когда она находится на биометрическом сканере. Скрытые и чернильные отпечатки ладоней также могут быть отсканированы и помещены в систему, как в случае с системами АСДИ.

Данные о минуциях извлекаются блоком извлечения признаков, признаки ладони сохраняются в виде шаблона (биометрического эталона) в базе данных.

Новый отпечаток, захваченный при помощи прямого сканирования, с использованием техники сканирования скрытых или расположенных на бумаге отпечатков, сопоставляется с базой данных контрольных шаблонов.

3.4 Технологии, построенные на анализе геометрии контура кисти руки

Для идентификации по геометрии контура кисти руки необходимы одно или несколько двухмерных изображений кисти руки, на которых определяется форма и измеряется длина пальцев и фаланг. Данная технология применяется с начала 80-х годов XX века преимущественно в области контроля доступа. Несмотря на то, что технология идентификации по геометрии контура кисти руки, как и технология идентификации по геометрии контура пальца (см. ниже), не обеспечивает максимальную точность распознавания, эта технология удобна в применении, и ее основное преимущество заключается в большой пропускной способности. По этой причине технологии идентификации по геометрии контура кисти руки и геометрии контура пальца часто применяются в парках отдыха для повторных проходов субъектов.

Субъект помещает кисть руки на считывающее устройство, располагая пальцы в соответствии с инструкцией по правильному положению пальцев. Зеркало отражает свет горизонтально вдоль тыльной стороны руки, создавая двумерную тень от кисти руки. Камера, расположенная над рукой, захватывает изображение. Далее выполняются измерения характеристик выбранных точек на кисти руки.

Блок извлечения признаков преобразует измерения в уникальный числовой идентификатор, на основе которого для данного субъекта создается шаблон (биометрический эталон).

Геометрия контура кисти руки используется преимущественно при верификации (сравнении «один-к-одному»). Полученный образец сравнивается с базой данных шаблонов (контрольных эталонов).

3.5 Технологии, построенные на анализе геометрии контура пальца

Многие поставщики биометрических услуг используют для идентификации личности геометрию контура пальцев или результаты измерения формы пальцев. В данной технологии используются те же принципы, что и в технологии идентификации по геометрии контура кисти руки. В зависимости от используемой биометрической системы может анализироваться геометрия контура одного или двух пальцев. Проводится измерение таких уникальных характеристик пальцев, как ширина, длина, толщина и размер фаланг.

Системы идентификации по геометрии контура пальцев могут проводить верификацию (сравнение «один-к-одному») или идентификацию (сравнение «один-ко-многим»). Основными преимуществами данных систем являются устойчивость к сбоям и большая пропускная способность.

Как и в системах верификации по отпечаткам пальцев, метод захвата изображений зависит от используемой системы. В настоящее время на рынке представлены две основные технологии получения изображений.

Первая заключается в измерении геометрии контура двух или более пальцев. Зеркало отражает свет горизонтально вдоль тыльной стороны кисти руки, создавая двухмерную тень от кисти руки. Камеры, расположенные над рукой, получают изображения и в трех координатах проводят измерение характеристик контура указательного и среднего пальцев правой либо левой руки.

Вторая технология заключается в том, что субъект помещает палец в специальный тоннель, в котором проводится измерение характеристик контура пальца в трех координатах.

Далее блок извлечения признаков обрабатывает результаты измерений и создает для данного субъекта шаблон (биометрический эталон).

3.6 Технологии, построенные на анализе динамики подписи

Биометрия подписи часто называется верификацией динамики подписи (ВДП) и заключается в анализе того, как мы пишем свое имя или визируем документ. Важно отметить, что метод заключается не в анализе самой подписи, а в анализе процесса ее получения. Именно в этом отличие ВДП от анализа законченных подписей на бумаге. При помощи технологии ВДП можно извлечь и измерить множество характеристик. К примеру, угол, под которым пишущий держит ручку, время, которое пишущий отводит на написание, скорость движения ручки и акселерацию, силу, с которой пишущий держит ручку, и то, сколько раз ручка отрывалась от бумаги, — все эти показатели могут быть рассмотрены как уникальные поведен-

ческие 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, а отсутствие этих знаний значительно усложнит подделку подписи.

Другим преимуществом биометрических технологий, построенных на анализе динамики подписи, является их распространенность в качестве метода подтверждения личности. Вместе с этим, технологии, построенные на анализе динамики подписи, применяются в 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 соцобеспечение, до управления документооборотом и использования электронной подписи.

Стоит отметить, что данные о динамике подписи могут быть захвачены при помощи электронного планшета без ведома субъекта.

Данные о подписи могут быть захвачены при помощи чувствительного пера или электронного планшета. В первом случае суть метода заключается в наличии чувствительных элементов-датчиков внутри пера, а второй метод основан на том, что планшет регистрирует уникальные характеристики динамики подписи. Одной из вариаций двух этих методов является акустическая эмиссия, которая измеряет звук, производимый ручкой во время контакта с бумагой. Как правило, для системы ВДП, как и для других биометрических техник, необходимо, чтобы субъект ввел свою подпись несколько раз, только в этом случае система может сформировать профиль характеристик подписи.

После выделения уникальных признаков подписи блок извлечения признаков кодирует данные и сохраняет в виде шаблона (биометрического эталона) для конкретного субъекта.

3.7 Технологии, построенные на анализе голоса

Распознавание субъекта является биометрической технологией верификации и идентификации говорящего по голосу. Не стоит путать распознавание субъекта с похожей не биометрической технологией распознавания речи, используемой для распознавания слов при диктовке или автоматической обработке инструкций, переданных по телефону.

Звук человеческого голоса является следствием резонанса, возникающего в речевом тракте. Особенности голоса определяются длиной речевого тракта и формами ротовой и носовой полостей.

В технологии измерения голоса может применяться либо текстонезависимый, либо текстозависимый метод. Другими словами, при захвате голоса можно использовать специально подготовленные вопросы, отвечая на которые, субъект будет произносить определенный текст, сочетающий фразы, слова или цифры (текстозависимый метод), или субъект может произносить любые фразы, слова или цифры без определенного задания (текстонезависимый метод). На сегодняшний день текстозависимые (с вопросом) техники доминируют в сфере коммерческих систем распознавания субъекта по голосу.

Технологии распознавания субъекта по голосу особенно полезны в приложениях, связанных с телефонами. Мы все разговариваем по телефону, а биометрическая система может быть встроена в частную или общественную телефонную сеть. Однако на работу систем распознавания субъекта влияют окружающие субъект шумы и помехи на линиях.

Субъект произносит в микрофон заранее подготовленную (текстозависимый метод) либо произвольную фразу (текстонезависимый метод). Данный процесс обычно повторяется несколько раз во время регистрации, чтобы позволить системе сформировать подходящий профиль голоса.

Блок извлечения признаков выделяет уникальный голосовой сигнал и создает шаблон (биометрический эталон). Предпочтительным методом является верификация «один-к-одному». Диктор произносит в микрофон фразу, далее происходит сопоставление нового образца голоса с биометрическим шаблоном.

3.8 Технологии, построенные на анализе рисунка вен

Биометрические технологии, анализирующие образцы рисунков вен, характеризуются высокой аутентификационной точностью. Вены, которые находятся в подкожной области тела каждого человека, формируют уникальный рисунок. Даже рисунки генетически идентичных близнецов имеют отличия. Более того, рисунок вен представляет собой данные внутри человеческого тела, которые не могут быть кем-то украдены при помощи обычного фотоаппарата или сведены каким-то образом с объектов, с которыми контактировал субъект (по сравнению с отпечатками пальцев). Рисунок вен может быть захвачен при помощи ИК-излучения. Кожа отражает ИК-излучение, поэтому может быть получено изображение. С другой стороны, более темное изображение рисунка вен получается в том случае, когда пониженный уровень гемоглобина

в вене поглощает ИК-излучение. Таким образом, система захвата изображения способна получить уникальный рисунок вен посредством более темного изображения.

В данной технологии выбираются такие части человеческого тела (ладонь, палец, запястье и тыльная сторона ладони), в которых присутствует уникальный рисунок кровеносных сосудов, следовательно, биометрический сканер может зарегистрировать эти данные. Рисунки вен извлекаются, кодируются блоком извлечения признаков и сохраняются в виде шаблона (биометрического эталона) для конкретного субъекта.

На данный момент существует два метода регистрации изображений вен, построенные на разных типах: отражение и передача. При первом типе на конкретный участок тела наводится ИК-излучение и проводится фотографирование. При втором типе ИК-излучение направляется сквозь часть человеческого тела, после чего проводится фотографирование.

При помощи техник обработки признаков изображения можно получить четкие и устойчивые паттерны вен.

3.9 Технологии, построенные на анализе динамики работы на клавиатуре

В биометрии клавиатурного почерка или динамике работы на клавиатуре анализируется ритм печати. Динамика работы на клавиатуре является поведенческой характеристикой и имеет свойство со временем развиваться, так как субъект учится печатать на клавиатуре, тем самым развивая свой уникальный образец печати. Основная цель технологии заключается в способности непрерывно проверять личность субъекта во время его работы на клавиатуре, то есть контролировать, что именно данный субъект работает за компьютером. Одна из проблем состоит в том, что субъекты могут уставать или отвлекаться от работы в течение дня, что заметно влияет на ритм печати.

3.10 Биометрические технологии в будущем

Биометрические технологии будущего, вероятно, будут усовершенствованными версиями биометрических технологий, описанных выше. Все биометрические технологии нуждаются в улучшениях процесса захвата (включая скорость, эргономичность, точность и качество захвата) и сопоставления (включая улучшенную точность, скорость и работу с низкокачественными данными в пределах допускаемых погрешностей). Несмотря на успех существующих технологий, исследования и развитие более разнообразных и интересных технологий будет продолжаться.

3.10.1 Запах

Система, анализирующая химический состав запаха тела, в настоящее время находится в стадии развития. Неинвазивные датчики системы способны захватывать запах частей тела, например, таких, как тыльная сторона ладони. Каждый уникальный запах человеческого тела состоит из химических летучих веществ. Данные вещества извлекаются системой и преобразуются в шаблон.

3.10.2 Анализ ДНК

Процесс анализа человеческого ДНК недостаточно автоматизирован, чтобы считать анализ ДНК биометрической технологией, несмотря на то, что результат можно получить в течение 10 минут. Однако в настоящее время получение пробы человеческого ДНК является инвазивной технологией, для этого необходимы образцы ткани, крови или чего-то иного, относящегося к телу.

3.10.3 Форма ушей

Идентификация личности по форме ушей активно применяется в правоохранительных органах, т. к. уши видны на фотографиях, но в настоящее время данный процесс проводится вручную. Развитие данной технологии нацелено на ее использование в биометрии в сочетании с технологией распознавания лица, особенно в отношении изображений в профиль.

3.10.4 Асимметрия тела

В настоящее время происходит развитие новой довольно интересной технологии, которая заключается в измерении (мелких) потенциальных различий, которые существуют между правой и левой частью тела. Данные потенциальные различия создают уникальный рисунок, повторяющийся с каждым ударом сердца (из-за движения крови по всему телу). Измерения проводится с помощью датчика размером с кредитную карточку, на котором размещены контакты, прикрепляемые к правой и левой рукам.

4 Обобщенная биометрическая система

Примечание — В разделе А.2 приложения А приведена многоуровневая модель стандартов в области биометрии.

4.1 Принципиальная схема обобщенной биометрической системы

Разные биометрические системы имеют много общих элементов. Сбор биометрических образцов субъекта проводят с помощью датчика. С выхода датчика сигнал посылают на процессор, с помощью которого извлекают отличительные повторяющиеся характеристики образца (признаки), отбрасывая все остальные элементы. Полученные в результате выделения признаки хранятся в базе данных в виде «эталона», который иногда называется «биометрический эталон» или (в данном случае) биометрический «шаблон». Образец (без выделения признаков) также может храниться в виде биометрического шаблона. Новый образец сравнивают с конкретным шаблоном, множеством шаблонов или со всеми шаблонами базы данных для определения соответствия. Решение относительно запрошенной идентичности принимают на основании соответствия признаков образца и сравниваемого шаблона или шаблонов.

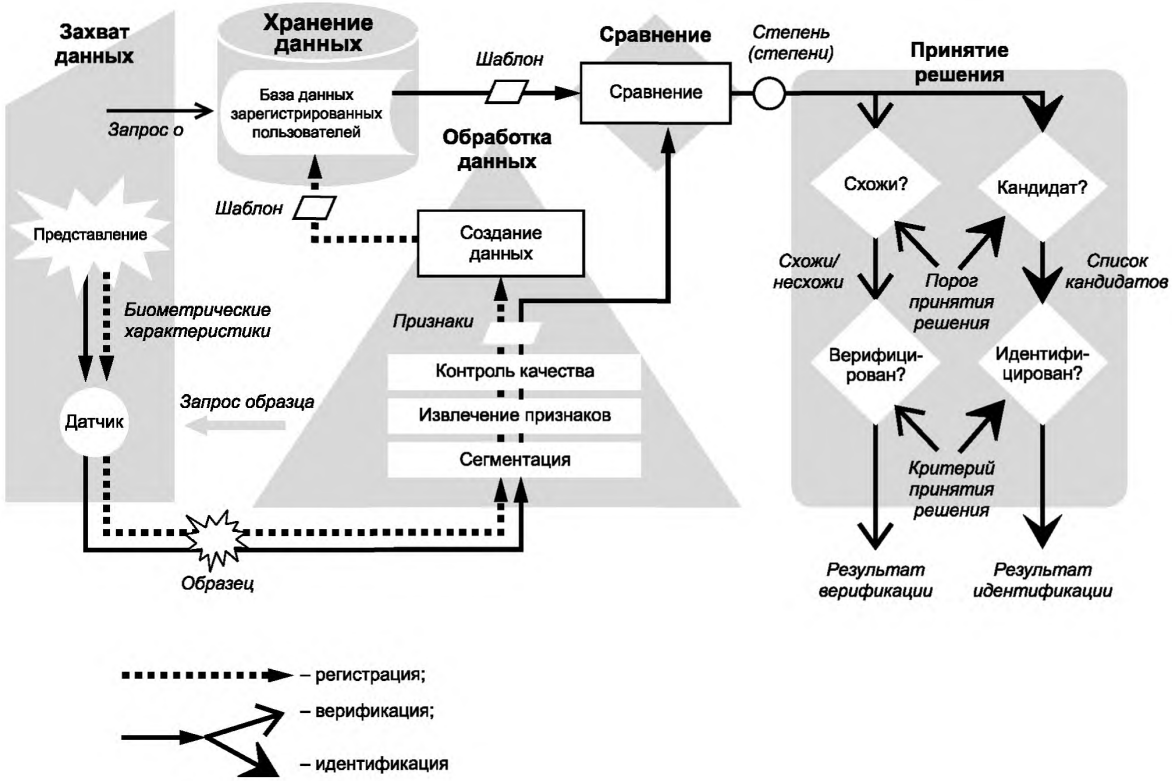

Рисунок 1 — Компоненты обобщенной биометрической системы

Информационные потоки внутри обобщенной биометрической системы, содержащей подсистемы захвата данных, обработки сигнала, хранения, сравнения и принятия решения, показаны на рисунке 1. На рисунке 1 также показаны процесс регистрации и работа систем верификации и идентификации. Детальные описания подсистем приведены в следующих подразделах. Состав реальной биометрической системы может отличаться от состава обобщенной биометрической системы, например, контроль качества может проводиться перед сегментацией или выделением признаков.

4.2 Принципиальные компоненты обобщенной биометрической системы

4.2.1 Подсистема захвата данных

Подсистема захвата данных предназначена для получения изображения или сигнала биометрических характеристик субъекта, предоставившего их биометрическому датчику, и преобразования их в биометрический образец (также называемый «блоком биометрических данных» (ББД) см. 6.1).

Работа биометрических систем начинается со сбора сигналов поведенческих/биологических характеристик. Так как данные биологических датчиков могут быть одномерными (речь), двухмерными (отпечаток пальца) или многомерными (динамика письма), то мы не всегда имеем дело с «изображениями». Для упрощения терминологии назовем необработанные сигналы «образцами».

Основным допущением для всех систем считается то, что наблюдаемый сигнал биометрической характеристики является одновременно и отличительной особенностью между субъектами и повторяется со временем в случае одного и того же субъекта. Таким образом, желательно, чтобы было как можно больше различий между разными субъектами и как можно меньше различий в случае одного субъекта. Трудности измерения и контроля различий начинаются в подсистеме сбора данных.

Характеристика субъекта должна быть изучена датчиком, например, микрофоном, устройством сканирования отпечатков пальцев, цифровой камерой или клавиатурой компьютера. В системах, верифицирующих только положительные запросы на идентификацию, субъект может предоставить датчику биометрические характеристики. Процесс предоставления биометрической характеристики датчику включает в себя поведенческую составляющую в рамках любого метода, т. к. субъект должен так или иначе взаимодействовать с датчиком в процессе сбора данных. Выходные данные датчика являются комбинацией:

1) биометрической характеристики;

2) способа предоставления биометрической характеристики;

3) технических характеристик датчика.

Все характеристики и результаты, произведенные системой, основаны на этих выходных данных датчика. Изменения любого из представленных трех факторов влекут за собой негативное влияние как на повторяемость, так и на отличительные особенности характеристик. В случае, если предполагается обмен данными между системами, процесс предоставления характеристик и технические характеристики датчика должны быть стандартизированы для того, чтобы биометрические характеристики, собранные при помощи одной системы, были совместимы с биометрическими характеристиками того же субъекта, собранными другой системой.

4.2.2 Подсистема передачи данных

Примечание — Подсистема передачи на рисунке 1 не представлена.

Подсистема передачи, которая не всегда (или неявно) входит в состав биометрической системы, осуществляет передачу образцов, признаков и (или) шаблонов между различными подсистемами. Образцы, признаки и (или) шаблоны могут передаваться с использованием стандартного формата обмена записями биометрической информации (ЗБИ) и блока биометрических данных (ББД) — ББД с метаданными (см. 6.1). Биометрический образец может быть сжат и (или) закодирован перед передачей и распакован и (или) раскодирован перед использованием. Биометрический образец может быть изменен во время передачи из-за наличия помех в канале передачи, а также искажен в процессе сжатия или распаковки. Для защиты подлинности, целостности и конфиденциальности хранимых и передаваемых биометрических данных следует использовать методы кодирования.

Некоторые биометрические системы собирают данные в одном месте, а обрабатывают в другом (см. 6.3). Если проводится сбор большого количества данных, то может потребоваться их сжатие для экономного использования канала передачи. В системах, где необходимо хранение биометрических образцов, биометрические образцы чаще всего сохраняются в сжатом виде. Процессы сжатия и передачи, производимые системой до обработки сигнала и сохранения образца, показаны на рисунке 1. В архитектуре БиоАПИ/ПМВ (протокол межсетевого взаимодействия) (см. 6.3, 6.4) ЗБИ перед передачей отдаленного приложения посредством ПМВ БиоАПИ подвергнется локальной обработке. Переданные или сохраненные в сжатом виде данные могут быть распакованы перед дальнейшим использованием или получены посредством выделения признаков. На сегодняшний день стандартов для общего сжатия данных не существует, только выделение признаков как следствие обработки ББД в целях создания другого типа ББД. Процесс общего сжатия и распаковки приводит к потере качества сохраненного сигнала, и чем выше уровень сжатия, тем эти потери значительнее. На данный момент идет поиск таких методов сжатия для выбранной

биометрической технологии, которые способны нанести минимальный ущерб при дальнейшей обработке сигнала. Следует заметить, что в случае со сжатием данных по отпечаткам пальцев уже найдены методы ограниченного сжатия, что улучшает работу программного обеспечения в процессе распознавания паттернов (см. таблицу 6 в [50]), так как основная потеря данных первоначального сигнала происходит в наименее повторяемых высокочастотных составляющих.

4.2.3 Подсистема обработки данных

Подсистема обработки данных предназначена для выделения характерных признаков из биометрических образцов. Данная подсистема обеспечивает обнаружение характерных признаков субъекта в полученном образце (процесс называется «сегментацией»), выделение признаков и контроль качества для обеспечения различимости и воспроизводимости выделяемых признаков. Если подсистема контроля качества отклоняет полученный образец или образцы, то в подсистему захвата данных поступает управляющая команда для сбора дополнительных образцов.

