



ПРЕДВАРИТЕЛЬНЫЙ
НАЦИОНАЛЬНЫЙ
СТАНДАРТ
РОССИЙСКОЙ
ФЕДЕРАЦИИ

ПНСТ
875—
2023
(ИСО/МЭК
24714:2023)

Информационные технологии

БИОМЕТРИЯ

Социальные аспекты
применения биометрических технологий.
Общие положения

(ISO/IEC 24714:2023, Biometrics — Cross-jurisdictional
and societal aspects of biometrics — General guidance, MOD)

Издание официальное

Москва
Российский институт стандартизации
2023

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным бюджетным образовательным учреждением высшего образования «МИРЭА — Российский технологический университет» (РТУ МИРЭА) и Некоммерческим партнерством «Русское общество содействия развитию биометрических технологий, систем и коммуникаций» (Некоммерческое партнерство «Русское биометрическое общество») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 27 ноября 2023 г. № 69-пнст

4 Настоящий стандарт является модифицированным по отношению к международному стандарту ИСО/МЭК 24714:2023 «Биометрия. Межюрисдикционные и социальные аспекты применения биометрии. Общее руководство» (ISO/IEC 24714:2023 «Biometrics — Cross-jurisdictional and societal aspects of biometrics — General guidance», MOD) путем изменения отдельных фраз (слов, значений показателей, ссылок), которые выделены в тексте курсивом, а также путем изменения его структуры для приведения в соответствие с правилами, установленными в ГОСТ 1.5—2001 (подразделы 4.2 и 4.3). Внесение указанных технических отклонений направлено на учет потребностей национальной экономики Российской Федерации.

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

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

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

5 Некоторые элементы настоящего стандарта могут быть объектами патентных прав. Федеральное агентство по техническому регулированию и метрологии не несет ответственности за установление подлинности каких-либо или всех таких патентных прав

Правила применения настоящего стандарта и проведения его мониторинга установлены в ГОСТ Р 1.16—2011 (разделы 5 и 6).

Федеральное агентство по техническому регулированию и метрологии собирает сведения о практическом применении настоящего стандарта. Данные сведения, а также замечания и предложения по содержанию стандарта можно направить не позднее чем за 4 мес до истечения срока его действия разработчику настоящего стандарта по адресу: 107045 Москва, Сретенский тупик, д. 3, стр.1 и/или в Федеральное агентство по техническому регулированию и метрологии по адресу: 123112 Москва, Пресненская набережная, д. 10, стр. 2.

В случае отмены настоящего стандарта соответствующая информация будет опубликована в ежемесячном информационном указателе «Национальные стандарты» и также будет размещена на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.rst.gov.ru)

© ISO, 2023

© IEC, 2023

© Оформление. ФГБУ «Институт стандартизации», 2023

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

II

Содержание

1 Область применения 1

2 Нормативные ссылки 1

3 Термины и определения 2

4 Сокращения 2

5 Межюрисдикционные и социальные аспекты 2

Приложение ДА (справочное) Сведения о соответствии ссылочных национальных стандартов
международным стандартам, использованным в качестве ссылочных
в примененном международном стандарте. 15

Приложение ДБ (справочное) Сопоставление структуры настоящего стандарта со структурой
примененного в нем международного стандарта 16

Введение

Настоящий стандарт представляет собой руководство по проектированию биометрических систем в отношении:

- социальных норм;
- приватности/защиты данных идентифицируемого;
- доступа человека к системе и использованию информации в ней;
- вопросов безопасности человека при сборе биометрических персональных данных.

Следование рекомендациям настоящего стандарта обеспечивает следующие преимущества:

- благоприятное отношение субъектов персональных данных к биометрическим технологиям;
- улучшенное общественное восприятие и понимание биометрических технологий;
- беспрепятственное внедрение и эксплуатация биометрических систем;
- потенциальное долгосрочное снижение затрат в течение всего срока эксплуатации;
- использование общепринятой передовой практики обеспечения приватности;
- повышение осведомленности в вопросах доступности.

Настоящий стандарт предназначен для использования:

- пользователями, использующими результаты биометрических систем;
- разработчиками технических стандартов;
- субъектами персональных данных;
- разработчиками системных спецификаций, системными архитекторами и ИТ-проектировщиками;
- представителями органов законодательной власти.