В случае регистрации некоторые системы, например, используемые при работе с биометрическими паспортами, могут просто хранить полученный образец в качестве шаблона, характеризующего субъект. В других системах, анализирующих некоторые идентификационные карты, подсистема обработки данных создает шаблон из выделенных биометрических признаков, которые используются как эталон. Часто процесс регистрации требует наличия признаков нескольких представлений биометрических характеристик субъекта для создания шаблона, который может быть использован в качестве эталона. Тем не менее другие системы, такие как системы распознавания личности по голосу и лицу, могут создавать из выделенных признаков более сложные математически абстрактные «шаблоны». Независимо от того, что собой представляет эталон, — образцы, шаблоны или абстрактные шаблоны, он является основной характеристикой субъекта для всех последующих процессов распознавания.

Подсистема обработки биометрического сигнала состоит из четырех модулей: сегментация, выделение признаков, контроль качества и (только при регистрации) создание шаблона. Все эти модули прописаны в концепции «обработки ПБУ» (поставщик биометрической услуги) в БиоАПИ. Модуль сегментации должен определить, существует ли биометрический сигнал в потоке полученных данных (определение сигнала) от устройства, и если существует, то выделить его из окружающего шума. Если модуль сегментации провел определение или выделение биометрического сигнала с ошибкой, то в этом случае говорят, что произошел «отказ сбора данных». В архитектуре БиоАПИ данное событие (посредством структуры БиоАПИ) сообщается контрольному приложению.

Модуль выделения признаков (того или иного поставщика биометрической услуги (ПБУ) в определениях БиоАПИ) (см. 6.3) должен обработать сигнал таким образом, чтобы сохранить или усилить различия между разными субъектами (отличительные особенности), минимизируя различия в случае одного субъекта (неповторяемость). Выходными данными модуля является набор цифр, которые также называются «признаками», но, несмотря на это, может не иметь непосредственного поведенческого или биологического значения. Например, цифровые значения, выработанные системой, не определяют ширину губ, длину носа или расстояние между глазами и ртом, они представляют лицо в более абстрактном, математическом виде. Форматы базовых блоков данных (ББД) (см. 6.1), в которых записываются результаты выделения признаков, являются важной частью стандартизации в ИСО/МЭК СТК 1/ПК 37.

Модуль контроля качества анализирует выделенные признаки, чтобы удостовериться в том, что они достаточного качества и присутствуют в достаточном количестве для эффективной обработки. Если проверка на качество оказывается неудачной, то система предупреждает субъекта о том, что необходимо повторить операцию захвата образца (ов). В случае, если биометрическая система так и не смогла создать приемлемый набор признаков, происходит «отказ регистрации» или «отказ сбора данных», о которых система докладывает контрольному приложению посредством структуры БиоАПИ. «Отказ регистрации / сбора данных» происходит из-за ошибки в алгоритме сегментации, вследствие которой набор признаков не создается. Модуль контроля качества может даже повлиять на процесс принятия решения, указывая подсистеме принятия решений на то, чтобы система, например, повысила требования к сопоставлению низкокачественного входного образца.

Модуль создания шаблонов (только во время регистрации, см. рисунок 1) создает такой биометрический образец (также называемый «контрольным шаблоном», «абстрактным шаблоном» или просто «контрольным образцом»), который является ББД в определенном (обычно стандартизированном) формате, приемлемом для хранения и дальнейшего использования в подсистеме сопоставления. Биометрический образец является однозначным указателем или «ссылкой» на субъект, который был зарегистрирован.

4.2.4 Подсистема хранения данных

Шаблоны, хранимые в базе данных зарегистрированных пользователей, содержатся в подсистеме хранения данных. Каждый шаблон связан с информацией о зарегистрированном субъекте. Шаблоны перед сохранением в базе данных зарегистрированных пользователей могут быть преобразованы в соответствии с форматом обмена биометрическими данными (ЗБИ, состоящая из ББД с метаданными). Шаблоны могут быть сохранены в устройстве захвата биометрических данных на портативном носителе, таком как смарт-карта, или локально, т. е. на персональном компьютере в локальной сети или в центральной базе данных.

В терминологии БиоАПИ (см. 6.3) — это ПБУ архив. Обработанные признаки или созданный абстрактный шаблон признаков каждого субъекта сохраняется или «регистрируется» в базе данных для дальнейшего сравнения с входящими образцами признаков посредством сопоставителя паттернов (ПБУ сопоставления). Для верификации отрицательных запросов на идентификацию требуется централизованная база данных всех зарегистрированных шаблонов [или некий эквивалент, присоединенные децентрализованные базы данных, возможно, при помощи БПМВ БиоАПИ (см. 6.4) для входа в них], чтобы можно было бы верифицировать запрос и убедиться, что данный субъект в системе не зарегистрирован. Подобные системы в основном возвращают записи о любых найденных прежних регистрациях, поэтому называются «идентификационными». Крупные идентификационные системы могут разделить базу данных на группы по признакам пола или возраста, и таким образом потребуется проверять не все централизованно сохраненные шаблоны для определения того, что данный субъект не находится в базе данных. Подобные системы иногда условно называют «один-ко-многим», указывая на то, что представленный образец должен быть сопоставлен со множеством зарегистрированных (контрольных) или абстрактных шаблонов.

В системах, верифицирующих только положительные запросы на идентификацию, база данных шаблонов может быть сохранена на читаемой оптическим способом магнитной ленте или на смарт-картах, которые имеются у каждого зарегистрированного субъекта. Несмотря на то, что в таком случае централизованная база данных не требуется, ее отсутствие приводит к невозможности проверить множество регистраций и затрудняет восстановление потерянных или поврежденных карт. Системы, верифицирующие только положительные запросы, часто условно называют «один-к-одному», указывая на то, что представленный образец должен быть сопоставлен с контрольными шаблонами или абстрактными шаблонами единственного запроса на идентификацию. Однако системы верификации, основанные на технике оценки вероятности, сопоставляют образцы не только с запрошенными зарегистрированными (контрольными) шаблонами, но и с шаблонами других субъектов или с «предшествующими абстрактными моделями», поэтому эти системы на самом деле могут не быть системами «один-к-одному».

Несмотря на то, что размещение или хранение на картах возможно, системы верификации положительных запросов по-прежнему могут использовать централизованную зашифрованную базу данных для предотвращения создания поддельных карт или восстановление потерянных карт без повторного сбора биометрических характеристик.

В основном исходные биометрические характеристики, такие как, например, отпечатки пальцев, не могут быть восстановлены из сохраненных контрольных шаблонов. Тем не менее, если доступ к незакодированным шаблонам осложнен, то для опытного взломщика при наличии системы идентификации вполне возможно создать искусственный муляж, способный воссоздать исходный шаблон. Несмотря на то, что искусственный муляж не будет иметь внешний вид, аналогичный исходному биометрическому образцу, биометрическая система создаст тот же шаблон. С биометрическими шаблонами по этой причине обращаются как с важной информацией, а также ограничивают к ним доступ, (особенно в процессе передачи) используют кодирование для обеспечения их целостности и аутентичности. Решение об эксплуатации централизованной базы данных шаблонов в приложениях по верификации должно приниматься с учетом рисков нарушения системы безопасности и конфиденциальности, возможности быть взломанной, как и для любых других проблем сохранения секретности.

Биометрические шаблоны зачастую создаются при помощи специализированных, собственных алгоритмов выделения признаков поставщика системы, несмотря на то, что стандартные ББД форматы, записывающие признаки, предоставляют обстоятельное руководство для выделения признаков при работе с этими форматами. Некоторые типичные примеры размеров незакодированных шаблонов для разных биометрических технологий приведены в таблице 1.

Таблица 1 — Размеры типичных биометрических шаблонов

Устройство	Размер, байт
Биометрический сканер отпечатка пальца	200—2000
Биометрический сканер голоса (микрофон)	2000 и выше (текстозависимый) 4000—50000 (текстонезависимый)
Биометрический сканер геометрии контура пальца	14
Биометрический сканер геометрии контура кисти руки	9
Биометрический сканер лица	100—3500
Биометрический сканер РОГ	512
Биометрический сканер сосудов	256—1000

4.2.5 Подсистема сравнения

В подсистеме сравнения происходит сравнение признаков субъекта с признаками одного или более шаблонов и передача значений степеней схожести в подсистему принятия решения. Степени схожести показывают степень соответствия между сравниваемыми шаблонами. В некоторых случаях признаки представляются в виде шаблонов, хранимых в базе данных. При верификации имеется единственный запрос регистрации субъекта, поэтому подсистема сравнения возвращает единственное значение степени схожести. При идентификации происходит сравнение признаков субъекта с признаками нескольких или всех шаблонов, и возвращается значение степени схожести для каждого сравнения или список «кандидатов» на соответствие из базы данных.

Модуль сопоставления паттернов сравнивает данные образца признака с предварительно зарегистрированными данными признака («контрольными шаблонами») в базе данных и создает цифровой «результат сопоставления». Если и шаблон, и признак представляют собой вектор, то сопоставление может быть таким же простым, как вычисление Евклидова расстояния. Вместе с тем, могут быть применены и нейронные сети или статистические измерения, например, отношения правдоподобия. На данный момент алгоритмы сопоставления не стандартизированы в ИСО/МЭК СТК 1/ПК 37, так как многие алгоритмы являются «конфиденциальной информацией компании» или субъектов права интеллектуальной собственности или патентного права, но концепция «ПБУ сравнения» полноценно отражена. Независимо от используемой техники сопоставления паттернов шаблоны и признаки, выделенные из образцов, не будут полностью совпадать из-за повторяющихся моментов, которые были описаны выше (см. 4.2.1). В конечном итоге, результаты сопоставления, определенные модулем сопоставления паттернов, должны быть расшифрованы подсистемой принятия решения.

В таких системах, как верификация личности по голосу, «шаблоны» регистрации могут быть «абстрактными шаблонами» процесса генерации признаков — совершенно другие структуры данных, нежели наблюдаемые признаки. Модуль сопоставления паттернов определяет совместимость наблюдаемых признаков с сохраненным абстрактным шаблоном. Некоторые модули сопоставления паттернов могут даже распорядиться о проведении адаптивного повторного вычисления признаков, выделенных из входящих данных, чтобы узнать, можно ли найти более хорошие совпадения посредством незначительных корректировок во входящих данных. Этот процесс может быть проведен в абстрактном шаблоне БиоАПИ при соответствующем применении ПБУ.

4.2.6 Подсистема принятия решения

Подсистема принятия решения использует значения степеней схожести, полученные после одной или нескольких попыток, для предоставления результата транзакции верификации или идентификации.

При проведении верификации считают, что оцениваемая характеристика схожа со сравниваемым шаблоном, если степень схожести превышает установленный порог принятия решений. Запрос о регистрации субъекта может быть выполнен в соответствии с политикой принятия решения, которая может регламентировать несколько попыток.

При проведении идентификации считают, что поступающий идентификатор является потенциальным кандидатом для субъекта в том случае, если степень схожести превышает установленный порог принятия решений и (или) если значение степени схожести находится среди первых значений, число которых равно установленному значению *k*. Политика принятия решения может разрешить или потребовать сделать несколько попыток, прежде чем выдать результат идентификации.

Примечание — Мультимодальные биометрические системы (см. А.11.1.13 приложения А) могут использоваться аналогично унимодальным биометрическим системам путем обработки общих биометрических образцов, шаблонов или степеней схожести, как если бы они были отдельными образцами, шаблонами или степенью схожести и позволяли подсистеме принятия решений проводить операцию объединения степеней схожести и решений (если уместно).

Подсистема принятия решения рассматривается отдельно от модуля сопоставления паттернов и может быть в определениях архитектуры БиоАПИ отдельным ПБУ обработки (возможно, предоставленным другим поставщиком). Подсистема принятия решения должна вынести решение «совпадает» или «не совпадает», сопоставляя выходной результат модуля сопоставления паттернов с определенным заранее пороговым значением. Окончательное решение по запросу идентификации личности «принятие» или «отклонение» может быть основано на множестве решений «совпадение/несовпадение», исходящих из множества измерений, или по критериям принятия решения, определенным динамически, зависящим от пользователя или измерения. Например, при обычных алгоритмах принятия решения транзакция примется, если из трех попыток произойдет совпадение или при совпадении с одним шаблоном из нескольких.

Модуль принятия решения также может направлять процессы к сохраненной базе данных, сохраняя признаки во время регистрации в качестве шаблонов, обновляя шаблоны базы данных после успешной передачи, привлекая дополнительные шаблоны для сравнения в модуле сопоставления паттернов или управляя поиском по базе данных.

Вследствие того, что входные образцы и сохраненные шаблоны полностью не совпадают, модули принятия решений совершают ошибки — ошибочно отвергая верный запрос идентификации зарегистрированного субъекта или ошибочно принимая запрос идентификации «самозванца». Таким образом, существует два вида ошибок: ложное несовпадение и ложное совпадение. Количество данных ошибок может быть изменено за счет друг друга, но в ограниченном масштабе: уменьшение количества ложных несовпадений приводит к увеличению ложных совпадений и наоборот. На практике свойственные каждому субъекту различия (неповторяемость) ограничивают масштаб, до которого ложные несовпадения могут быть снижены, за исключением ситуации принятия всех сопоставлений. Алгоритмы принятия решений «совпадает/не совпадает» характерны для эксплуатационных требований системы и требований системы к безопасности и показывают окончательную значимость и вероятность ошибок обоих типов.

Вследствие неизбежности ошибок (как ложные несовпадения, так и ложные совпадения) все системы должны быть снабжены механизмами «исключительной обработки особой ситуации». Если механизмы исключительной обработки особой ситуации не так мощны, как базовая система биометрической безопасности, то результатом этого может стать уязвимость системы. Большое число ложно отвергнутых сравнений может вызвать перегрузку даже мощных механизмов исключительной обработки особой ситуации и понижение уровня ответной реакции системного администрирования на потенциальные атаки. Соответственно высокий уровень ложных несовпадений может не только вызвать неудобства пользователя и привести к задержке в работе системы, но и подвергнуть риску систему безопасности. Ложные совпадения и ложные несовпадения тесно связаны с системными понятиями «ложного допуска» и «ложного недопуска».

Для различных систем требуются крайне разные соотношения между уровнями вероятности ошибок. Например, биометрический портал может быть эффективен даже при 20% вероятности ложного совпадения (80% вероятность перехвата самозванца), которая может оказаться достаточно низкой для снижения частоты атак на биометрическую систему до такого уровня, когда успешное проникновение «самозванца» невозможно. Мошенники могут найти другие входные точки, включая исключение механизма обработки, более привлекательные, чем биометрический портал. С другой стороны, в системах идентификации преступников ложное совпадение может повлечь за собой ошибочный арест или тюремное заключение; именно поэтому необходимо максимально снизить вероятность ложного совпадения.

4.2.7 Подсистема управления

Примечание — Подсистема управления на рисунке 1 не представлена.

Подсистема управления регулирует общую политику, внедрение и эксплуатацию биометрической системы в соответствии с правовыми, юридическими и социальными требованиями и ограничениями, такими как:

- обеспечение обратной связи с субъектом во время и (или) после захвата данных;

- запрос дополнительной информации от субъекта;
- хранение и форматирование биометрических шаблонов и (или) биометрических данных;
- обеспечение окончательной экспертизы результата на основании принятых решений и (или) оценок;
- установка пороговых значений;
- установка настроек биометрической системы;
- проверка условий эксплуатации и хранение небиометрических данных;
- обеспечение необходимых мер безопасности для конфиденциальности конечного пользователя;
- взаимодействие с приложением, которое использует биометрическая система.

4.2.8 Интерфейс

Биометрическая система может взаимодействовать с внешним приложением через прикладной программный интерфейс (см. 6.3), интерфейс аппаратного обеспечения или интерфейс протокола (см. 6.4).

4.3 Функции обобщенной биометрической системы

4.3.1 Регистрация

При регистрации транзакция субъекта обрабатывается системой для создания и сохранения регистрационного шаблона данного субъекта. Регистрационный шаблон состоит из биометрического шаблона (сохраненного образца, шаблона или абстрактного шаблона) субъекта или, возможно, иной информации, такой как, например, имя. Во время регистрации достоверность иной информации должна быть уточнена из внешних источников, таких как свидетельство о рождении, паспорта или иных достоверных надежных документов. Применение биометрии не исключает необходимости уточнять достоверность данных документов во время регистрации. Следует заметить, что регистрация в некоторых идентификационных системах может не быть отдельной стадией; в том случае, если субъект не найден в базе данных, происходит его регистрация.

Регистрация состоит из следующих этапов:

- получение образца;
- сегментация и выделение признаков;
- проверка качества (в результате которой образец или признаки, непригодные для создания шаблона, могут быть отклонены, и будет сформирован запрос на получение дополнительных образцов);
- создание шаблона (может потребовать признаки нескольких образцов) с возможным преобразованием его в формат обмена биометрическими данными и хранения;
- попытки верификации или идентификации, чтобы гарантировать пригодность регистрации;
- попытки повторной регистрации, которые могут быть предоставлены, если первоначальная регистрация оказалась неудовлетворительной (зависит от политики регистрации).

4.3.2 Распознавание

4.3.2.1 Верификация

При верификации транзакция субъекта обрабатывается системой для проверки конкретного запроса о регистрации субъекта (например, «Я зарегистрирован как субъект X»). Верификация примет или отклонит запрос. Результат верификации считается ложным, если принимается ошибочный запрос (ложный допуск) или отклоняется правильный запрос (ложный недопуск). Необходимо отметить, что некоторые биометрические системы позволяют одному конечному пользователю регистрировать более одного экземпляра биометрических характеристик (например, система регистрации РОГ может позволить конечному пользователю зарегистрировать изображения РОГ двух глаз, а система регистрации отпечатков пальцев может зарегистрировать два или более пальцев конечного пользователя в качестве резервных на случай, если один из пальцев будет поврежден).

Процесс верификации состоит из следующих этапов:

- получение образца;
- сегментация и выделение признаков;
- проверка качества (в результате которой образец или признаки, непригодные для создания шаблона, могут быть отклонены, и будет сформирован запрос на получение дополнительных образцов);
- сравнение признаков образца с признаками, извлеченными из шаблона, для определения степени схожести;
- формирование решения о соответствии признаков образца признакам, извлеченным из шаблона, которое принимают, если степень схожести образца превышает порог принятия решений;

- возвращение результата верификации одной или более попыток в соответствии с политикой принятия решений.

Пример — В системе верификации, позволяющей сделать не более трех попыток сравнения с зарегистрированным шаблоном, ложный недопуск возникает при любой комбинации с отказом сбора данных и ложного несоответствия по результатам трех попыток. Ложный допуск возникает в том случае, если образец получен и ложно совпал с зарегистрированным шаблоном для запрошенной идентичности по результатам трех попыток.

4.3.2.2 Идентификация

При идентификации транзакция субъекта обрабатывается системой для нахождения идентификатора зарегистрированного субъекта. Результат идентификации предоставляет собой список кандидатов, который может быть пустым или содержать один и более идентификаторов. Идентификация считается правильной в том случае, если субъект зарегистрирован и его идентификатор находится в списке кандидатов. Идентификация считается ошибочной, если зарегистрированный идентификатор субъекта отсутствует в списке кандидатов (ложноотрицательная идентификация) или транзакция незарегистрированного пользователя выдает список кандидатов (ложноположительная идентификация). Существует два вида подходов к созданию списка кандидатов: идентификация на замкнутом множестве и идентификационная на открытом множестве (см. 7.1).

Процесс идентификации состоит из следующих этапов:

- получение образца;
- сегментация и выделение признаков;
- проверка качества (которая может отклонить образец или признаки, непригодные для сравнения, и потребовать получения дополнительных образцов);
- сравнение с некоторыми или со всеми шаблонами базы данных, определяющее степень схожести для каждого сравнения;
- формирование решения об идентичности шаблонов, которое принимается, если степень схожести превышает порог принятия решений и (или) находится среди первых значений k степеней схожести;
- возвращение результата идентификации, верификации одной или более попыток в соответствии с политикой принятия решений.

5 Основные концепции

С 1970 г. были определены три основных принципа автоматического распознавания личности [19]. Это распознавание:

- по чему-то известному или сохраненному в запоминающем устройстве;
- по чему-то, что есть у субъекта с собой;
- по личной физической (биометрической) характеристике.

Теперь мы можем с уверенностью сказать, что субъект может быть автоматически распознан по тому, что он (она) «знает, имеет или чем является», посредством ПИН-кодов и паролей, токену или биометрическим характеристикам. Последним и наиболее безопасным из трех принципов является биометрическая технология, которая может быть применена как отдельно, так и в совокупности с другими формами идентификации (ПИН-коды, пароли или физические токены) в системе контроля доступа в целом. Приложения контроля физического доступа, применяющие биометрию, используются в аэропортах, парках отдыха, банкоматах обслуживания частных клиентов, точках въезда в страну, университетах, офисных зданиях и объектах государственной безопасности. Подобные технологии используются в информационных системах, поэтому биометрия становится важнейшим элементом информационной безопасности, т. к. биометрическая информация не может быть забыта или потеряна. Идеальная биометрическая характеристика для любых областей применения должна быть:

- характерной — различной у всех субъектов;

- повторяющейся — неизменной во времени у каждого субъекта в течение длительного периода времени (несколько лет);

- доступной — легко доступной для устройства съема (например, биометрические сканеры лица (камеры), биометрические сканеры отпечатков пальцев или биометрические сканеры геометрии контура пальца);

- приемлемой — субъект может воспользоваться биометрической характеристикой в установленном применении;

- универсальной — наблюдаемой и имеющейся у всех субъектов.

К сожалению, ни одна биометрическая характеристика не обладает всеми вышеуказанными свойствами, например, между разными субъектами существует много сходств; биометрические характеристики изменяются со временем; некоторые физические ограничения субъекта препятствуют доступу к биометрической характеристике; некоторые субъекты возражают против сдачи биометрических характеристик; не все субъекты обладают всеми характеристиками. При практическом применении биометрических технологий все указанное выше должно учитываться. Как следствие, важной задачей при внедрении биометрических технологий является разработка устойчивой к сбоям системы для работы с неожиданно изменяющимися условиями и вариациями в теле субъекта.

Биометрические системы верифицируют запросы (проверяют гипотезы), учитывая источник биометрического паттерна в базе данных. Запрос в системе может быть произведен субъектом, предоставляющим биометрический образец (например, «Я являюсь источником записи биометрических данных в базе данных»), или другим действующим субъектом (например, «Она является источником записи биометрических данных в базе данных»). Запросы могут быть положительными (например, «Я являюсь источником записи биометрических данных в базе данных») или отрицательными (например, «Я не являюсь источником записи биометрических данных в базе данных»). Запросы могут быть уточняющими (например, «Я являюсь источником записи биометрических данных А в базе данных») или общими (например, «Я не являюсь источником никакой записи биометрических данных в базе данных»). Запрос может быть уточняющим и общим, положительным и отрицательным, от первого и третьего лица. Для введения терминологии национальных стандартов можно найти «соответствие» между биометрическими характеристиками субъекта и идентифицированного биометрического шаблона, сохраненного в базе данных (верификация), или можно найти совокупность биометрических шаблонов в базе данных для сопоставления с предоставленными биометрическими образцами субъекта (идентификация). В обоих случаях необходимо установить пороги того, насколько велика должна быть схожесть, чтобы можно было полагать, что предоставленный биометрический образец и биометрический шаблон принадлежат одному и тому же субъекту. Естественно, может произойти ошибка: «ложное несовпадение», несмотря на то, что паттерны действительно принадлежат одному и тому же субъекту, либо «ложное совпадение», несмотря на то, что паттерны действительно принадлежат двум разным субъектам. Речь идет о проценте подобных ошибок в общем числе сопоставлений – «вероятности ложного совпадения» (ВЛС) и «вероятности ложного несовпадения» (ВЛНС) для конкретной технологии и в условиях конкретного приложения.

Системы, требующие положительного запроса на конкретный зарегистрированный шаблон, воспринимают биометрический паттерн как элемент записи регистрации. Подобные системы, «верифицирующие» то, что биометрический элемент в запрошенной регистрации сопоставляется с представленным субъектом образцом, называются системами «верификации». Некоторые системы, которые применяются в системе социального обслуживания населения или при выдаче водительских прав, верифицируют отрицательные запросы еще не существующего биометрического паттерна в базе данных, воспринимая биометрический паттерн в качестве уникального индекса или указателя. Данные системы, ищущие в базе данных биометрических указателей один единственный указатель, который совпадает с представленным образцом, называются системами «идентификации». Впрочем, процесс поиска индекса (или указателя) в списке индексов также верифицируется общим запросом регистрации в базе данных, а если указатель не найден, то верифицируется отрицательный запрос регистрации. Различия между системами «идентификации» и «верификации» могут быть не всегда четкими, а данные определения — не взаимоисключающими.

В простейших системах «верификации» положительного запроса определенной записи регистрации может понадобиться сопоставление представленных образцов только с теми биометрическими элементами, которые находятся в единственной запрашиваемой записи. Например, субъект может утверждать, что является источником сохраненной записи об отпечатке пальца на иммиграционной карте. Для того чтобы подтвердить запрос о том, что субъект является источником записи об отпечатке пальца, он помещает карту в устройство считывания, которое считывает информацию, затем помещает свой палец на устройство считывания отпечатка пальца. Система сопоставляет записанный шаблон отпечатка пальца на карте с тем, что предоставлен субъектом. Если два паттерна достаточно схожи, то устройство выносит решение о том, что субъект действительно является источником записи на карте и поэтому должен получить права и привилегии, которые ему предоставляются картой (естественно, при условии, что карта не поддельная. Основная цель биометрической верификации состоит в определении того, что субъект, предоставивший биомет-

рические характеристики, действительно является субъектом, являющимся источником биометрических характеристик, записанных на карте).

«Простая идентификация» может потребовать сравнения представленного биометрического образца со всеми биометрическими идентификаторами, хранящимися в базе данных. Заявителям на пособия по социальному обеспечению в штате Калифорния необходимо верифицировать отрицательный запрос о том, что они не были ранее занесены в систему путем предоставления отпечатков пальцев обоих указательных пальцев. В зависимости от особенностей принципа автоматического поиска данные отпечатки пальцев сопоставляются с отпечатками пальцев всех подателей заявления на пособие по социальному обеспечению в этой базе данных с тем, чтобы убедиться в том, что аналогичных отпечатков пальцев еще в системе нет. Поиск может проходить только в той части базы данных, где собраны отпечатки пальцев людей, чей пол соответствует полу подателя заявления. Если соответствующие отпечатки пальцев найдены, то запись о регистрации, созданная по предоставленным отпечаткам пальцев, возвращается системному администратору для подтверждения отказа по запросу подателя о том, что регистрации ранее не было.

Выше были представлены примеры простейших систем. Более сложные системы могут применять сопоставления со множеством записей регистрации для верификации предъявляемой идентификационной информации или осуществлять крайне ограниченное число сопоставлений для идентификации из числа всех зарегистрированных записей. Достоверной связи между «верификацией» или «идентификацией» и числом сопоставлений, которые система должна провести, не существует.

В основном биометрия в системах информационной безопасности применяется для верификации положительных запросов о том, что предъявитель является источником конкретной или неконкретной записи регистрации в базе данных. Такие системы обычно называются системами «верификации» независимо от принципа поиска и применяемой архитектуры. Если запрос регистрации верифицирован, то права, соответствующие верифицированной или идентифицированной записи регистрации на затребованные действия, такие как, например, вход в систему, могут быть с уверенностью переданы. Несмотря на то, что гибридные системы, верифицирующие в процессе регистрации отрицательное утверждение (запрос) о том, что субъекта еще нет в базе данных, затем верифицируют положительные запросы о регистрации, также существуют, но в настоящее время менее распространены.

Биометрические технологии играют все большую роль в системах информационной безопасности для передачи пользователям системных полномочий посредством верификации предъявляемой идентификационной информации. Аргументом в пользу биометрических характеристик можно считать то, что они теснее связывают процесс авторизации с субъектом, чем «что у вас есть» и «что вы знаете».

Биометрические характеристики сложнее переместить, забыть или украсть, чем ПИН-коды, пароли и токены, поэтому они повышают уровень безопасности систем, в которых применяются. Для повышения уровня безопасности биометрия может быть совмещена с ПИН-кодами и токенами в «многофакторные» системы. В случае, если ПИН-код, пароль или токен украдут или разгласят, или будут разглашены биометрические характеристики, ПИН-код, пароль или токен могут быть заблокированы.

6 Стандарты на биометрические технические интерфейсы

6.1 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). Блок биометрических данных представляет собой формат обмена стандартизированными данными для записи особых биометрических характеристик, таких 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. приложение А, А.3, ИСО/МЭК 19794), каждый из которых определяет один или более форматов ББД (например, форматы компактных смарт-карт наравне с обычными форматами). У каждой технологии есть один (или более) родственный идентификатор формата ББД, позволяющий любой системе расшифровывать или обрабатывать родственный формат, о котором у системы есть информация.

Вторая концепция основана на «записи биометрической информации» (ЗБИ). ЗБИ — это ББД, но с дополнительными метаданными: дата захвата, дата истечения срока хранения захваченных данных, данные об устройстве регистрации, информация о том, закодированы данные или нет. Некоторые форматы ЗБИ установлены в ИСО/МЭК 19785-3 (см. А.11.2.3 приложения А) как части продолжающейся работы в данной

области на базе как количества информации, включенной в ЗБИ, так и компактности используемой схемы кодирования. К тому же у форматов ЗБИ есть идентификатор, который в данном случае называется «главным идентификатором формата ЕСФОБД».

ЗБИ является единицей, применяемой в большинстве национальных стандартов для хранения и обмена между модулями программного обеспечения и компьютерными системами, например, используя интерфейсы БиоАПИ (в рамках системы) или протокол межсетевого обмена (ПМО) (между системами).

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

6.2 Единая структура форматов обмена биометрическими данными (ЕСФОБД)

Настоящий стандарт (см. А.11.2.1 приложения А) предназначен для обеспечения взаимодействия программных и аппаратных средств, применяемых в области биометрии, путем установления стандартных структур записей биометрических данных (ЗБИ). ЗБИ представляют собой один или несколько ББД с дополнительными данными, формирующими заголовок ЗБИ. Заголовок состоит из набора элементов данных и их абстрактных значений, соответствующих требованиям ЕСФОБД.

ЗБИ представляет собой данные, записанные в соответствии с форматом ведущей организации ЕСФОБД (см. ниже). ЗБИ всегда состоит не менее чем из двух частей: стандартного биометрического заголовка (СБЗ) и по меньшей мере из одного (ББД). ЗБИ может содержать также и третью часть, называемую 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; стандартизованные форматы ББД для ряда биометрических технологий установлены в серии стандартов ИСО/МЭК 19794.

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 использовать дополнительные абстрактные значения, установленные форматом ведущей организации ЕСФОБД, вместе с одним или более ББД.

ИСО/МЭК 19785 состоит из трех частей. В ИСО/МЭК 19785-1 установлен полный набор элементов данных и их абстрактных значений (без определения способов записи). В ИСО/МЭК 19785-2 установлены процедуры действий регистрационного органа в области биометрии, который присваивает идентификаторы для биометрических организаций, ББД, форматов ведущей организации (форматов ЗБИ) и форматов БЗИ. ИСО/МЭК 19785-3 устанавливает конкретные спецификации форматов ведущей организации, размер заголовков которых варьируется от минимального до максимального и способ записи которых может быть бинарным или в формате XML.

6.3 Стандарт БиоАПИ

6.3.1 Биометрический программный интерфейс: спецификация биометрического программного интерфейса (ИСО/МЭК 19784-1)

БиоАПИ (см. приложение А, А.11.3.1, ИСО/МЭК 19784) является стандартом, предоставляющим спецификацию архитектуры программного интерфейса для биометрических приложений. Описываемая модель позволяет использовать компоненты биометрической системы разных изготовителей и обеспечивать их взаимодействие посредством установленных программных интерфейсов приложений.

Основная концепция заключена в приложениях (от множества поставщиков), которые взаимодействуют со структурой БиоАПИ (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 БиоАПИ показана на рисунке 2.

Взаимодействие между разными компонентами осуществляется посредством передачи ЗБИ.

ПБУ может выполнять захват (получение), сопоставление, архивацию или обработку ЗБИ.

В последнем издании, посвященном архитектуре БиоАПИ, ПБУ может состоять из кода одного поставщика, взаимодействующего с «Элементом БиоАПИ», 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, сводится к минимуму.

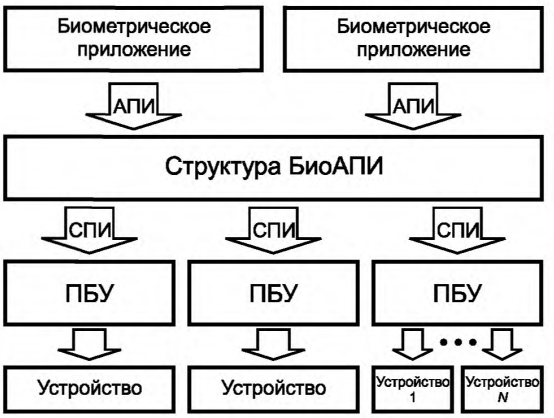

Рисунок 2 — Архитектура БиоАПИ

6.4 Стандарт протокола межсетевого обмена БиоАПИ

Стандарт протокола межсетевого обмена БиоАПИ (см. ИСО/МЭК 24708, А.11.4 приложения А) предоставляет собой линейный битовый контакт, обеспечивающий взаимодействие приложения в одной системе БиоАПИ с ПБУ удаленной системы БиоАПИ. Данное обновление в архитектуре БиоАПИ является важным элементом дополнительной стандартизации, которая формирует часть подсистемы передачи, описанной в пункте 4.2.2 (см. рисунок 3).



Рисунок 3 — Применение ПМО для контакта между системами

7 Эксплуатационные испытания

7.1 Общие сведения

Биометрические устройства и системы могут быть подвергнуты различным испытаниям. Испытания могут включать в себя оценку (см. также А.11.5 приложения А):

- эксплуатационных характеристик (в терминах вероятностей ошибок и производительности);
- надежности, доступности и удобства эксплуатации;
- степени защищенности;
- безопасности;
- приемлемости системы для пользователя;
- влияния человеческих факторов;
- коэффициента эффективности затрат;
- степени соответствия правилам конфиденциальности.

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, разрабатываются стандарты, устанавливающие процедуры проведения испытаний (серия стандартов ИСО/МЭК 19795, а также А.11.5 приложения А).

Эксплуатационные испытания могут проводиться на замкнутом множестве либо на открытом множестве. Испытание на замкнутом множестве предполагает, что все субъекты зарегистрированы в системе, и не допускает существования «самозванцев». В процессе испытания на замкнутом множестве возвращается ранг истинного совпадения, когда входной образец сравнивается со всеми зарегистрированными шаблонами. В процессе испытания на замкнутом множестве вычисляют вероятность того, что истинный шаблон был найден во время поиска по базе данных размера N с рангом k или лучше. 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 образцы имели соответствующий зарегистрированный в базе данных шаблон. В процессе испытаний на открытом множестве определяют вероятность отсутствия истинного совпадения (вероятность ложного несовпадения) либо вероятность ложного совпадения несоответствующих шаблонов (вероятность ложного совпадения). Результаты испытаний на открытом множестве не зависят от размера базы данных, в которой происходил поиск, и сходятся к верной статистической оценке по мере увеличения объема испытания. 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, определяют в процессе проведения испытаний на открытом множестве следующие характеристики: вероятность отказа регистрации, вероятность отказа сбора данных, вероятность ложного допуска, вероятность ложного недопуска, пропускная способность. Вероятность отказа регистрации определяют как долю субъектов, которые представили системе для регистрации свои биометрические характеристики, но не смогли зарегистрироваться вследствие человеческой ошибки или ошибки системы. Вероятность отказа сбора данных определяют как долю представлений всех зарегистрированных субъектов, которые не были приняты системой. Вероятность ложного недопуска определяют как долю подлинных субъектов, чей запрос на идентичность был отвергнут системой (противоположным показателем является вероятность истинного допуска). Данный показатель включает в себя отказы регистрации и сбора данных, а также ложные несовпадения при сопоставлении с сохраненными шаблонами субъектов. Вероятность ложного допуска — это вероятность, с которой «самозванцы», совершая пассивные попытки и не пытаясь имитировать чужие биометрические характеристики, ошибочно отождествляются с некоторым случайным шаблоном. Поскольку вероятности ложного допуска/недопуска и вероятности ложного совпадения/несовпадения представляют собой противоположные показатели, они могут быть изображены одновременно на кривой компромиссного определения ошибки (КОО). Вероятности ложного допуска и истинного допуска могут быть изображены на кривой рабочей характеристики (РХ).

Пропускная способность системы представляет собой число субъектов, которое система может обработать за одну минуту, и определяется с учетом как времени взаимодействия человека и устройства, так и времени обработки данных.

7.2 Виды эксплуатационных испытаний

Ниже приведено описание трех видов эксплуатационных испытаний: технологического, сценарного и оперативного [37].

Технологическое испытание — целью технологического испытания является сравнение нескольких алгоритмов распознавания одинаковых биометрических модальностей (например, отпечатков пальцев) с использованием стандартизованной базы данных образцов, собранной с помощью устройства захвата биометрических данных, соответствующего стандартам (т. е. «универсального» датчика). Технологические испытания проводятся для систем распознавания по голосу [29], по лицу [32], по отпечаткам пальцев [4], [31], [33], [34], по РОГ [20], [35].

Сценарное испытание — целью сценарного испытания является оценка эксплуатационных характеристик всей биометрической системы, осуществляемая при использовании реальных взаимодействующих с системой субъектов и в условиях, моделирующих реальное применение системы. Каждая испытуемая биометрическая система имеет свой собственный датчик для сбора данных, в результате чего могут быть небольшие различия в получаемых исходных данных. Сценарные испытания проводились на больших выборках, но в открытых источниках публикуется только малая часть результатов сценарных испытаний [7], [25], [41].

Оперативное испытание — целью оперативного испытания 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 параметры). Поскольку вероятности ошибок в значительной степени зависят от используемой операционной системы, в открытых источниках публикуется только малая часть результатов оперативных испытаний [51].

Все биометрические технологии распознавания предусматривают взаимодействие субъекта с устройством захвата данных. В общем случае технологическое испытание направлено на снижение влияния взаимодействия системы с субъектом, в то время как при сценарном и оперативном испытаниях это оказываемое влияние должно учитываться и оцениваться. Вероятности ошибок сравнения, отказа регистрации и сбора данных и показатели пропускной способности определяются взаимодействием системы с субъектом, что, в свою очередь, зависит от особенностей условий сбора данных. Дисциплина, изучающая человеческие факторы при сборе биометрических данных, находится на стадии становления.

8 Биометрия и информационная безопасность

На данный момент ясно, что биометрия может играть крайне важную роль в информационной безопасности, потому что намного теснее связана с субъектом, подобные данные сложнее забыть, раскрыть или потерять, чем токены, ПИН-код или пароль. Применение биометрии может служить дополнительным свидетельством того, что авторизационные данные представлены именно тем субъектом, которому они были выданы. Однако биометрические технологии не становятся чем-то вроде «панацеи», избавляющей от необходимости использования ПИН-кодов, паролей и токенов при решении проблем безопасности.

При разработке системы верификации позитивных запросов идентификации необходимо решить:

- будет ли биометрический шаблон находиться у самого субъекта на токене (если это так, то в такой обработанной форме, как шаблон, или в той же форме, которая была получена первоначально, например, в форме изображения) либо шаблон будет сохранен централизованно в базе данных, соединенной с пунктом обслуживания коммуникационной системы (см. 6.4). В первом случае конфиденциальность данных несомненно подвергается опасности [21], а в случае централизованного сохранения возникают следующие вопросы:

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

- если данные из пункта обслуживания переданы в центральный пункт, то будут ли данные иметь необработанный вид или уже преобразованный в признаки. В том случае, если преобразования данных в признаки происходит перед передачей, на каждом пункте обслуживания потребуются вычислительные возможности и информация об алгоритме извлечения признаков, но пропускная способность передачи при этом снизится;

- каким образом будет происходить дешифровка зашифрованных данных в том случае, когда это необходимо для процесса сопоставления;

- 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 задачи не является непреодолимыми, они указывают на то, что биометрия не решает всех обычных проблем безопасности.

Еще с 70-х годов XX века было известно, что биометрическое устройство может быть введено мошенником в заблуждение (см. [23], [28], [40]). «Средство имитации соединения», или «Спуфинг», является способом подделки биометрических характеристик субъекта с целью их предоставления от лица субъекта и, таким образом, может быть распознанным в качестве этого субъекта. Также возможно замаскировать чьи-то собственные биометрические характеристики, чтобы избежать распознавания. Подделать биометрические характеристики какого-либо субъекта значительно сложнее, чем замаскировать собственные, но, тем не менее, вполне возможно.