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

БИОМЕТРИЯ

Социальные аспекты применения биометрических технологий.
Общие положения

Information technology. Biometrics. Social aspects of the application of biometric technologies.
General provisions

Срок действия — с 2024—01—01
до 2027—01—01

1 Область применения

Настоящий стандарт содержит рекомендации для следующих этапов жизненного цикла биометрических систем и связанных с ними элементов системы, включая:

- сбор и разработку требований;
- разработку и внедрение;
- эксплуатацию, включая регистрацию и последующее использование;
- взаимосвязи с другими системами;
- хранение данных и их безопасность;
- обновление и ведение данных;
- обучение и осведомленность;
- оценка системы и аудит;
- контролируемое завершение работы системы.

Внедрение биометрии ограничивается следующими факторами:

- правовые и социальные ограничения на использование биометрических персональных данных;
- доступность для значительной части населения;
- здоровье и безопасность пользователей в отношении прямых потенциальных опасностей, а также вероятность ненадлежащего использования биометрических персональных данных.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

ГОСТ Р 58273 (ИСО/МЭК 29197:2015) Информационные технологии. Биометрия. Методология испытаний эксплуатационных характеристик биометрической системы на воздействие условий окружающей среды

ГОСТ Р 58624.1 Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 1. Структура

ГОСТ Р 58624.2 Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 2. Форматы данных

ГОСТ Р 58624.3 Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 3. Испытания и протоколы испытаний

ГОСТ Р ИСО/МЭК 27002 Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности

ГОСТ Р ИСО/МЭК 27017 Информационные технологии. Методы и средства обеспечения безопасности. Правила применения мер обеспечения информационной безопасности на основе ИСО/МЭК 27002 при использовании облачных служб

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

3 Термины и определения

В настоящем стандарте применены термины по *ГОСТ ISO/IEC 2382-37*, а также следующие термины с соответствующими определениями:

3.1

доступность (accessibility): Свойство продукции, систем, сред или оборудования, при наличии которого они могут быть использованы людьми с самым широким диапазоном возможностей для достижения установленных целей в определенных условиях использования.

Примечание — Условия использования включают прямое использование или использование с помощью вспомогательных технологий.

[ГОСТ Р 55241.1—2012, пункт 2.7]

3.2 расползание функций (function creep): Расширение функций системы за пределы их первоначальных целей в результате преднамеренного или непреднамеренного изменения, которые происходят в виде небольших последовательных этапов и могут привести к значительным изменениям.

3.3

удобство использования (usability): Степень, в которой система, продукт или услуга могут использоваться указанными пользователями для достижения определенных целей с эффективностью, результативностью и удовлетворенностью в определенном контексте использования.

[Адаптировано из ГОСТ Р ИСО/МЭК 25066—2019, пункт 3.16]

4 Сокращения

В настоящем стандарте применены следующие сокращения:

ИКТ — информационно-коммуникационные технологии;

ПИН — персональный идентификационный номер;

РЕТ — технология повышения приватности (privacy enhancing technology).

5 Межюрисдикционные и социальные аспекты

5.1 Общие положения

Настоящий стандарт содержит общие рекомендации, которые не относятся к определенным технологиям или приложениям. Настоящий раздел определяет принципы, рекомендации и факторы разработки и внедрения биометрических приложений в отношении:

- межюрисдикционных аспектов, связанных с приватностью и защитой биометрических персональных данных (см. 5.2);
- доступности (см. 5.3);
- проверки вопросов здоровья и безопасности при использовании биометрических приложений при проектировании и реализации (см. 5.4);
- удобства использования и физических условий окружающей среды, которые могут повлиять на работу и удобство использования биометрического приложения (см. 5.5);
- социальных, культурных и этических аспектов биометрии (см. 5.6);
- приемлемости использования биометрических приложений (см. 5.7).

5.2 Межюрисдикционные вопросы

5.2.1 Общие положения

Разработчик биометрического приложения должен учитывать аспекты, связанные с конкретными юрисдикционными требованиями. Часть аспектов рассмотрена в следующих пунктах. Часть аспектов выходит за рамки настоящего стандарта, включая:

- антидискриминационные законы;
- законы о раскрытии информации;
- механизмы возмещения ущерба;
- договорные вопросы;
- предоставление биометрических персональных данных сторонам, не являющимся их владельцем;
- доступ правоохранительных органов к биометрической и сопутствующей информации;
- права согласия и отказа и связанные с ними требования для резервных процессов;
- условия хранения данных, включая период времени и стандарты безопасности;
- требования к доказательствам для использования биометрических персональных данных в суде;
- особые сценарии использования биометрических персональных данных (например, безопасный доступ к военным объектам и объектам критической инфраструктуры);
- применимость использования биометрии в Интернете с юридической точки зрения;
- законы о пограничном контроле.