Способы мошенничества в сфере биометрии лица, отпечатков пальцев и РОГ описываются во многих исследованиях (см. [5], [8], [9], [26], [45], [48]). Испытания на живучесть (испытания на возможность быть введенным мошенником в заблуждение) возможны в нескольких биометрических технологиях. Например,

в случае с системами распознавания личности по голосу мошенничество можно значительно затруднить, если при авторизации субъекту будет необходимо произнести цифры, которые в случайном порядке выбираются компьютером; в случае систем распознавания личности по РОГ проверять наличие колебаний зрачка; в случае систем распознавания личности по отпечаткам пальцев проверять кровоток. Однако испытания на живучесть находятся в процессе исследований, а эффективность подобных испытаний без увеличения вероятности ложных недопусков ставится под вопрос. Вероятность мошенничества может быть снижена посредствам применения совокупности множества биометрических характеристик или вариантов технических решений и их совокупности (например, отпечатки десяти пальцев или РОГ и лицо) наряду с работой обученных операторов.

Использование биометрии не исключает необходимости в полной проверке всех заявителей на авторизацию. Биометрическая система может не только не верифицировать истинность самой зарегистрированной идентификационной информации, но и не установить автоматически с полной достоверностью связь с внешней идентификационной информацией. Определение «истинности» идентификационной информации субъекта при необходимости происходит в процессе регистрации по достоверным внешним документам, таким как, например, свидетельство о рождении (в зависимости от национальных нормативов), идентификационная карта или водительские права. 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 идентификационной информации 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 регистрация. Если системе требуется «истинная» идентификационная информация или продолжительность идентификационной информации, то для перерегистрации требуется предоставление достоверных удостоверяющих документов. Как для регистрации, так и для перерегистрации требуется присутствие субъекта, чья регистрация проводится. В противном случае нельзя достоверно определить то, что зарегистрированная биометрическая характеристика принадлежит телу именно того субъекта, который их предоставляет.

9 Примеры областей применения

Области применения биометрических технологий крайне разнообразны. На сегодняшний день биометрические технологии широко используются правоохранительными органами, а также применяются в различных системах контроля доступа к физическим или логическим ресурсам.

9.1 Правоохранительные органы

В сообществе правоохранительных органов применяются самые масштабные биометрические системы, интегрируемые лишь с некоторыми системами иммиграционного контроля (см. 9.2.4). В данной области двумя основными функциями биометрии является идентификация подозреваемых (чаще всего по набору отпечатков пальцев) и идентификация улик (судебных доказательств) (чаще всего по скрытым отпечаткам пальцев или по ДНК, оставленному на месте преступления). Поиск отпечатков пальцев в США осуществляется по Интегральной автоматизированной системе дактилоскопической идентификации (АСДИ) ФБР, насчитывающей на данный момент отпечатки пальцев примерно 50 миллионов человек с криминальным прошлым. Полиция всего мира применяет технологию АСДИ для обработки биометрических данных лиц, подозреваемых в совершении преступления, сопоставляет отпечатки пальцев и привлекает виновных к суду.

9.2 Гражданское применение

Применение биометрии в других областях, не включающих в себя идентификацию преступников, заключается в той или иной форме контроля доступа. Основным принципом является контроль доступа к физическим или логическим ресурсам, независимо от того, система ли это защиты вознаграждений и льгот от мошенничества, предотвращение нелегального проникновения иммигрантов в страну или выхода заключенных из тюрьмы. Контроль доступа обеспечивает авторизированным субъектам получение доступа к определенной защищенной области или ресурсу, который не могут получить неавторизированные лица. Рынок гражданского применения биометрии расширяется огромными темпами. Мошенничество является

постоянно растущей проблемой, а необходимость в безопасности наблюдается во все большем числе сфер человеческой деятельности. Таким образом, применение контроля доступа не ограничивается сферами, описанными ниже, и уже сейчас появляется необходимость в применении контроля доступа во все новых и новых областях.

9.2.1 Банковское применение

В банковской системе на протяжении многих лет использовались разнообразные биометрические технологии. Мошенничество и нарушения системы безопасности должны строго контролироваться, если банки хотят остаться конкурентоспособными в постоянно развивающейся и диверсифицирующейся индустрии финансовых услуг. Биометрия может сыграть роль данного элемента контроля во многих ситуациях. Такие слабые каналы передачи данных, как банкоматы и транзакции в точках продаж, крайне уязвимы для мошенников и могут быть защищены с помощью биометрических технологий. Появляющиеся сегодня рынки банковских услуг по телефону и через Интернет также должны быть полностью безопасны не только для клиентов банков, но и для банковских служащих. На сегодняшний день огромное число различных биометрических технологий стремятся доказать свою работоспособность во всех сферах и на всех рынках.

9.2.2 Системы вознаграждений, льгот и соцобеспечения

Системы вознаграждений и льгот, подобно банковским системам, уязвимы для мошенников. Многие годы и во многих странах министерства социального обеспечения ведут решительную борьбу с мошенничествами. Основная задача состоит в предотвращении многократной регистрации одного и того же лица, таким образом, важнейшей особенностью системы является обязательная проверка «один-ко-многим» в процессе регистрации, при выплате социального обеспечения проверка «один-к-одному» также обязательна. В данной сфере применяется огромное число разнообразных биометрических технологий, самой распространенной из которых считается распознавание по отпечаткам пальцев. Технология АСДИ и верификация «один-к-одному» могут быть применены для гарантии того, что заявитель на соцобеспечение правомерно получает чек. Еще одной разработкой, которая обещает стать революционной в сфере соцобеспечения, является электронная система перевода вознаграждений и льгот, которая перечисляет средства на пластиковую карту. Данная карта может быть применена при покупке еды и других необходимых вещей в магазинах, оборудованных специальными аппаратами по приему карт, биометрические технологии имеют все возможности для капитализации на данном рынке, а поставщики биометрических услуг укрепляют взаимоотношения с сообществом по соцобеспечению, которое на данный момент этими взаимоотношениями довольно.

9.2.3 Контроль доступа к компьютерным системам

Контроль доступа к компьютерным системам (также известный как «контроль логического доступа») крайне важен, потому что несанкционированный доступ к компьютерным системам может нанести вред частным компьютерным сетям и пользователям интернета. При несанкционированном доступе сеть не может работать в полном объеме до тех пор, пока существует пробел в системе безопасности. Биометрические технологии доказывают свою способность защищать компьютерные сети. Данная область рынка демонстрирует высокий потенциал, особенно в том случае, когда биометрическая индустрия переключится на крупномасштабные применения в интернете. Так как банковские данные, бизнес-информация и аналитика, пароли кредитных карт, медицинские данные и иные личные данные все чаще становятся объектами атак мошенников, возможности поставщиков биометрических услуг в этом случае только увеличиваются.

9.2.4 Контроль иммиграции

Терроризм, перевозка наркотиков, нелегальная иммиграция и увеличивающееся число законопослушных путешественников и туристов ставит иммиграционные власти во всем мире в затруднительное положение. Необходимо в автоматическом режиме быстро осматривать путешественников и туристов, проверять их на предмет криминального прошлого, выявлять поддельные визы и идентифицировать тех, кому просто нельзя по той или иной причине въезжать в конкретную страну или выезжать из нее. Биометрические технологии уже активно применяются для осуществления перечисленных выше действий. Многие службы иммиграции и натурализации успели оценить преимущества биометрических технологий. На сегодняшний день подобные системы применяются во многих странах для автоматической обработки потока законопослушных путешественников и туристов, предотвращения въезда нелегальных иммигрантов.

9.2.5 Идентификационные карты

Биометрия становится полезной в государственных целях. С помощью биометрических технологий фиксируется прирост численности населения, идентифицируются граждане и предотвращаются мошенничества во время местных или всеобщих выборов. Применение подобных систем обычно связано с хранением шаблона (биометрического эталона) на карте, которая, в свою очередь, выступает в роли документа о национальной принадлежности. В системе особенно распространено применение технологии отпечатков пальцев, а сами схемы активно разрабатываются и совершенствуют во многих странах мира.

9.2.6 Контроль непосредственного доступа

На примере контроля непосредственного доступа можно продемонстрировать использование биометрии, которая не поддается классификации. Многие организации применяют биометрию для защиты физического перемещения людей. Школы, атомные станции, военные объекты, парки отдыха, больницы, офисы и супермаркеты по всему миру применяют биометрические технологии для минимизации угроз безопасности.

9.2.7 Применение в тюрьмах, следственных изоляторах и камерах предварительного заключения

В тюрьмах, следственных изоляторах и камерах предварительного заключения в отличие от применения в правоохранительных органах биометрия не применяется для поимки преступников; применение необходимо для уверенности в том, что заключенные гарантировано находятся под стражей. Другими словами, речь идет о контроле доступа в условиях тюрем, следственных изоляторов и камер предварительного заключения. Удивительно, но многие заключенные выходят из тюрьмы еще до официального освобождения. По всему миру применяется огромное количество биометрических технологий для контроля доступа в тюрьму, в области, контролируемые правоохранительными органами, выполнения решений о домашнем заключении и контроля действий условно осужденных преступников и условно-досрочно освобожденных. Системы распознавания личностей по голосу становится все более востребованными для контроля условно-досрочно освобожденных посредством автоматической записи свидетельства их присутствия (с помощью наземной линии телефонной связи) без необходимости в их присутствии в отделении правоохранительных органов.

9.2.8 Телефонные системы

За последние десятилетия значительно развилась глобальная коммуникационная система. На данный момент доступны мобильные телефоны с прямым внутрисистемным доступом и другие телекоммуникационные услуги. Сотовые компании также уязвимы в отношении клонирования (при котором создается новый номер телефона при помощи украденных цифр кода) и контрактного мошенничества (при котором телефонный номер приобретается при помощи поддельной идентификационной информации). Между тем, прямой внутрисистемный доступ, позволяющий авторизированным субъектам соединяться с центральной автоматической телефонной станцией и совершать бесплатные звонки, является мишенью для телефонных взломщиков. В очередной раз биометрия призвана защищать систему от подобных атак. Биометрия распознавания по голосу отлично подходит для применения в сфере телефонии и постепенно приходит на этот рынок. Система распознавания субъекта по голосу имеет огромный потенциал; ее наличие не позволит тем, кто украл мобильный телефон, воспользоваться им.

9.2.9 Применения для регистрации времени, посещаемости и наблюдения

Записи о перемещениях и наблюдение за перемещением работников в то время, когда они приходят на работу, обедают и уходят с работы, обычно осуществлялись с помощью машин отметки времени прихода на работу и ухода с работы на специальных часах. Однако процесс их деятельности можно перехитрить. Такая возможность лишает работу подобных машин смысла, нарушает планирование рабочего времени и контроль расходов. Замена такого оборудования на биометрическое снижает возможность неправильной эксплуатации системы и может быть интегрировано с программным обеспечением планирования рабочего времени для ведения управленческого учета и создания отчетов о сотрудниках.

9.2.10 Проверка граждан на криминальное прошлое

Все чаще и чаще биометрические системы применяются для проверки граждан на криминальное прошлое посредством проверки отпечатков пальцев. Обычно подобные проверки ограничивались теми

профессиями, в которых требовалось оформление допуска к секретной информации, но сейчас они требуются в разнообразных профессиях, таких как, например, профессии адвокат (для работы в суде), учитель или водитель школьного автобуса и школьный сторож. В США подобные проверки осуществляются по АСДИ ФБР, ежедневно обрабатываются данные десятков тысяч человек. В других странах существуют определенные законодательные требования на осуществление подобных проверок, хотя в настоящее время биометрия применяется еще не всегда.

10 Биометрия и конфиденциальность

10.1 Общие положения

Понятие «конфиденциальность» в разных культурах интерпретируется совершенно по-разному. Официальное определение «конфиденциальности» в каждой стране свое, в США — свое даже для каждого штата [1]. Классическим определением конфиденциальности является «естественное право быть оставленным в покое» [49], но современное определение конфиденциальности включает в себя также понятие «конфиденциальности информации»: право человека «определять самому, как и до какой степени информация о нем может быть сообщена другим лицам» [53], и право «информационного самоопределения» как право знать, кто получает информацию о субъекте, когда и с какой целью. Еще одним недавно определившимся правом является защищенность субъекта от кражи его идентификационной информации или право на быструю и достоверную идентификацию в условиях аварии или несчастного случая. Все эти три типа конфиденциальности сегодня подвергаются положительному и отрицательному воздействиям биометрических технологий.

10.2 Приемлемость биометрических технологий

Существует различие между способами сбора информации различными биометрическими системами с целью идентификации или допуска субъекта. Для некоторых систем необходим физический контакт субъекта с системой (например, в случае сканера, регистрирующего отпечаток пальца), что не отличается от применения обычной клавиатуры для ввода ПИН-кода. Для других биометрических систем необходимо освещение глаза субъекта, например, при регистрации изображения РОГ. Многие технологии крайне неинтрузивны, например, распознавание субъекта по изображению лица или сканирование РОГ субъекта. Для ряда культур считается недопустимым показывать лицо перед камерой. В некоторых культурах считается, что отпечаток ладони связан с библейским «знаком зверя». Для того чтобы приспосабливаться ко всем культурным традициям, необходимо создавать большое число различных биометрических технологий. Можно с успехом оспаривать (см. [2], [22]) тот факт, что тело не тождественно субъекту, которому оно принадлежит. В то время как ПИН-коды и пароли являются идентификационной информацией о личности субъекта, биометрические характеристики являются идентификационной информацией о теле субъекта.

Биометрические измерения могли бы связать различные психологические портреты личности, которые мы демонстрируем при общении в рамках социальных структур. Зарегистрированные биометрические характеристики субъекта могут способствовать соотнесению данных, например, трудовых книжек субъектов с их историями болезни. Объединение подобных данных о субъекте может проводиться на законных основаниях, однако источники биометрических данных должны оставаться анонимными, ни один субъект не должен быть идентифицирован. Аналогичные средства безопасности необходимы при повсеместном распространении биометрических технологий.

10.3 Защита от хищения персональных данных

Хищение и подделка персональной идентификационной информации являются серьезной и все более обостряющейся проблемой. На сегодняшний день существует большое количество способов избежать деятельности субъекта под разными электронными портретами его личности с целью обеспечения безопасности персональной конфиденциальной информации, а также прав и привилегий субъекта, в том числе на то, что никто не может скрываться под электронным портретом его личности. Применение биометрических технологий центральных баз данных биометрических шаблонов предоставляет современные способы гарантии того, что идентификационные документы могут быть получены лишь единожды и не смогут быть использованы кем-то другим при идентификации субъекта. Применение сложного шифрования для гарантии целостности биометрических шаблонов, записанных на картах, и проверка центральной базы на попытки повторной регистрации доказывает тот факт, что биометрические технологии являются необходимым и надежным средством обеспечения безопасности во всех сферах деятельности, связанных с удостоверением личности.

10.4 Конфиденциальность

По мере роста использования биометрических технологий по всему миру вопрос конфиденциальности становиться все важнее и важнее. Важно осознавать, какие именно задачи поставлены перед законом о защите информации и политикой защиты информации. Речь идет о защите прав субъектов, чьи биометрические данные обрабатываются, а также о защите субъектов, предоставляющих свои персональные данные. В биометрических системах в большинстве случаев применяются персональные данные субъектов, таким образом, в данном случае необходимо применение национальных законов в области конфиденциальности. В зависимости от способа использования биометрической системы применение биометрии может ставить под угрозу конфиденциальность персональных данных субъекта либо ее защищать. Возможность защиты является особенно реальной в свете особенностей биометрических характеристик, поскольку они находятся при субъекте и связаны с ним всю жизнь в отличие от ПИН-кодов и паролей, которые связаны с субъектом косвенно либо крайне неустойчиво и слабо. Таким образом, применение биометрических технологий обеспечивают лучшую сохранность персональных данных, чем при применении традиционных средств защиты. Вследствие этого биометрия может выступать в роли как объекта, так и инструмента в разных аспектах обсуждения. Во всех областях применения биометрических технологий должен присутствовать принцип пропорциональности, т. е. используемые биометрические данные должны быть адекватными, подходящими и неизбыточными в соответствии с теми целями, с которыми они собираются и обрабатываются. Биометрия может быть также применена в качестве технологии усиления конфиденциальности (ТУК) информации. Принцип ТУК 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 заключается в том, что биометрия сама по себе может быть методом усиления конфиденциальности. Основной вопрос, касающийся концепции ТУК и применения биометрии по принципу пропорциональности, заключается в том, требует или нет идентификация процессов традиционной информационной системы. В большинстве случаев нет необходимости в знании персональной идентификационной информации субъекта для предоставления ему прав доступа. Однако существуют ситуации, в которых субъект, предоставляющий персональные данные, должен раскрыть свою личность для осуществления верификации.

11 Заключение

Для применения биометрических технологий в таких областях, как криминалистика, проверка граждан на преступное прошлое и иммиграционный контроль, созданы и существуют биометрические системы высокого технического уровня. В иных областях применения биометрических технологий, таких как контроль физического и логического доступа и систем вознаграждений и льгот, биометрические системы только принимаются на вооружение.

Биометрические технологии существовали на протяжении десятилетий, однако их массовое выведение на потребительских рынок началось несколько лет назад (см. [40]), и даже сегодня существуют трудности с определением экономического обоснования, которое бы стимулировало потребительский спрос, и созданием единой системы, соответствующей различным типам людей. Тем не менее биометрическая индустрия медленно, но верно развивается, поскольку государство, организации и многие другие потребители находят подходящее применение биометрическим технологиям. Несмотря на то, что вопрос конфиденциальности продолжает вызывать споры, биометрия имеет все шансы применяться с целью усиления конфиденциальности. Тот факт, что биометрические технологии будут широко применяться в областях, связанных с информационной безопасностью, является лишь вопросом времени.

Приложение А
(справочное)

Краткая информация о биометрических стандартах

А.1 Развитие биометрической стандартизации

Примечание — Основные сокращения, определения и аббревиатуры, используемые в настоящем стандарте, приведены в приложении В.

А.1.1 Большинство работ в области биометрической стандартизации было инициировано в США. В 2002 г. для работы в области биометрической стандартизации был учрежден подкомитет ИСО/МЭК СТК 1/ПК 37, который впервые был представлен в декабре 2002 г. в городе Орландо.

А.1.2 Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК) образуют специализированную систему стандартизации во всем мире. Национальные органы по стандартизации, которые являются членами ИСО и МЭК, принимают участие в разработке международных стандартов через технические комитеты (ТК), учрежденные соответствующей организацией для решения вопросов в отдельных областях технической деятельности.

А.1.3 Технические комитеты ИСО и МЭК сотрудничают в областях взаимного интереса. Другие международные организации, правительственные и неправительственные, взаимодействуя с ИСО и МЭК, также принимают участие в работе.

А.1.4 В области информационных технологий ИСО и МЭК организовали соединенный технический комитет ИСО/МЭК СТК 1 «Информационные технологии». В июне 2002 г. ИСО/МЭК СТК 1 учредил подкомитет ПК 37 «Биометрия». Главной задачей соединенного технического комитета является подготовка международных стандартов. Данные стандарты необходимы для поддержки быстрого внедрения более совершенных и открытых систем безопасности на базе национальных стандартов,а также для предотвращения возможных краж идентификаторов.

А.1.5 Областью работы подкомитета ИСО/МЭК СТК 1/ПК 37 «Биометрия» является стандартизация универсальных биометрических технологий, касающихся человека, для поддержки взаимодействия и обмена биометрическими данными между приложениями и системами. Стандарты универсальных биометрических технологий включают в себя: общую файловую структуру; биометрический программный интерфейс, форматы обмена биометрическими данными; соответствующие биометрические профили; приложения для формирования критерия оценки в биометрических технологиях; эксплуатационные испытания, протоколы испытаний и другие социальные и юридические аспекты, зависящие от прикладной области.

А.2 Области биометрической стандартизации и рабочие группы

А.2.1 На данный момент не существует согласованной многослойной модели биометрической работы ИСО/МЭК СТК 1/ПК 37, используемая в настоящей программе модель биометрической системы представлена в разделе 4. Другая многослойная модель взаимодействия областей стандартизации ИСО/МЭК СТК 1/ПК 37 представлена в ИСО/МЭК 24713-1 «Информационные технологии — Биометрические профили для взаимодействия и обмена данными — Часть 1: Общая архитектура биометрической системы и биометрические профили» (см. А.11.6.1).

А.2.2 Шесть уровней биометрической стандартизации и дополнительные области, связанные с вопросами конфиденциальности и социума, представлены на рисунке А.1. Порядок уровней определяется порядком реализации стандартов, где реализация стандартов верхних уровней зависит от реализации стандартов нижних уровней. Вопросы конфиденциальности и социума в данную модель включены не были. Структура стандартов в виде диаграммы многослойной модели биометрических стандартов представлена на рисунке А.1.

А.2.3 В настоящей программе отражены:

- **(уровень 1)** Форматы ББД;
- **(уровень 2)** Форматы ЗБИ (ББД и метаданные ЕСФОБД);
- **(уровень 3)** Интерфейсы БиоАПИ между приложениями, структурой и поставщиками биометрической системы;
- **(уровень 4)** Протокол межсетевого взаимодействия БиоАПИ для обмена данными между биометрическими системами;
- **(уровень 5)** Стандарты испытаний на производительность и соответствие требованиям;
- **(уровень 6)** Биометрические профили для прикладных областей применения;
- **(уровень 7)** Социальные и юридические аспекты, зависящие от предметной области.

В основе лежит унифицированный словарь.

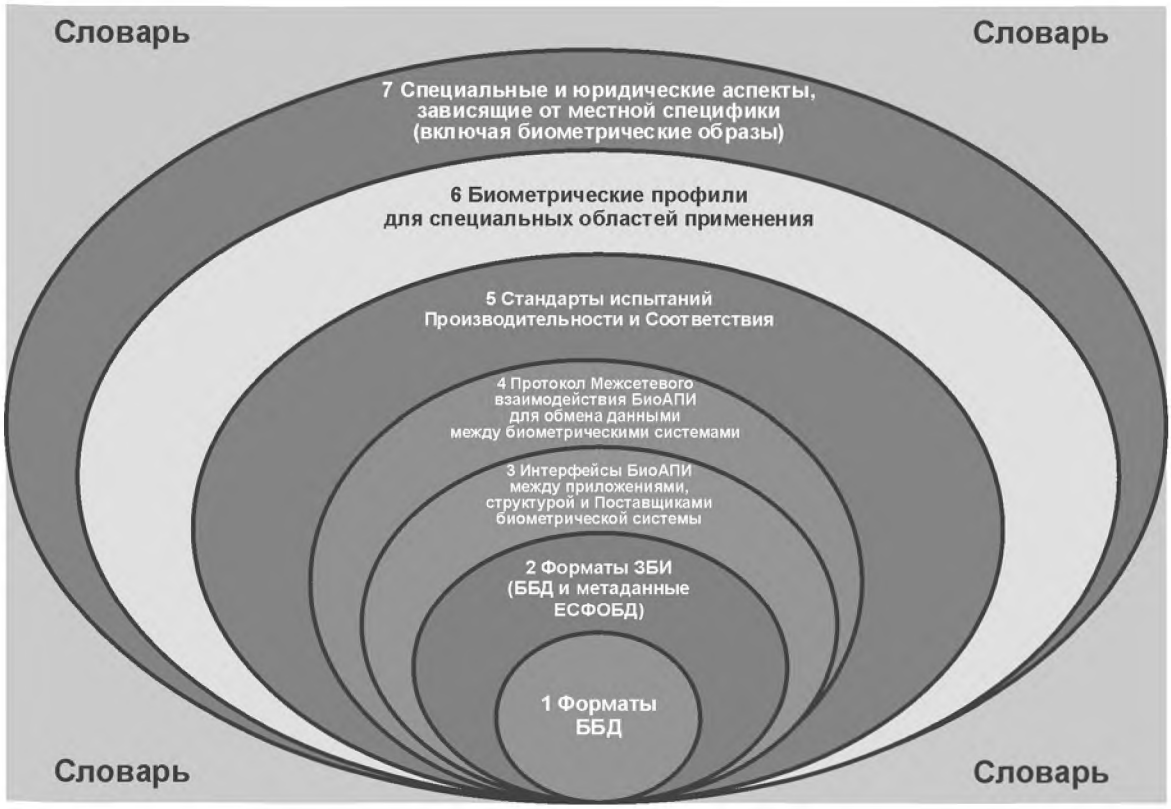

Рисунок А.1 — Многослойная модель биометрических стандартов

А.2.4 Работа по разработке стандартов проводится в следующих рабочих группах ИСО/МЭК СТК 1/ПК 37:

РГ1 — гармонизированный словарь терминов и определений;

РГ2 — технические интерфейсы в биометрии (стандарты уровней 2, 3, 4 и 5);

РГ3 — форматы обмена данными в биометрии (стандарты уровня 1);

РГ4 — биометрическая функциональная архитектура и связанные профили (стандарты уровня 6);

РГ5 — испытания и отчеты об испытаниях в биометрии (стандарты уровня 5);

РГ6 — социальные и кросс-юридические аспекты применения биометрических технологий (стандарты уровня 7).

А.3 Стандарты уровня 1 (утверждены или находятся в процессе разработки)

ИСО/МЭК 19794-1 *Информационные технологии — Форматы обмена биометрическими данными — Часть 1: Структура*

ИСО/МЭК 19794-2 *Информационные технологии — Форматы обмена биометрическими данными — Часть 2: Данные изображения отпечатка пальца — контрольные точки*

ИСО/МЭК 19794-3 *Информационные технологии — Форматы обмена биометрическими данными — Часть 3: Спектральные данные изображения отпечатка пальца*

ИСО/МЭК 19794-4 *Информационные технологии — Форматы обмена биометрическими данными — Часть 4: Данные изображения отпечатка пальца*

ИСО/МЭК 19794-5 *Информационные технологии — Форматы обмена биометрическими данными — Часть 5: Данные изображения лица*

ИСО/МЭК 19794-6 *Информационные технологии — Форматы обмена биометрическими данными — Часть 6: Данные изображения радужной оболочки глаза*

ИСО/МЭК 19794-7 *Информационные технологии — Форматы обмена биометрическими данными — Часть 7: Данные динамики подписи*

ИСО/МЭК 19794-8 *Информационные технологии — Форматы обмена биометрическими данными — Часть 8: Данные структуры остова отпечатка пальца*

ИСО/МЭК 19794-9 *Информационные технологии — Форматы обмена биометрическими данными — Часть 9: Данные изображения сосудистого русла*

ИСО/МЭК 19794-10 *Информационные технологии — Форматы обмена биометрическими данными — Часть 10: Данные геометрии контура кисти руки*

ИСО/МЭК 19794-11 *Информационные технологии — Форматы обмена биометрическими данными — Часть 11: Обработанные данные динамики подписи*

ИСО/МЭК 29794-1 *Информационные технологии — Качество биометрического образца — Часть 1: Структура*

ИСО/МЭК 29794-4 *Информационные технологии — Качество биометрического образца — Часть 4: Качество образца отпечатка пальца*

ИСО/МЭК 29794-5 *Информационные технологии — Качество биометрического образца — Часть 5: Качество образца данных изображения лица*

А.4 Стандарты уровня 2 (утверждены или находятся в процессе разработки)

ИСО/МЭК 19785-1 *Информационные технологии — Единая структура форматов обмена биометрическими данными — Часть 1: Спецификация элементов данных*

ИСО/МЭК 19785-2 *Информационные технологии — Единая структура форматов обмена биометрическими данными — Часть 2: Процедуры действий регистрационного органа в области биометрии*

ИСО/МЭК 19785-3 *Информационные технологии — Единая структура форматов обмена биометрическими данными — Часть 3: Спецификация форматов ведущей организации*

А.5 Стандарты уровня 3 (утверждены или находятся в процессе разработки)

ИСО/МЭК 19784-1 Информационные технологии — Биометрический программный интерфейс — Часть 1: Спецификация биометрического программного интерфейса

ИСО/МЭК 19784-2 Информационные технологии — Биометрический программный интерфейс — Часть 2: Интерфейс поставщика функции биометрического архива

ИСО/МЭК ТО 24722 Информационные технологии — Биометрия — Мультимодальные и другие мультибиометрические технологии

А.6 Стандарты уровня 4 (утверждены или находятся в процессе разработки)

ИСО/МЭК 24708 *Информационные технологии — Биометрия — Протокол межсетевого обмена БиоАПИ*

А.7 Стандарты уровня 5 (утверждены или находятся в процессе разработки)

ИСО/МЭК 19795-1 *Информационные технологии — Эксплуатационные испытания и протоколы испытаний в биометрии — Часть 1: Принципы и структура*

ИСО/МЭК 19795-2 *Информационные технологии — Эксплуатационные испытания и протоколы испытаний в биометрии — Часть 2: Методики испытаний для оценки технологий и программ*

ИСО/МЭК ТО 19795-3 *Информационные технологии — Эксплуатационные испытания и протоколы испытаний в биометрии — Часть 3: Особенности проведения испытаний при различных биометрических модальностях*

ИСО/МЭК 19795-4 *Информационные технологии — Эксплуатационные испытания и протоколы испытаний в биометрии — Часть 4: Испытания на совместимость*

ИСО/МЭК 24709-1 *Информационные технологии — Испытания на соответствие биометрическому программному интерфейсу (БиоАПИ) — Часть 1: Методы и процедуры*

ИСО/МЭК 24709-2 *Информационные технологии — Испытания на соответствие биометрическому программному интерфейсу (БиоАПИ) — Часть 2: Утверждения проверки для поставщиков биометрических услуг*

ИСО/МЭК 24709-3 *Информационные технологии — Испытания на соответствие биометрическому программному интерфейсу (БиоАПИ) — Часть 3: Утверждения проверки для структуры БиоАПИ*

ИСО/МЭК 24709-4 *Информационные технологии — Испытания на соответствие биометрическому программному интерфейсу (БиоАПИ) — Часть 4: Утверждения проверки для приложений БиоАПИ*

А.8 Стандарты уровня 6 (утверждены или находятся в процессе разработки)

ИСО/МЭК 24713-1 *Информационные технологии — Биометрические профили для взаимодействия и обмена данными — Часть 1: Общая архитектура биометрической системы и биометрические профили*

ИСО/МЭК 24713-2 *Информационные технологии — Биометрические профили для взаимодействия и обмена данными — Часть 2: Контроль физического доступа работников аэропортов*

ИСО/МЭК 24713-3 *Информационные технологии — Биометрические профили для взаимодействия и обмена данными — Часть 3: Биометрическая верификация и идентификация моряков*

А.9 Стандарты уровня 7 (утверждены или находятся в процессе разработки)

ИСО/МЭК ТО 24714-1 *Юридические и социальные аспекты внедрения биометрических технологий, зависящие от местной специфики — Часть 1: Руководство по доступности, аспектам конфиденциальности, здоровья и безопасности при применении биометрических систем в коммерческих целях*

ИСО/МЭК ТО 24714-2 *Юридические и социальные аспекты внедрения биометрических технологий, зависящие от местной специфики — Часть 2: Практическое применение в конкретных условиях*

А.10 Словарь терминов (утверждены или находятся в процессе разработки)

Гармонизированный словарь терминов и определений по биометрии (самостоятельный документ ИСО/МЭК СТК 1/ПК 37) ИСО/МЭК 2382-37 *Информационные технологии — Словарь — Часть 37: Гармонизированный словарь терминов и определений по биометрии*

А.11 Краткая информация об используемых стандартах и технических отчетах

А.11.1 Стандарты уровня 1

А.11.1.1 Форматы обмена биометрическими данными: структура (ИСО/МЭК 19794-1)

Данный стандарт устанавливает требования к стандартизации ББД и их применению в иных структурах биометрических данных. В данном стандарте рассматриваются вопросы захвата, извлечения признаков и при-

менения биометрических данных на уровне ББД, включая различие между ББД, содержащим данные об изображении, и ББД, извлекающим признаки. Также в данном стандарте рассматриваются требования к устройству регистрации, некоторые термины, используемые при работе с мультимодальными системами, и механизмы регистрации идентификатора формата ББД.

А.11.1.2 Форматы обмена биометрическими данными: данные изображения отпечатка пальца — контрольные точки (ИСО/МЭК 19794-2)

Данный стандарт устанавливает структуру данных и формат ББД, содержащую цифровую запись признаков, которые могут быть найдены и извлечены из цифрового изображения отпечатка пальца и записаны в базу данных. Данные признаки называются минуциями (контрольными точками) отпечатка пальца. Большинство людей знает, что при внимательном рассмотрении пальца можно обнаружить узор папиллярных линий, состоящий из гребней и впадин с точками, в которых один гребень разделяется на два, создавая новую впадину (бифуркация гребней), или в которых гребень заканчивается, а впадины по обеим сторонам сливаются в одну. Пример отпечатка пальца показан на рисунке А.2.



Рисунок А.2 — Пример отпечатка пальца

Посредством идентификации минуций и последующей записи их расположения относительно друг друга и подсчета количества гребней между парами минуций можно получить компактный шаблон цифрового изображения, который может быть использован для сопоставления двух отпечатков пальцев и выяснения принадлежности их одному и тому же субъекту. Принцип минуций отпечатков пальцев является достаточно сформировавшейся и надежной техникой сопоставления отпечатков пальцев.

В данном стандарте также установлены способы идентификации минуций и записи их расположения относительно друг друга и, что важно, определен формат, который необходимо использовать при записи информации (следует отметить, шаблон не является полным цифровым изображением отпечатка пальца, а представляет собой запись о расположении минуций относительно друг друга, что достаточно для точного сопоставления отпечатков пальцев).

Данный стандарт предоставляет возможность открытого взаимодействия различных производителей, что позволяет сопоставлять записи ББД изображений отпечатков пальцев, созданных на оборудовании различных производителей.

Соответствующие алгоритмы сопоставления не являются стандартизированными, примеры алгоритмов сопоставления и руководства по их использованию должны быть представлены в приложении.

Обычно ББД «захватывается» (формируется) в тот момент, когда субъект (личность) «регистрируется» (регистрируется организацией) и «вносится в базу данных» (сохраняется) с включением дополнительных метаданных о времени захвата, использованном оборудовании и т. д. Данная информация может быть сохранена на смарт-карте, которая находится у субъекта с собой или сохранена в центральной базе данных; также существует возможность сохранять информацию в нескольких местах. Данные варианты хранения ББД зависят от политики конфиденциальности, которая определяется самим субъектом либо национальным законодательством, и необходимости восстановления.

В данном стандарте определены два типа форматов данных изображений отпечатка пальца. Первый формат предоставляет возможность быстрого и простого сопоставления отпечатков пальцев, второй — возможность сжатия данных для хранения ББД на смарт-карте (и возможности сопоставления отпечатков пальцев при помощи смарт-карты).

А.11.1.3 Форматы обмена биометрическими данными: спектральные данные изображения отпечатка пальца (ИСО/МЭК 19794-3)

В данном стандарте устанавливается принцип математического преобразования изображения в «спектральные данные» для формирования одноразмерных областей изображения. Получение спектральных данных проводится с помощью компонентов дискретного преобразования Фурье, извлекаемых как из пересекающихся, так и из непересекающихся областей изображения. Рассмотрение математических принципов преобразования изображения выходит за рамки данного стандарта (речь идет об алгоритмах распознавания отпечатков пальцев, использующих спектральные данные для сопоставления сохраненного эталона, и с захваченным изображением отпечатка пальца).

А.11.1.4 Форматы обмена биометрическими данными: данные изображения отпечатка пальца (ИСО/МЭК 19794-4)

Данный стандарт устанавливает структуру данных и формат ББД, содержащую цифровую запись изображения одного или нескольких пальцев (или ладони). В данном стандарте определены способы регистрации изображения, преобразования его в цифровой вид и цифровой формат изображения отпечатка пальца.

Данный стандарт предоставляет возможность открытого взаимодействия производителей, что позволяет сопоставлять записи ББД изображений отпечатков пальцев, созданных на оборудовании различных производителей.

Соответствующие алгоритмы сопоставления не стандартизированы и являются конфиденциальной информацией организаций-производителей.

Обычно ББД «захватывается» (формируется) в тот момент, когда субъект (личность) «регистрируется» (регистрируется организацией) и «вносится в базу данных» (сохраняется) с включением дополнительных метаданных о времени захвата, использованном оборудовании и т. д. Данная информация может быть сохранена на смарт-карте, которая находится у субъекта с собой или сохранена в центральной базе данных, также существует возможность сохранять информацию в нескольких местах. Данные варианты хранения ББД зависят от политики конфиденциальности, которая определяется самим субъектом либо национальным законодательством, и необходимости восстановления.

А.11.1.5 Форматы обмена биометрическими данными: данные изображения лица (ИСО/МЭК 19794-5)

Данный стандарт устанавливает структуру данных и формат ББД, содержащие цифровую запись изображения лица.

В данном стандарте определены требования к условиям получения изображения лица (включая освещение, позу субъекта, выражение лица, головные уборы и т. д.) и его преобразования в цифровой вид, определен формат записи данных.

Данный стандарт предоставляет возможность открытого взаимодействия различных производителей, что позволяет сопоставлять записи ББД изображения лица, созданных на оборудовании различных производителей.

Алгоритмы сопоставления не стандартизированы и являются конфиденциальной информацией организаций.

Обычно ББД «захватывается» (формируется) в тот момент, когда субъект (личность) «регистрируется» (регистрируется организацией) и «вносится в базу данных» (сохраняется) с включением дополнительных метаданных о времени захвата, использованном оборудовании и т. д. Данная информация может быть сохранена на смарт-карте, которая находится у субъекта с собой или сохранена в центральной базе данных, также существует возможность сохранять информацию в нескольких местах. Данные варианты хранения ББД зависят от политики конфиденциальности, которая определяется самим субъектом либо национальным законодательством, и необходимости восстановления.

Некоторые контрольные точки на изображении лица представлены нарисунке А.3.

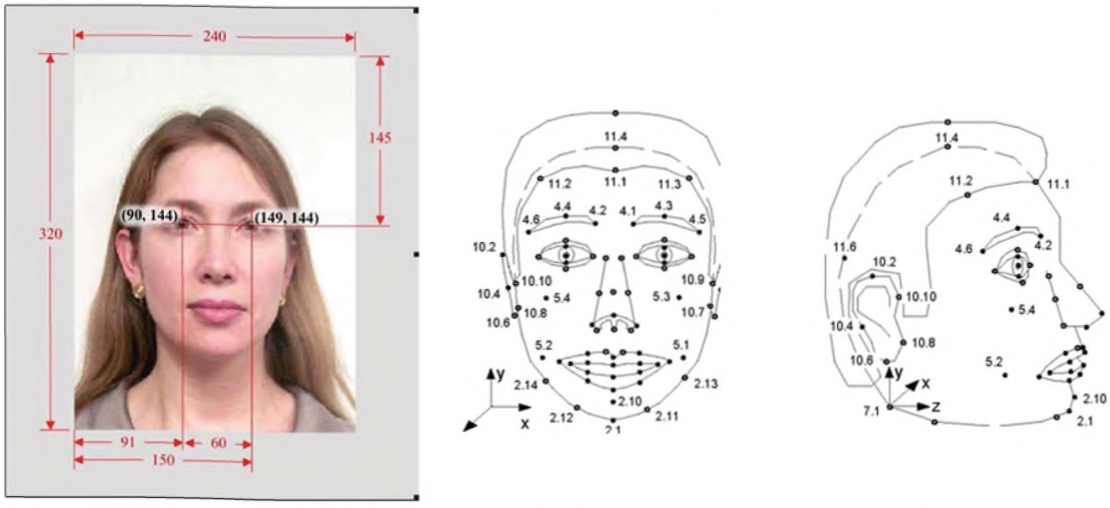

Рисунок А.3 — Некоторые контрольные точки на изображении лица

А.11.1.6 Форматы обмена биометрическими данными: данные изображения радужной оболочки глаза (ИСО/МЭК 19794-6)

В данном стандарте регламентирована структура данных (формат ББД), содержащая цифровую запись изображения РОГ (см. рисунок А.4).

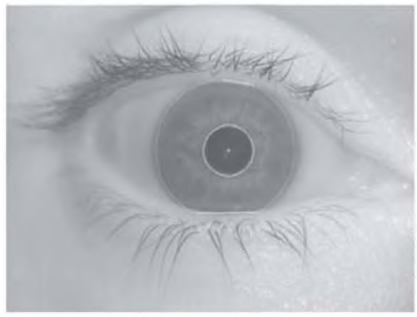

Рисунок А.4 — Изображение РОГ

В данном стандарте определены способы получения изображения, его преобразования в цифровой вид и формат цифрового изображения. Данным стандартом регламентировано два формата ББД: первый формат является полным, и для его создания требуется минимальная обработка изображения; второй формат представляет собой сжатый формат данных, и для его создания требуется бóльшая степень обработки изображения.

Данный стандарт предоставляет возможность открытого взаимодействия производителей, что позволяет сопоставлять записи ББД изображения РОГ, созданные на оборудовании различных производителей (при условии, что оба ББД предоставляют собой формат полного отображения информации об изображении либо сжатый формат).

Алгоритмы сопоставления не стандартизированы и являются конфиденциальной информацией организаций.

Обычно ББД «захватывается» (формируется) в тот момент, когда субъект (личность) «регистрируется» (регистрируется организацией) и «вносится в базу данных» (сохраняется) с включением дополнительных метаданных о времени захвата, использованном оборудовании и т. д. Данная информация может быть сохранена на смарт-карте, которая находится у субъекта с собой или сохранена в центральной базе данных, также существует возможность сохранять информацию в нескольких местах. Данные варианты хранения ББД зависят от политики конфиденциальности, которая определяется самим субъектом либо национальным законодательством, и необходимости восстановления.

А.11.1.7 Форматы обмена биометрическими данными: данные динамики подписи (ИСО/МЭК 19794-7)

Данный стандарт устанавливает форматы обмена данными для хранения, записи и передачи информации о динамических данных подписи, захваченной с использованием таких устройств, как планшеты или специальные ручки (см. рисунок А.5). Формат обмена данными динамики подписи/символа может быть применен как для получения промежуточных данных (служащих в качестве отправного момента для дальнейшего извлечения признаков), так и для получения непосредственно данных о признаке (для сопоставления алгоритмами измерения динамики). Зарегистрированные данные представляют собой последовательность значений различных точек во времени, включая такие параметры подписи субъекта, как положение пера ручки, нажим, скорость движения ручки, акселерация и наклон ручки. Важно отслеживать начальные координаты положения ручки во всех контрольных точках подписи; регистрация координат последующих положений ручки необязательна. Регистрация шаблонов подписи может происходить через установленные интервалы времени или варьироваться в зависимости от ситуации. Данный стандарт определяет два основных формата записи: полный и сжатый — для хранения данных с меньшим количеством параметров подписи, последний формат предпочтителен для хранения ББД на смарт-картах.

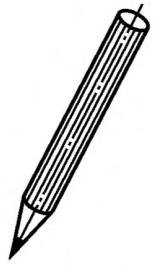

Рисунок А.5 — Ручка, перо

А.11.1.8 Форматы обмена биометрическими данными: данные структуры остова отпечатка пальца (ИСО/МЭК 19794-8)

Термин «остов» означает, что ББД основан на упрощении изображения до ряда линий размером с один пиксель (см. рисунок А.6), представляющих собой гребни отпечатка пальца, и дальнейшем извлечении из «скелета» данных о минуциях либо спектральных данных. Таким образом, данный стандарт включает в себя информацию и понятия о минуциях, отпечатке пальца, спектральном паттерне отпечатка пальца.



Рисунок А.6 — Пример остова изображения отпечатка пальца

А.11.1.9 Форматы обмена биометрическими данными: данные изображения сосудистого русла (ИСО/МЭК 19794-9)

В данном стандарте установлен формат ББД изображений «сосудистого русла» различных частей тела субъекта. «Данные сосудистого русла» представляют собой изображение паттерна кровеносных сосудов определенной части тела субъекта, зарегистрированное, как правило, с помощью соответствующего сканера, работающего в ближнем ИК-диапазоне. Для регистрации паттернов сосудистого русла подходят ладони, пальцы, запястья и тыльная сторона руки субъекта.

А.11.1.10 Форматы обмена биометрическими данными: данные геометрии контура кисти руки (ИСО/МЭК 19794-10)

В данном стандарте установлен формат записи ББД контура кисти руки. Для получения данных кисть руки с расставленными пальцами располагают на светочувствительной поверхности, освещают ярким светом и регистрируют черно-белое изображение, получаемое на поверхности. На практике для регистрации контура кисти руки, как правило, используют камеру, расположенную над рукой, лежащей на плоскости регистрации со специальными штифтами для правильной расстановки пальцев. В ББД записывается линия, которая ограничивает контур кисти руки от начальной до конечной точки. Регистрация контура кисти руки может проводиться как для изображений вида сверху (снизу), так и для изображений вида сбоку.

Зарегистрированные данные контура кисти руки преобразовываются в относительно небольшой по объему ББД, но достаточный для проведения измерений различных характеристик контура для их последующего сопоставления.

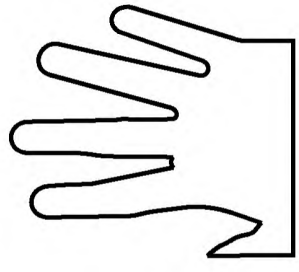

Рисунок А.7 — Контур кисти руки

А.11.1.11 Форматы обмена биометрическими данными: Обработанные данные динамики подписи (ИСО/МЭК 19794-11)

Данный стандарт является продолжением ИСО/МЭК 19794-7, посвященного записи различных статистических данных, связанных с захватом подписи субъекта.

А.11.1.12 Качество биометрических образцов (ИСО/МЭК 29794-1, ИСО/МЭК 29794-4 и ИСО/МЭК 29794-5)

Данная серия стандартов состоит из нескольких частей и устанавливает требования к способам измерения качества биометрических образцов в соответствии с серией стандартов ИСО/МЭК 19794.

А.11.1.13 Мультимодальные и другие мультибиометрические технологии (ИСО/МЭК ТО 24722)

Известно, что процедура биометрической идентификации может быть значительно улучшена, если в процессе сопоставления используются биометрические данные различных типов.

Такой подход называется мультибиометрическим. Он может быть основан на использовании нескольких шаблонов одних биометрических данных или (чаще всего) на использовании различных биометрических данных (например, изображение отпечатка пальца и изображение РОГ). Способ комбинирования результатов сопоставления биометрической информации, когда доступно большое количество биометрических шаблонов, достаточно сложен и называется «объединением» результатов.

Для определения мультибиометрической терминологии и рекомендаций в отношении реализации мультибиометрического подхода в ББД, единую структуру форматов обмена биометрическими данными и БиоАПИ необходима разработка технического отчета.

А.11.2 Стандарты уровня 2

А.11.2.1 Единая структура форматов обмена биометрическими данными (ЕСФОБД): спецификация элементов данных (ИСО/МЭК 19785-1)

В серии стандартов ИСО/МЭК 19794 установлены форматы цифрового представления биометрических данных различных биометрических характеристик человека: отпечатков пальцев, изображений лица и РОГ и т. д., каждый из которых представляет собой ББД. Как правило, ББД может быть обработан только при помощи модулей производителя биометрических услуг (ПБУ), предоставленного производителем, а не кодом прикладного уровня (как описано, например, в архитектуре БиоАПИ). Пока ББД на уровне приложения воспринимается в качестве данных с неясно выраженной структурой, которые приложение передает ПБУ или получает от ПБУ, оно не нуждается в информации о ББД, таким образом, приложение может определить, какой именно ПБУ (в системе с множеством ПБУ) должен обработать конкретный ББД.

В данном стандарте устанавливается архитектура для определения структур биометрических данных, включающих в себя как ББД, так и метаданные о ББД, которые могут быть получены на уровне приложения. Метаданные расположены в подструктуре «стандартный биометрический заголовок» (СБЗ), запись биометрической информации (ЗБИ) образуется объединением СБЗ и ББД. ЗБИ также может содержать доступные приложению данные с описанием атрибутов шифрования и целостности ЗБИ.

В данном стандарте установлены элементы данных, входящих в СБЗ для ЗБИ, содержащей только один ББД (простая ЗБИ) и ЗБИ, содержащей больше одного ББД (комплексная ЗБИ).

Спецификация данного стандарта устанавливает ряд абстрактных типов (элементов данных) и их семантику. Спецификация не устанавливает конкретных способов записи. Организация, отвечающая требованиям ЕСФОБД к ведущей организации ЕСФОБД, может опубликовать спецификацию поэлементного кодирования ЗБИ (структуру ЗБИ и содержание СБЗ), соответствующую требованиям ИСО/МЭК 19785-1. ИСО/МЭК СТК 1/ПК 37 разрабатывает форматы ведущих организаций ЕСФОБД (см. 11.2.3) как основные общепринятые форматы ЗБИ для хранения или передачи данных, которые могут служить в качестве примеров для иных организаций, желающих разработать собственные форматы ЗБИ.

В данном стандарте также определены правила преобразования форматов ЗБИ, поддерживающие различные наборы элементов данных ЕСФОБД или различные структуры ЗБИ.

А.11.2.2 Единая структура форматов обмена биометрическими данными (ЕСФОБД): процедуры действий регистрационного органа в области биометрии (ИСО/МЭК 19785-2)

Стандарты серии ИСО/МЭК 19794 устанавливают различные форматы блока биометрических данных для различных биометрических характеристик (отпечатка пальца, ладони, лица, РОГ и т. д.). ИСО/МЭК 19785-1 устанавливает основные элементы данных, связанные с ББД, для формирования ЗБИ. ИСО/МЭК 19785-3 устанавливает несколько форматов ЗБИ (см. А.11.2.3). Для идентификации форматов ББД, форматов ЗБИ и различных типов биометрической продукции необходимо установить соответствующие уникальные идентификаторы. В ИСО/МЭК 19785-2 установлены процедуры действий регистрационного органа в области биометрии для обеспечения уникальной идентификации (используя ASN.1 идентификатор объекта — см. ИСО/МЭК 8824 и ИСО/МЭК 9834) форматов и продуктов и организаций.

А.11.2.3 Единая структура форматов обмена биометрическими данными (ЕСФОБД): спецификации форматов ведущей организации (ИСО/МЭК 19785-3)

В данном стандарте установлено шесть (на данный момент) форматов ЗБИ (форматы ведущих организаций ЕСФОБД): форматы, предусматривающие использование минимального набора элементов данных ЕСФОБД; форматы, предусматривающие использования полного набора элементов данных ЕСФОБД; форматы, предполагающие и не предполагающие использования выравнивания по границе байта; форматы использующие битовую карту для обозначения присутствия определенных элементов данных. Некоторые элементы данных обозначены на английском языке с пояснениями в таблицах, некоторые обозначены при помощи ASN.1.

А.11.3 Стандарты уровня 3

А.11.3.1 Биометрический программный интерфейс: спецификация биометрического программного интерфейса (ИСО/МЭК 19784-1)

Данный стандарт представляет собой спецификацию архитектуры программного интерфейса для биометрических приложений (БиоАПИ). Описываемая модель позволяет использовать компоненты биометрической системы разных изготовителей и обеспечивать их взаимодействие посредством установленных программных интерфейсов приложений.

Основным компонентом программного обеспечения является инфраструктура БиоАПИ. Одной компьютерной системе соответствует одна инфраструктура. Вторым компонентом являются биометрические программные приложения, работающие в системе. Третьим компонентом являются модули ПБУ. Инфраструктура БиоАПИ поддерживает вызовы на языке программирования С биометрических программных приложений в адрес одного или нескольких модулей ПБУ (которые могут иметь соответствующие аппаратные средства).

Модули ПБУ выполняют такие функции, как, например, получение блока биометрических данных (цифровое представление изображения отпечатка человеческого пальца, ладони, изображения лица или РОГ и т. д. — см. ИСО/МЭК 19794) или сопоставление захваченного изображения с изображением, захваченным ранее и находящимся в архиве, с целью биометрической идентификации или верификации. Интерфейс между приложениями и инфраструктурой БиоАПИ называется программным интерфейсом приложений (ПИП).

Интерфейс между инфраструктурой БиоАПИ и модулями ПБУ называется интерфейсом поставщика услуги (ИПУ). ПИП и ИПУ устанавливают вызов функций на языке программирования С с указанием параметров вызова функций. Модули могут быть написаны с использованием других языков программирования, например Java или C++, если они реализуют установленные ПИП и ИПУ для взаимодействия с инфраструктурой БиоАПИ.

А.11.3.2 Биометрический программный интерфейс: интерфейс поставщика функции биометрического архива (ИСО/МЭК 19784-2) и интерфейс поставщика функции захвата биометрического образца (ИСО/МЭК 19784-3)

Данные стандарты БиоАПИ являются первыми в ряду частей, каждая из которых описывает интерфейс ПБУ определенного типа. Более подробное описание требует детального изучения архитектуры БиоАПИ и не является целью настоящего стандарта.

А.11.4 Стандарты уровня 4

А.11.4.1 Протокол межсетевого обмена БиоАПИ (ИСО/МЭК 24708)

В данном стандарте описывается, главным образом, линейная битовая связь биометрического программного приложения одной системы и ПБУ (например, устройства захвата биометрического образца или биометрического архива) удаленной системы. В процессе установления связи происходит отбор вызовов функций БиоАПИ на языке программирования С и преобразование их в сообщение при помощи ASN.1 (язык для описания абстрактного синтаксиса данных).

В целях соответствия техническим требованиям необходимо корректное применение линейной битовой связи, при этом программный код должен основываться на архитектуре БиоАПИ и вызовах функций.

Данный стандарт обеспечивает возможность доступа к биометрическим программным приложениям различных систем (например, роторных турникетов на спортивных мероприятиях и в парках отдыха), произведенных различными изготовителями с различных точек доступа или центрального сервера. Также он позволяет центральной (государственной) базе данных биометрических шаблонов взаимодействовать с географически удаленными системами захвата, верификации или сопоставления данных, предоставленными сторонними изготовителями.

А.11.5 Стандарт уровня 5

А.11.5.1 Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1: Принципы и структура (ИСО/МЭК 19795-1)

В данном стандарте описываются принципы и структура эксплуатационных испытаний биометрических систем и устройств. Целью эксплуатационных испытаний являются определение вероятностей ошибок и производительности биометрических систем, а также прогнозирование значений данных показателей при практической эксплуатации биометрической системы. Ошибки включают в себя ложноположительные решения (ложное совпадение) и ложноотрицательные решения (ложное несовпадение), а также отказы регистрации и отказы сбора данных для испытываемой выборки. Показатели пропускной способности определяют число пользователей, обрабатываемых в единицу времени, и зависят как от скорости вычислений, так и от времени взаимодействия человека с биометрической системой.

В данном стандарте определены методы проведения эксплуатационных испытаний (объем испытываемой выборки и т. д.), а также способ представления результатов испытаний в статистической и графической формах.

А.11.5.2 Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 2: Методология проведения технологического и сценарного испытаний (ИСО/МЭК 19795-2)

В данном стандарте определены методы проведения эксплуатационных испытаний и приведены инструкции по организации, проведению и способу представления результатов технологического и сценарного испытаний.

А.11.5.3 Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 3: Особенности проведения испытаний при различных биометрических модальностях (ИСО/МЭК ТО 19795-3)

В данном стандарте представлена классификация биометрических приложений в соответствии с методами эксплуатационных испытаний для определения эксплуатационных характеристик. Необходимо отметить, что в данном случае под термином «приложение» понимают применение биометрии с определенной целью, а не компьютерную программу с биометрическим программным интерфейсом, являющуюся частью биометрической

системы. Также в данном стандарте определены соответствующие методы испытаний для каждого биометрического приложения.

А.11.5.4 Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 4: Тестирование производительности биометрических систем* (ИСО/МЭК 19795-4)

В данном стандарте установлены требования к оценке эксплуатационных характеристик разнородных биометрических систем, включающих в себя компоненты различных поставщиков, и, в частности, к проведению сравнения различных устройств захвата биометрических данных, подсистем формирования и подсистем сравнения биометрических данных. В данном стандарте особое внимание уделено следующим вопросам:

- работают ли системы, использующие стандартизованные данные и форматы данных, также эффективно по сравнению с системами, использующими фирменные форматы биометрических данных;

- работает ли система поставщика настолько же эффективно со стандартизованными блоками биометрических данных других поставщиков, как со своими собственными блоками биометрических данных.

Данный стандарт был разработан после создания ряда стандартов формата обмена данными, наиболее известными из которых являются стандарты, посвященные шаблонам изображений отпечатков пальцев (ИСО/МЭК 19794-2, ИСО/МЭК 19794-3, ИСО/МЭК 19794-8) и изображений РОГ (ИСО/МЭК 19794-6).

А.11.5.5 Испытания на соответствие биометрическому программному интерфейсу: методы и процедуры (ИСО/МЭК 24709-1)

Данный стандарт устанавливает понятия, структуру, методы испытаний и критерии, необходимые для проведения испытаний биометрической продукции на соответствие спецификации БиоАПИ (см. ИСО/МЭК 19784-1). Данный стандарт устанавливает требования по определению комплекта тестов для соответствия спецификации БиоАПИ, написанию обобщенных тестовых утверждений и определению процедур испытания на соответствие. Испытание на соответствие элементов БиоАПИ (главным образом, ПБУ) осуществляется путем взаимодействия данных элементов с тестовой программой компьютерной системы, для которой они были разработаны.

А.11.5.6 Испытания на соответствие биометрическому программному интерфейсу: тестовые утверждения для поставщиков биометрических услуг (ИСО/МЭК 24709-2), утверждение проверки для структур БиоАПИ (ИСО/МЭК 24709-3) и утверждение проверки для приложений БиоАПИ (ИСО/МЭК 24709-4)

В данных стандартах представлены подробные описания необходимых испытаний.

А.11.6 Стандарты уровня 6

А.11.6.1 Биометрические профили для взаимодействия и обмена данными: общая архитектура биометрической системы и биометрические профили (ИСО/МЭК 24713-1)

В данном стандарте устанавливаются и определяются функциональные блоки и компоненты унифицированной биометрической системы и индивидуальные характеристики каждого компонента. Данный стандарт является справочным руководством по работе с биометрическими приложениями и включает в себя концепцию «списка наблюдений», которая отсутствует в стандартах серии ИСО/МЭК СТК 1/ПК 37.

В данном стандарте присутствует многослойная диаграмма, демонстрирующая взаимоотношение различных стандартов серии ИСО/МЭК СТК 1/ПК 37. Данный стандарт рекомендуется для ознакомления лицам, заинтересованным в более подробном обзоре ИСО/МЭК СТК 1/ПК 37 и их структуры.

А.11.6.2 Биометрические профили для взаимодействия и обмена данными: контроль физического доступа сотрудников аэропорта (ИСО/МЭК 24713-2)

Основной задачей данного стандарта является описание процесса выпуска «токенов» (как правило, смарт-карт) для сотрудников, которым необходим доступ в охраняемую зону, включая описание использования «списка наблюдений».

А.11.6.3 Биометрические профили для взаимодействия и обмена данными: биометрическая верификация и идентификация моряков (ИСО/МЭК 24713-3)

Данный стандарт предоставляет информацию об идентификации работников на морских судах по биометрическим характеристикам в соответствии с требованиями Международной организацией труда (МОТ).

А.11.7 Стандарты уровня 7

Юридические и социальные аспекты внедрения биометрических технологий, зависящие от предметной области: руководство пользователя, аспекты конфиденциальности, здоровье и безопасность при применении биометрических систем в коммерческих целях (ИСО/МЭК ТО 24714-1) и практическое применение в конкретных условиях (ИСО/МЭК ТО 24714-2).

Данная техническая документация определяет руководство пользователя, примеры применения и дополнительную информацию об основных социальных и юридических аспектах, зависящих от предметной области применения биометрии.

Техническая документация направлена на решение вопросов:

- доступности (преодоления трудностей, возникающих у лиц с ограниченными возможностями, не способных использовать биометрию);

---

* В оригинале международного документа ИСО/МЭК ТО 24741 ошибочно приведено наименование «Эксплуатационные характеристики биометрических систем контроля доступа».

- здоровья и безопасности (включает в себя информирование о ложных представлениях; о рисках, связанных с использованием биометрии и биометрических интерфейсов с целью определения этнической принадлежности; состояния здоровья и пола по биометрическим характеристикам субъекта).

- соблюдения законодательных требований и учета социальных и юридических аспектов, относящихся к личной информации и конфиденциальности субъекта.

Данная техническая документация разработана для операторов и специалистов по интегрированным системам, внедренным в частный сектор.

А.11.8 Стандарты словаря

А.11.8.1 Гармонизированный словарь терминов и определений по биометрии

Данный стандарт устанавливает термины и определения в области биометрических технологий, применяемых в ИСО/МЭК СТК 1/ПК 37. В словаре представлены термины, применяющиеся во всех стандартах связанных с биометрией, нуждающихся в однозначных определениях.

А.11.8.2 Свод терминов и определений по биометрии, представлен в ИСО/МЭК 2382-37

Данный стандарт направлен на соотнесение различных биометрических определений и представления их в организованном структурированном виде с целью однозначного определения взаимосвязи между биометрическими терминами и определениями и скоординированности их значений перед выпуском заключительной редакции словаря биометрических терминов данного стандарта.

Приложение В
(справочное)

Термины и определения, используемые в биометрических стандартах

В.1 Основные понятия

В.1.1 **аутентифицировать**(authenticate): Доказать или показать неоспоримость происхождения или достоверность чего-либо; определить подлинность.

В.1.2 **аутентификация** (authentication) — исключено.

(определение не представлено)

Примечание 1 — Употребление данного термина в качестве синонима биометрической верификации и биометрической идентификации исключено.

Примечание 2 — До настоящего времени термин использовался в качестве синонима биометрической верификации и функции биометрической верификации, а также в качестве синонима биометрической идентификации и функции биометрической идентификации.

В.1.3 **биометрический** (biometric): Имеющий отношение к биометрии.

Примечание — Употребление термина «биометрика» в качестве имени существительного для обозначения биометрической характеристики или биометрической модальности исключено.

Пример — Неверное использование #1: Международная организация гражданской авиации приняла решение о том, что лицо является наиболее подходящей биометрикой для дорожных документов.

Пример — Верное использование #1: Международная организация гражданской авиации приняла решение о том, что лицо является наиболее подходящей биометрической модальностью для дорожных документов.

Пример — Неверное использование #2: биометрика моего лица находится в виде закодированных данных в паспорте.

Пример — Верное использование #2: биометрические характеристики моего лица находится в виде закодированных данных в паспорте.

В.1.4 **биометрические характеристики** (biometric characteristic):

биометрика (biometric) — исключено.

Биологические и поведенческие характеристики субъекта, которые могут быть зарегистрированы и использованы в качестве отличительных повторяющихся признаков, которые могут быть использованы для автоматической идентификации личности.

Примечание 1 — Биологические характеристики и поведенческие реакции являются физическими характеристиками частей тела субъекта, психологическими реакциями и их комбинациями, производимыми субъектом.

Примечание 2 — Различие необязательно подразумевает индивидуализацию.

Пример — примеры биометрических характеристик: структура гребней Гальтона, топография лица, текстура кожи лица, топография руки, топография пальца, структура РОГ, структура вен кисти руки, структура гребней ладони, шаблон сетчатки глаза и т. д.

В.1.5 **биометрия** (biometrics): Автоматическое распознавание личности человека, основанное на его поведенческих и биологических характеристиках.

Примечание — В соответствии с областью применения, установленной ИСО/МЭК СТК 1/ПК 37, термин «индивидуальность» относится только к человеку.

В.1.6 **система** (system): Установленная схема или метод; комплекс отдельных элементов; набор элементов, работающих сообща как механизм или взаимозависимая сеть.

В.2 Термины, относящиеся к данным

В.2.1 **биометрические данные** (biometric data): Биометрический образец на любой стадии обработки, биометрический шаблон, биометрический признак или биометрические характеристики субъекта.

В.2.2 **блок биометрических данных (ББД)** [Biometric Data Block (BDB)]: Блок данных определенного формата, содержащий один или несколько биометрических шаблонов или эталонов.

Примечание — Определение приведено в соответствии с ЕСФОБД.

В.2.3 **биометрический признак** (biometric feature): Цифровое представление информации, извлеченной из биометрического образца и используемой для создания шаблонов или сравнения с зарегистрированными в базе данных шаблонами.

Примечание 1 — Употребление данного термина должно соответствовать тому, как его используют специалисты по распознаванию паттерна и специалисты в области математики.

Примечание 2 — Незавершенный процесс извлечения биометрического признака может быть сигналом ошибки или нулевым вектором.

Примечание 3 — Набором биометрических признаков может считаться обработанный биометрический образец.

В.2.4 **запись биометрической информации (ЗБИ)** [Biometric Information Record (BIR)]: Структура данных, включающая в себя один или более ББД вместе с информацией, идентифицирующей форматы ББД, и дополнительной информацией, например, о типе ББД (подписанный, зашифрованный).

Примечание — Определение приведено в соответствии с ЕСФОБД.

В.2.5 **биометрическая характеристика** (biometric property): Описательные атрибуты субъекта, рассчитанные или извлеченные из биометрического образца.

Пример — Отпечатки пальцев могут быть классифицированы по биометрическим характеристикам узора папиллярных линий (т. е. «дуга», «петля», «завиток»).

В случае распознавания личности по изображению лица биометрическими характеристиками являются возраст и пол.

В.2.6 **биометрическая модель** (biometric model): Сохраненная функция (индивидуальная для каждого субъекта), сформированная на основе одной или нескольких биометрических характеристик.

Примечание 1 — При сравнении функция применяется к биометрическим характеристикам шаблона для распознавания и последующего сопоставления.

Примечание 2 — Функция может быть определена посредством обучения на контрольной выборке.

Пример — Примерами сохраненных функций могут быть скрытая модель Маркова или искусственные нейронные сети.

В.2.7 **биометрический эталон** (biometric reference): Один или несколько сохраненных биометрических образцов, биометрических шаблонов или биометрических моделей, относящихся к субъекту и используемых для сопоставления.

Пример — Изображение лица в паспорте, эталон минуций отпечатка пальца на национальной идентификационной карте; гауссова модель смешения для идентификации личности по голосу в базе данных.

Примечание — Биометрический эталон может быть создан с косвенным или явным использованием вспомогательных данных, например, с помощью универсальных фоновых моделей.

В.2.8 **биометрический образец** (biometric sample): Аналоговое или цифровое представление (изображение) биометрических характеристик перед процессом извлечения биометрических признаков, получаемое от устройства захвата биометрического образца или подсистемы захвата биометрического образца.

Примечание — Устройство захвата биометрического образца представляет собой подсистему захвата образца с одним элементом.

В.2.8.1 **захваченный биометрический образец** (captured biometric sample):

необработанный биометрический образец (raw biometric sample) — исключено.

Биометрический образец, служащий входными данными для процесса обработки промежуточного биометрического образца.

В.2.8.2 **промежуточный биометрический образец** (intermediate biometric sample): Биометрический образец, являющийся выходными данными процесса обработки промежуточного биометрического образца.

Пример — Качество промежуточного биометрического образца может быть улучшено с целью дальнейшего извлечения биометрических характеристик или сжато с целью хранения в более компактном виде и т. д.

В.2.8.3 **биометрический образец для распознавания** (recognition biometric sample): Биометрический образец, используемый для распознавания посредством сопоставления с биометрическим шаблоном.

В.2.9 **биометрический шаблон** (biometric template): Набор сохраненных биометрических признаков для непосредственного сопоставления с биометрическими признаками распознаваемого биометрического образца.

Примечание 1 — Биометрический шаблон, состоящий из изображения или иного захваченного биометрического образца в оригинальном, улучшенном или сжатом виде, не является биометрическим эталоном.

Примечание 2 — Биометрические характеристики не считаются биометрическим шаблоном, если они не сохранены в качестве шаблона.

В.2.10 **объект данных** (data object): Дискретные данные, рассматриваемые как элемент, представляющий пример структуры данных, которая известна или предполагается известной.

Примечание — Источник определения: ИСО 2382-17, дата введения: 17.01.2011.

В.2.11 **база данных** (data base): Набор данных, упорядоченных в соответствии с концептуальной структурой, описывающей характеристики этих данных и взаимоотношение их соответствующих элементов, поддерживающих одно или несколько приложений.

В.2.12 **запись** (record): Объект данных, представляющий собой пример типа записи.

Примечание — Источник определения: ИСО 2382-17, дата введения: 17.05.2012.

В.3 Термины, связанные с захватом данных

В.3.1 **устройство захвата биометрических данных** (biometric capture device): Устройство, регистрирующее биометрические характеристики субъекта и преобразующее их в биометрический образец.

Примечание 1 — Осуществляется не только регистрация непосредственных биометрических характеристик субъекта, но и данных, непосредственно с ними связанных, например регистрация распределения отраженного светового потока при получении изображения лица.

Примечание 2 — Устройством может быть любое аппаратное устройство, поддерживающее программное и программно-аппаратное обеспечение.

В.3.2 **процесс захвата биометрических данных** (biometric capture process): Процесс сбора или попытки сбора биометрических характеристик и их преобразования в биометрический образец.

Примечание — Осуществляется не только регистрация непосредственных биометрических характеристик субъекта, но и данных, непосредственно с ними связанных, например, регистрация распределения отраженного светового потока при получении изображения лица.

В.3.3 **подсистема захвата биометрических данных** (biometric capture subsystem): Элементы и подпроцессы, необходимые для осуществления процесса захвата биометрических данных.

Пример — Некоторые системы, преобразующие сигнал от биометрической характеристики в биометрический образец, могут включать в себя такие элементы, как камера, фотобумага, принтер, чернила и бумага.

В.3.4 **захват данных** (capture): Процесс сбора биометрических образцов в текстовом или графическом формате с последующим сохранением в базе данных.

В.4 Термины, связанные с регистрацией

В.4.1 **адаптация биометрического шаблона** (biometric reference adaptation): Автоматическая постепенная корректировка биометрического шаблона для улучшения характеристик изображения.

Примечание — Например, ухудшение может быть следствием незначительных изменений в биометрической характеристике, канале или датчике.

В.4.2 **повторная проверка регистрации** (duplicate enrolment check): Сравнение биометрического образца /биометрического признака / биометрической модели для распознавания с некоторыми или со всеми биометрическими шаблонами в регистрационной базе данных с целью определения аналогичных биометрических шаблонов.

В.4.3 **регистрировать** (enrol): Создать или сохранить для личности регистрационную запись данных, относящихся к личности и включающую в себя: биометрический (ие) шаблон (ы) и, как правило, персональные данные о субъекте.

В.4.4 **запись регистрационных данных** (enrolment data record): Запись, создаваемая при регистрации, относящаяся к субъекту и включающая в себя один или несколько биометрических шаблонов.

В.4.5 **регистрация** (enrolment): Процесс регистрации или внесения в список.

В.4.6 **запись регистрационных данных** (enrolment data record): Запись, создаваемая при регистрации, относящаяся к субъекту и включающая в себя один или несколько биометрических шаблонов и, как правило, персональные данные о субъекте.

В.4.7 **повторная регистрация** (re-enrolment): Процесс создания нового биометрического шаблона для личности, уже зарегистрированной в базе данных.

Примечание 1 — Для процесса повторной регистрации требуется наличие одного или нескольких новых биометрических образцов.

Примечание 2 — Например, повторная регистрация может потребоваться в случае серьезных изменений в системе или биометрических характеристиках.

B.4.8 **внесение в список** (registration): Действие или процесс внесения в список; соответствие положения печатной информации на обеих сторонах листа.

Примечание 1 — Регистрировать(глагол) — вводить или вносить в журнал регистраций.

Примечание 2 — Журнал регистраций (существительное) — официальной список регистрационных записей.

Примечание 3 — Источником определения слов «регистрировать» и «журнал регистраций» (глагол и существительное) является оксфордский словарь.

B.5 Термины, связанные с процессами и системой

B.5.1 **процесс извлечения биометрических признаков** (biometric feature extraction process): Алгоритм, применяемый к биометрическому образцу с целью определения локализации и выделения, повторяющихся или характерных цифр и признаков, которые могут быть сравнимы с цифрами и признаками, извлеченными из других биометрических образцов.

Примечание 1 — Фильтры, применяемые к биометрическим образцам, не являются биометрическими признаками, несмотря на то, что выходные данные фильтра, примененного к этим образцам, могут быть биометрическими признаками. Таким образом, например, айгенфейсы не являются биометрическими признаками.

Примечание 2 — Термин «повторяющиеся» предполагает низкую степень разброса между выходными данными, полученными из образцов одного субъекта.

Примечание 3 — Термин «дистинктивные» предполагает высокую степень разброса между выходными данными, полученными из образцов разных субъектов.

B.5.2 **биометрическая система** (biometric system): Система, применяемая для автоматической идентификации личности, основанной на их поведенческих реакциях и биологических характеристиках.

B.5.3 **дешифрование** (decryption): Действие обратное шифрованию.

Примечание — Источник определения: ИСО 18033-1.

B.5.4 **шифрование** (encryption): Обратимое преобразование данных с помощью криптографического алгоритма для создания зашифрованного текста с целью защиты информации (обеспечения конфиденциальности).

Примечание — Источник определения: ИСО 18033-1.

B.5.5 **обработка промежуточного биометрического образца** (intermediate biometric sample processing): Любые виды манипуляций с биометрическим образцом, результатом которых не становится создание биометрических признаков.

Пример — Примерами обработки промежуточного биометрического образца являются: обрезание, субдискретизация, сжатие, преобразование в формат обмена данными и улучшение изображения.

B.6 Термины, связанные с личностью

B.6.1 **заявитель** (applicant): Человек, запрашивающий какую-либо информацию.

B.6.2 **обслуживающее лицо** (attendant): Оператор биометрической системы, который непосредственно взаимодействует с субъектом захвата биометрических данных.

Пример — Сотрудник иммиграционной службы, который руководит процессом захвата биометрических данных и предпринимает действия по вынесению результата сопоставления.

B.6.3 **субъект захвата биометрических данных** (biometric capture subject): Личность, являющаяся субъектом захвата биометрических данных.

B.6.4 **субъект биометрических данных** (biometric data subject): Личность, чьи персональные биометрические данные находятся в биометрической системе.

Примечание — Назначение слова «персональная» состоит в поиске различий между субъектами биометрических данных и теми, чьи совокупные данные послужили для создания алгоритма биометрического распознавания. К ним относятся личности, не являющиеся субъектами биометрических данных, зарегистрированные на этапе создания универсальной фоновой модели в системах распознавания личности по голосу или способствовавшие созданию базисного набора айгенфейсов в системе распознавания личности по изображению лица.

B.6.5 **биометрический «самозванец»** (biometric impostor): Субъект захвата биометрических данных, который хочет быть неверно опознанным посредством создания ложного совпадения или обойдя биометрическую систему положительных запросов.

Примечание 1 — Биометрический «самозванец» может обойти биометрическую систему посредством любой формы социально-технического нападения (социальной инженерии) (например, подкуп).

Примечание 2 — Подлинный пользователь, ошибочно идентифицированный как другой субъект, не является биометрическим «самозванцем».

B.6.6 **оператор биометрической системы** (biometric system operator): Человек, управляющий биометрической системой в соответствии с правилами и порядком управления конкретной биометрической системы.

B.6.7 **владелец биометрической системы** (biometric system owner): Человек, полностью отвечающий за получение, внедрение и эксплуатацию биометрической системы.

B.6.8 **обычный «самозванец»** (casual impostor): Биометрический «самозванец», действующий без применения искусственных средств идентификации, знаний и умений.

B.6.9 **мошенник** (deceiver): Субъект захвата биометрических данных, пытающийся избежать идентификации посредством создания ложного несовпадения или обойдя биометрическую систему с помощью ложноотрицательных запросов.

B.6.10 **конечный пользователь** (end-user) — исключено.

(определение не представлено)

Примечание — Термин «конечный пользователь» предполагает активное взаимодействие с биометрической системой и не может быть спутан с владельцем биометрической системы, оператором биометрической системы или биометрическим субъектом.

B.6.11 **регистрируемый** (enrolee): Субъект биометрических данных, чьи биометрические данные хранятся в регистрационной базе данных.

B.6.12 **индивидум** (individual): Конкретный человек; один человек в отличие от группы.

B.6.13 **субъект-злоумышленник** (malicious subject): Субъект захвата биометрических данных, который намеренно производит ложные запросы при работе с биометрической системой.

B.6.14 **мотивированный «самозванец»** (motivated impostor): «Самозванец», действующий подготовлено, используя искусственные средства идентификации, знания и умения.

B.6.15 **пользователь** (user): Любой человек, тем или иным образом взаимодействующий с биометрической системой.

Примечание — При обсуждении определенной группы людей, вовлеченных во взаимодействие с биометрической системой для обозначения каждого класса, необходимо наличие определенных терминов, например, люди, чьи биометрические данные собираются, должны называться субъектами.

B.7 Термины, связанные с сопоставлением

B.7.1 **решение биометрического приложения** (biometric application decision): Решение, обусловленное политикой решений об одном или нескольких совпадениях, результатах сопоставления и других персональных данных о субъекте.

Примечание 1 — Решение биометрического приложения может быть вынесено на основе комплекса правил, допускающих различное число положительных решений о совпадении.

Примечание 2 — Протокол биометрической верификации может вынести положительное решение даже в том случае, если имеется одно или более несовпадений при сопоставлении с зарегистрированным биометрическим шаблоном.

Пример — решением может быть принятие запроса.

B.7.2 **биометрический запрос** (biometric claim): Утверждение о том, что личность является или не является источником конкретного или неконкретного шаблона в биометрической регистрационной базе данных.

Примечание 1 — Запрос биометрической системе может быть сделан любым пользователем.

Примечание 2 — Фраза «запрос на идентификацию» часто используется для обозначения общего представления.

Примечание 3 — Запрос может быть положительным — личность/источник зарегистрированы; отрицательным — личность/источник не зарегистрированы; конкретным — личность/источник зарегистрирован или не зарегистрирован в качестве определенной зарегистрированной личности; неконкретным — личность/источник присутствует или не присутствует во множестве или подмножестве зарегистрированных личностей.

Примечание 4 — Биометрические запросы могут быть сделаны от первого, второго или третьего лица.

B.7.3 **биометрическая идентификация (функция биометрической системы)** (biometric identification (biometric system function)): Функция биометрической системы, которая производит поиск «один-ко-многим» для получения списка кандидатов.

Пример — BioAPI_IdentifyMatch.

Примечание — Биометрическая функция идентификации может быть использована для верификации запроса на регистрацию в регистрационной базе данных без определенного идентификатора биометрического шаблона.

В.7.4 **приложение биометрической идентификации** (biometric identification application): Система, содержащая приложение идентификации на открытом множестве и на замкнутом множестве.

В.7.5 **биометрическая верификация (биометрическое приложение)** [biometric verification (biometric application)]:

аутентификация (authentication) — исключено.

Приложение, определяющее подлинность/неподлинность запроса о схожести одного или нескольких биометрических эталонов и биометрических образцов для распознавания путем проведения одного или нескольких сопоставлений.

Пример — Верификацией считается установление истины любого из следующих запросов: «я зарегистрирован как субъект X», «я зарегистрирован в базе данных как администратор», «я не зарегистрирован в базе данных».

Примечание — Запрос на регистрацию в базе данных без предъявления идентификатора биометрического шаблона может быть верифицирован посредством полного перебора вариантов во время поиска.

В.7.6 **биометрическая верификация (функция биометрической системы)** [biometric verification (biometric system function)]:

аутентификация (authentication) — исключено.

положительная идентификация (positive identification) — исключено.

Функция биометрической системы, осуществляющая сопоставление «один-к-одному».

Пример — BioAPI_VerifyMatch.

Примечание — Биометрическое приложение идентификации может использовать полный набор вызовов функции верификации.

В.7.7 **идентификатор биометрического эталона** (biometric reference identifier): Указатель на биометрический эталон в регистрационной базе данных.

В.7.8 **кандидат** (candidate): Идентификатор биометрического образца в регистрационной базе данных, установленный в качестве схожего с биометрическим образцом для распознавания.

Примечание — Установление может осуществляться на основе результата сопоставления и/или ранга.

В.7.9 **список кандидатов** (candidate list): Набор, состоящий из нуля, одного или нескольких промежуточных или окончательных кандидатов.

Примечание — Промежуточный список кандидатов может быть создан многопроходной биометрической идентификацией.

В.7.10 **результат кандидата** (candidate score): Результат сопоставления кандидата.

В.7.11 **сопоставление** (comparison):

сравнение / совпадение (match / matching) – исключено в качестве синонима сопоставления.

Оценка, вычисление или измерение степени схожести и различия между биометрическими образцами / биометрическими признаками / биометрическими моделями для распознавания и биометрическими шаблонами.

Примечание 1 — Сопоставлять — оценивать, измерять или отмечать степень схожести и различия между чем-то и чем-то.

Примечание 2 — Сравнивать «исключено» в качестве синонима «сопоставлять».

В.7.12 **решение сопоставления** (comparison decision): Определение того, имеет ли биометрический образец(ы) и биометрический шаблон(ы) один и тот же источник, основанный на одном или нескольких результатах сопоставления, политика(и) решения, включающая в себя пороговые значения, и, возможно, иные выходные данные.

Примечание 1 — Совпадение является положительным решением сопоставления.

Примечание 2 — Несовпадение является отрицательным решением сопоставления.

Примечание 3 — Также может быть выдано решение «не определено».

В.7.13 **результат сопоставления** (comparison score):

результат сравнения (matching score) — исключено.

Цифровое значение (или ряд значений), являющееся(иеся) результатом сопоставления.

Примечание — Максимальное значение ряда не обязательно обозначает высокую степень схожести.

В.7.14 **результат меры различия / результат несхожести** (distance score/dissimilarity score): Результат сопоставления, уменьшающийся со схожестью.

В.7.15 **ложное совпадение** (false match): Решение о совпадении «совпадение» при распознавании биометрического образца и биометрического эталона, не имеющих общего источника.

В.7.16 **ложное несовпадение** (false non-match): Решение о совпадении «несовпадение» при распознавании биометрического образца и биометрического эталона, имеющих общий источник.

В.7.17 **совпадение** (match): Решение о том, что биометрический образец(ы) для распознавания и биометрический шаблон имеют общий источник.

В.7.18 **степень схожести** (matching score) — исключено (определение не представлено).

Примечание — Данный термин исключен и заменен термином «результат сопоставления».

В.7.19 **отрицательная идентификация** (negative identification) — исключено (определение не представлено).

Примечание 1 — Употребление данного термина исключено во избежание путаницы между биометрической верификацией и биометрической идентификацией.

Примечание 2 — Данный термин употребляется в области биометрии для обозначения запроса биометрической верификации «не является источником какого-либо биометрического шаблона базы данных».

Примечание 3 — Предпочтительное выражение — отрицательный запрос идентификационной информации.

В.7.20 **несовпадение** (non-match): Решение о том, что биометрический образец(ы) для распознавания и биометрический шаблон не имеют общего источника.

В.7.21 **поиск «один-ко-многим»** (one-to-many search):

«один-к-нескольким» (one-to-few) — исключено.

Процесс сопоставления, при котором биометрический образец / биометрический признак / биометрическая модель для распознавания сопоставляются с биометрическим эталоном более чем одной личности, и возвращается ряд результатов сопоставления.

Примечание 1 — Поиск «один-ко-многим» осуществляет биометрическая функция идентификации.

Примечание 2 — В случае с мультимодальной биометрической системой биометрический образец / биометрический признак / биометрическая модель для распознавания и биометрический шаблон в вышеуказанном определении включают в себя индивидуальные биометрические образцы / биометрические признаки / и биометрические шаблоны модальностей элементов.

Примечание 3 — Универсальная фоновая модель не является индивидуальной, поэтому сопоставление биометрического образца субъекта с запрошенным шаблоном и универсальной фоновой моделью по существу не является сопоставлением «один-ко-многим».

Примечание 4 — В случае применения универсальной фоновой модели сопоставление все же может считаться сопоставлением «один-к-одному».

В.7.22 **сопоставление «один-к-одному»** (one-to-one comparison): Процесс, при котором набор биометрических образцов / биометрических признаков / биометрических моделей для распознавания одной личности сопоставляется с одним или несколькими биометрическими эталонами для выдачи результата сопоставления по одной личности, возможно использование дополнительных данных из регистрационной базы данных.

Примечание 1 — Сопоставление «один-к-одному» осуществляет функция биометрической верификации.

Примечание 2 — В случае с мультимодальной биометрической системой биометрический образец / биометрический признак / биометрическая модель для распознавания, биометрический шаблон и, возможно, результат сопоставления в вышеуказанном определении включают в себя компоненты определенной биометрической модальности.

Примечание 3 — В случае коэффициентов вероятности вычисления включают в себя сопоставления, определяющие согласованность наборов биометрических образцов / биометрических признаков / биометрических моделей для распознавания, принадлежащие одной личности с биометрическими шаблонами нескольких личностей. Тем не менее выведенный результат сопоставления относится к степени схожести между наборами биометрических образцов / биометрических признаков / биометрических моделей для распознавания, принадлежащих одной личности, и биометрического шаблона, принадлежащего одной личности, поэтому процесс сопоставления — «один-к-одному».

Примечание 4 — Сопоставление считается сопоставлением «один-к-одному» даже в случае применения универсальной фоновой модели или когортных моделей.

В.7.23 **оценивание схожести** (scoring): Процесс получения результата сопоставления.

В.7.24 **результат оценки схожести** (similarity score): Результат сопоставления, увеличивающийся со схожестью.

В.7.25 **определение порога** (thresholding) / **отбраковывать** (cull) / **исключать** (exclude): Исключение одного или нескольких идентификаторов биометрического эталона, связанных с биометрическим эталоном(ами) и/или идентификаторами биометрического образца(ов), не соответствующих уровню оценки результата.

Примечание — Оценками могут быть оценка качества результата, оценка результата сопоставления.

В.7.26 **проверка соответствия** (validation): Процесс проверки или подтверждения пригодности результата.

Примечание 1 — Данное определение взято из оксфордского словаря и является определением, наиболее четко выражающим общее представление о термине в области биометрии.

Примечание 2 — Пригодный (прил.) — действительно отвечающий предполагаемому смыслу или запросу (оксфордский словарь).

В.7.27 **верифицировать** (verify): Удостовериться или показать, что объект является истинным, точным и обоснованным.

В.8 Термины, связанные с ЕСФОБД

В.8.1 **Организация — участник ЕСФОБД** (CBEFF biometric organization): Организация, зарегистрированная регистрационным органом в области биометрии в соответствии с ИСО/МЭК 19785-2.

Примечание — Организация — участник ЕСФОБД может устанавливать форматы ББД, присваивать им идентификаторы форматов ББД, присваивать биометрическим продуктам идентификаторы биометрических продуктов, устанавливать форматы БЗИ и присваивать им идентификаторы форматов БЗИ. Если организация является ведущей организацией ЕСФОБД, то она также может устанавливать форматы ведущей организации ЕСФОБД и присваивать им идентификаторы форматов ведущей организации ЕСФОБД.

В.8.2 **Ведущая организация ЕСФОБД** (CBEFF patron): Организация, занимающаяся разработкой стандартов (орган по стандартизации, рабочая группа или промышленный консорциумом), зарегистрированная в качестве ведущей организации ЕСФОБД регистрационным органом в соответствии с ИСО/МЭК 19785-2, которая имеет право определять один или несколько форматов ведущей организации ЕСФОБД.

В.8.3 **формат ведущей организации ЕСФОБД** (CBEFF patron format): Формат ЗБИ, установленный ведущей организацией ЕСФОБД.

В.8.4 **полезная информация** (payload):Данные, собранные во время регистрации и относящиеся к контрольному шаблону, которые могут быть выданы после удачной биометрической верификации.

Примечание — Примерами информационного наполнения являются имена пользователей, счета, пароли, криптографические ключи и цифровые идентификаторы.

В.8.5 **блок защиты информации** (security block): Блок данных, имеющий определенный формат и содержащий информацию о шифровании ББД в рамках ЗБИ и механизмах целостности ЗБИ.

В.9 Термины, связанные с БиоАПИ

В.9.1 **присоединенная сессия** (attach session): Временная связь между приложением, отдельным ПБУ и набором модулей, напрямую или косвенно управляемых ПБУ.

В.9.2 **компонент БиоАПИ** (BioAPI component): Компонент архитектуры БиоАПИ с определенным интерфейсом, который может быть предоставлен отдельным изготовителем, используемый при испытании на соответствие.

Примечание — Компоненты БиоАПИ включают в себя приложения БиоАПИ, инфраструктуру БиоАПИ, ПБУ и ПБФ.

В.9.3 **поставщик функции БиоАПИ (ПБФ)** [BioAPI Function Provider (BFP)]: Компонент, управляющий одним или более модулями БиоАПИ определенной категории. Компонент, управляющий одним или более элементами БиоАПИ определенной категории.

Примечание — ПБУ распределены на типы, соответствующие типам модулей БиоАПИ, которыми они управляют.

В.9.4 **модуль БиоАПИ** (BioAPI Unit): Абстракция аппаратного или программного уровня, напрямую управляемая ПБУ или ПБФ.

Примечание — Модули БиоАПИ категоризированы и включают в себя модули сканеров, архива, алгоритмов сравнения и алгоритмов обработки.

В.9.5 **поставщик биометрической услуги (ПБУ)** [Biometric Service Provider (BSP)]: Компонент, осуществляющий для приложения определенные действия с помощью определенного интерфейса путем непосредственного управления одним или несколькими модулями БиоАПИ либо через поставщиков функции БиоАПИ также с помощью определенного интерфейса.

В.9.6 **независимое устройство** (self-contained device): Комбинированное устройство, которое включает в себя биометрический сканер, а так же все или часть функций ПБУ.

Примечание — Независимое устройство может не только захватывать биометрические образцы, но также обрабатывать, сопоставлять и/или хранить их. Данные функции обычно реализованы на аппаратном уровне или на уровне встроенных программных средств.

В.10 Термины, связанные с приложениями

В.10.1 **приложение** (application): Программа или часть программного обеспечения, разработанная для выполнения конкретных задач.

Примечание — Данное словарное определение не препятствует использованию термина «определение» в контексте биометрии, например, биометрические образцы могут быть получены от субъектов во время подачи заявки на получение паспорта или визы.

В.10.2 **идентификация на замкнутом множестве (биометрическое приложение)** [closed-set identification (biometric application)]: Приложение, ранжирующее биометрические шаблоны в базе данных в порядке уменьшения степени их схожести с биометрическим образцом для распознавания.

Примечание 1 — При идентификации на замкнутом множестве всегда возвращается непустой список кандидатов.

Примечание 2 — Идентификации на замкнутом множестве редко используется на практике, но иногда используется в экспериментальных целях.

В.10.3 **идентифицировать** (identify): Акт осуществления ряда сопоставлений с регистрационной базой данных с целью найти и вывести один или более идентификатор биометрического шаблона.

В.10.4 **идентификация на открытом множестве (биометрическое приложение)** [open-set identification (biometric application)]: Приложение, определяющее возможный пустой список кандидатов посредством получения одного или более биометрических образцов от личности и поиска схожих биометрических шаблонов в регистрационной базе данных.

Примечание — Биометрические шаблоны могут быть признаны схожими (похожими) на основе результата сопоставления.

В.11 Термины, связанные с эксплуатацией

В.11.1 **вероятность отказа регистрации** (failure-to-acquire rate): Доля выборки, для которой система не может завершить процесс регистрации.

В.11.2 **вероятность отказа сбора данных** (failure-to-enrol rate): Доля попыток верификации или идентификации, для которых система не может получить или отобрать изображение или сигнал удовлетворительного качества.

В.11.3 **вероятность ложного допуска; ВЛД** (false acceptance rate; FAR): Доля транзакций верификации «самозванца», которые будут ошибочно приняты.

Примечание — В приложениях, в которых требуется верификация положительных запросов, ВЛД обусловлен вероятностью ложного совпадения и политикой системы, определяющими необходимое количество попыток подтверждения предъявляемой идентификационной информации. В системах отрицательной идентификации ВЛД может включать в себя вероятность отказа сбора данных и вероятность ложного несовпадения.

В.11.4 **вероятность ложного совпадения; ВЛС** (false match rate; FMR): Доля образцов, захваченных в результате пассивных попыток «самозванца», которые ошибочно признаны совпадающими с шаблоном другого пользователя.

В.11.5 **вероятность ложного несовпадения; ВЛНС** (false non-match rate; FNMR): Доля образцов, захваченных в результате попыток подлинного лица, которые ошибочно признаны не совпадающими с шаблоном той же биометрической характеристики данного пользователя, представившего образец.

В.11.6 **вероятность ложного недопуска; ВЛНД** (false rejection rate; FRR): Доля транзакций верификации подлинного лица, которые будут ошибочно отвергнуты.

Примечание — В системах положительной идентификации ВЛНД может включать в себя как вероятность отказа регистрации и вероятность отказа сбора данных, так и вероятность ложного несовпадения.

Библиография

[1] Alderman, E. and Kennedy, C. (1995). The Right to Privacy. New York: Vintage

[2] Baker, L.R., (2000). Persons and Bodies: A Constitution View Cambridge: Cambridge University Press

[3] Beavan, C. (2001). Fingerprints New York: Hyperion

[4] Biometric Systems Lab University of Bologna, Pattern Recognition and Image Processing Laboratory, Michigan State University, Biometric Test Center San Jose State University (2000 — 2006). Fingerprint Verification Competition (FVC). Available at gost.e-ecolog.ru (Date of access:15 Nov 2006)

[5] Blackburn, D., Bone, M., Grother, P., and Phillips, P.J. (2001). Facial Recognition Vendor Test 2000: Evaluation Report, Available at gost.e-ecolog.ru Date of access: 15 Nov 2006)

[6] Bledsoe, W.W. (1966). Man-machine Facial Recognition: Report on a Large-scale Experiment, Panoramic Research, Inc, Palo Alto, CA.

[7] Bouchier, F., Ahrens, J. and Wells, G. (1996). Laboratory Evaluation of the IriScan Prototype Biometric Identifier, Available on-line at gost.e-ecolog.ru (Date of access: 15 Nov 2006)

[8] BSI Germany (2003) BioP I

[9] BSI Germany (2005) BioP II

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

[11] Cole, S. (2001). Suspect Identities, Cambridge: Harvard University Press

[12] Daugman, J. (1993). High confidence visual recognition of persons by a test of statistical independence, Trans. on Pattern Analysis and Machine Intelligence 15, 1148—1161 Available on-line at gost.e-ecolog.ru jgd10-00/PAMI93.pdf. (Date of access: 15 Nov 2006)

[13] Faulds, H. (1880). On the Skin Furrows of the Hand, Nature, 22, 605 Available on-line at gost.e-ecolog.ru library/100101.html (Date of access: 15 Nov 2006) Fejfar, A. and Myers, J.W. (1977). The testing of three automatic identity verification techniques, Proc. International Conference On Crime Countermeasures, Oxford

[14] Fejfar, A. (1978). Combining Techniques to Improve Security in Automated Entry Control, Carnahan Conference On Crime Countermeasures

[15] Flom, L. and Safir, A. (1987). Iris recognition system, U.S. Patent 4, 641, 349

[16] Galton, F. (1888). On Personal Identification and Description, Nature 21/28, 201—202 Available on-line at gost.e-ecolog.ru (Date of access: 15 Nov 2006)

[17] Goldstein, A.J., Harmon, L.D. and Lesk, A.B. (1971). Identification of Human Faces, Proc. Institute of Electrical and Electronic Engineers, 59, 748—760

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

[19] IBM (1970). The Considerations of Data Security in a Computer Environment, Report G 520—2169, White Plains, NY.

[20] International Biometric Group (2005). Independent Testing of Iris Recognition Technology. Available on-line at gost.e-ecolog.ru (Date of access: 15 Nov 2006)

[21] Kent, S.T. and Millett, L.I. (2003). Who Goes There? Authentication Through the Lens of Privacy, Washington, D.C.: National Academies Press Available on-line at gost.e-ecolog.ru (Date of access: 15 Nov 2006)

[22] Locke, J. (1690). An Essay Concerning Human Understanding, Book 2, Chapter 27, Available on-line at http:// gost.e-ecolog.ru (Date of access: 15 Nov 2006)

[23] Lummis, R.C., and Rosenberg, A. (1972). Test of an ASV method with intensively trained professionalmimics, Journal of the Acoustical. Society of America 51, 131

[24] Mansfield, A.J. and Wayman, J.L. (2002). Best Practices for Testing and Reporting Biometric Device Performance, Issue 2.0, U.K. Biometrics Working Group, Available on-line at gost.e-ecolog.ru BestPractice.pdf. (Date of access: 15 Nov 2006)

[25] Mansfield, A.J., Kelly, G., Chandler, D. and Kane, J. (2000). Biometric product testing final report. Available on-line at gost.e-ecolog.ru (Date of access: 15 Nov 2006)

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

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

[28] National Bureau of Standards (1977). Guidelines for Evaluation of Techniques for Automated Personal Identification, Federal Information Processing Standard Publication

[29] National Institute of Standards and Technology (1996—2006). Speaker Recognition Evaluation. Available on-line at gost.e-ecolog.ru (Date of access: 15 Nov 2006)

[30] National Institute of Standards and Technology (1993—1997). Facial Recognition Technology (FERET) Database Evaluation. Available on-line at gost.e-ecolog.ru (Date of access: 15 Nov 2006)

[31] National Institute of Standards and Technology (2003). Fingerprint Vendor Technology Evaluation (FpVTE). Available on-line at gost.e-ecolog.ru (Date of access: 15 Nov 2006)
[32] National Institute of Standards and Technology (2000—2006). Face Recognition Vendor Test (FVT). Available on-line at gost.e-ecolog.ru . (Date of access: 15 Nov 2006)
[33] National Institute of Standards and Technology (2004—2006). Fingerprint Software Development Kit Testing. Available on-line at gost.e-ecolog.ru . (Date of access: 15 Nov 2006)
[34] National Institute of Standards and Technology (2004—2006). Performance and Interoperability of the INCITS 378 Fingerprint Template. Available online at gost.e-ecolog.ru . (Date of access: 15 Nov 2006)
[35] National Institute of Standards and Technology (2005—2006). Iris Challenge Evaluation. Available on-line at gost.e-ecolog.ru)ate of access: 15 Nov 2006)
[36] Osborn, S. (1929). Questioned Documents, Chicago: Nelson-Hall
[37] Phillips, P.J., Martin, A., Wilson, C.L. and Przybocki, M. (2000). An introduction to evaluating biometric systems, Computer, 33, 56—63, Available online at gost.e-ecolog.ru . (Date of access: 15 Nov 2006)
[38] Potter, R.K., Kopp, G.A., and Green, H.C. (1947). Visible Speech, New York: van Nostran Co.
[39] Pruzansky, S. (1963). Pattern-matching procedure for automatic talker recognition, Journal of the Acoustical Society of America, 26, 403—406
[40] Raphael, D.E. and Young, J.R. (1974). Automated Personal Identification, Palo Alto: SRI, International
[41] Rodriguez, J.R., Bouchier, F., and Ruehie, M. (1993). Performance Evaluation of Biometric Identification Devices, Sandia National Laboratory Report SAND 93—1930, Albuquerque
[42] Roethenbaugh, G. (Ed) (1998). Biometrics Explained. ICSA Commercial Biometric Developers Consortium. NOTE Parts of this tutorial are based, with permission, on text in this publication
[43] Seildarz, J. (1998). Letter to the Editor, Philadelphia Inquirer April 6
[44] Simon, C. and Goldstein, I. (1935). A New Scientific Method of Identification, New York State Journal of Medicine, 35, 901—906
[45] Thalheim, L., Krissler, J. and Ziegler, P. (2002). Biometric Access Protection Devices and their Programs Put to the Test, C'T Magazine 11, Available on-line at gost.e-ecolog.ru . (Date of access 15 Nov 2006)
Trauring, M. (1963a). On the automatic comparison of finger ridge patterns, Nature, 197, 938—940
[46] Trauring, M. (1963). Automatic comparison of finger ridge patterns, Hughes Research Laboratory Report , 190, Malibu
[47] Twain, M. (1893). Pudd'nhead Wilson, The Century, serialized 47(2) — 48(2), New York: The Century Company
[48] van der Putte, T. and 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. See gost.e-ecolog.ru . (Date of access: 15 Nov 2006)
[49] Warren, S. and Brandeis, L. (1890). The Right of Privacy, Harvard Law Review, 4, (193) Available on-line at http://gost.e-ecolog.ru . (Date of access: 15 Nov 2006)
[50] Watson, C.I. and Wilson, C.L (2005). Effect of Image Size and Compression on One-to-One Fingerprint Matching. NISTIR 7201, Feb. 2005, available on-line at ftp://sequoyah.nist.gov/pub/nist_internal_reports/ir_7201.pdf. (Date of access: 15 Nov 2006)
[51] Wayman, J.L. (2000). Evaluation of the INSPASS Hand Geometry Data. In J.L. Wayman (Ed.), U.S. National Biometric Test Center Collected Works: 1997—2000, San Jose: San Jose State University
[52] Wegstein, J. (1970). Automated Fingerprint Identification, National Bureau of Standards, Technical Note, 538
[53] Westin, A. (1967). Privacy and Freedom, Boston: Atheneum

УДК 004.93'1:006.89 ОКС 35.040 П85

Ключевые слова: биометрия, обучающая программа

Редактор *В. Н. Копысов*
Технический редактор *В. Н. Прусакова*
Корректор *С. И. Фирсова*
Компьютерная верстка *Т. Ф. Кузнецовой*

Сдано в набор 06.11.2012. Подписано в печать 13.12.2012. Формат 60×84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 6,51. Уч.-изд. л. 6,15. Тираж 93 экз. Зак. 1716.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru
Набрано и отпечатано в Калужской типографии стандартов, 248021 Калуга, ул. Московская, 256.

gost.e-ecolog.ru