5.2.2 Аспекты приватности биометрических приложений

С распространением биометрических приложений аспект приватности приобретает все большее значение. В зависимости от того, как развернута система, биометрическая технология может поставить под угрозу или защитить приватность субъекта персональных данных. Необходимость и возможность защиты особенно актуальна в связи со свойствами биометрических персональных данных, которые однозначно привязаны к субъекту персональных данных на всю жизнь, в отличие от ПИН-кодов и паролей, косвенно и слабо связанных с человеком. Таким образом, биометрия является как объектом, так и инструментом в аспекте приватности.

Рекомендуется применить для биометрических персональных данных технологию PET. PET — это согласованная система мер ИКТ для защиты приватности путем удаления или сокращения персональных данных и для предотвращения несанкционированной, ненужной и/или нежелательной обработки персональных данных без потери функциональности системы данных.

Примечание — Несанкционированная, ненужная и нежелательная обработка может включать в себя такие операции с персональными данными, как сбор, запись, организация, хранение, адаптация, изменение, поиск, консультация, использование, раскрытие путем передачи, распространения или иного предоставления, совмещение, объединение, блокирование, стирание или уничтожение.

PET применяется к биометрии с двух точек зрения:

- в качестве объекта. Внедрение и применение биометрии должно следовать полному и корректному режиму приватности для повышения приватности;
- в качестве инструмента. Биометрия сама по себе может быть методом повышения приватности.

Общие правила PET включают (но не ограничиваются перечисленным) следующее:

- не использовать персональные данные или использовать их по мере необходимости;
- использовать шифрование при использовании персональных данных;
- удалять исходные данные в максимально короткие сроки;

- анонимизировать персональные данные по возможности;
- не использовать центральные базы данных там, где это не требуется;
- предоставлять субъектам персональных данных контроль над их персональными данными;
- использовать средства оценки и сертификации для подтверждения уровня доверия приложения.

Приватность — одна из наиболее важных задач организации, собирающей персональные данные. Следует уделить внимание вопросу совместного доступа к информации и многократному использованию биометрических баз данных. При этом во многих заявлениях о приватности не учитываются нюансы развертываний биометрических баз данных. Некоторые типы биометрических персональных данных вызывают большее вторжение в частную жизнь, в то время как другие типы мало влияют на проблемы приватности. Персональные данные являются первым этапом идентификации личности, и именно на этом этапе происходит много преступлений против личности. Следует отметить, что несмотря на риски предоставления биометрических персональных данных, идентификация будет проведена с помощью других документов, удостоверяющих личность, таких как свидетельство о рождении или паспорт. Поэтому большая часть людей может считать биометрические методы менее инвазивными, чем задавание вопросов, иногда лицом к лицу, касающихся их личной жизни, подробностей проживания и информации о других членах их семьи.

Активное внедрение биометрических технологий поднимает вопросы о влиянии технологии на приватность в широко используемых приложениях в общем доступе, на рабочем месте и дома. Ключевые аспекты вопросов приватности относятся либо к субъекту персональных данных, либо к организации. С точки зрения субъекта персональных данных вопросы связаны со сбором, выбором, использованием и безопасностью информации, а также с анонимностью. С организационной точки зрения вопросы связаны со способом и целью сбора, запросом, хранением и защитой информации, доступом к записям, релевантностью данных, ограничением на использование и раскрытие собранных данных.

Следует учесть такие вопросы приватности, как стереотипы и репутационный или финансовый ущерб. Примером стереотипа является связь отпечатков пальцев с преступной деятельностью, хотя в настоящее время снятие отпечатков пальцев ассоциируется с идентификацией законопослушного гражданина как владельца электронного удостоверения личности, держателя карты или члена клуба. Данные вопросы могут осложняться возможностью подделки биометрических персональных данных человека.

Другие вопросы приватности связаны с расползанием функций, ненадлежащим использованием информации, отслеживанием или объединением данных. При расползании функций использование данных для вторичных целей может быть целесообразным, но могут возникнуть социально-культурные и юридические проблемы, когда люди не информируются и не дают своего согласия на использование их данных для вторичной цели. Отслеживание данных является формой расползания функций, когда биометрические персональные данные используются в сочетании с дополнительными данными, например сведениями о расходах или поездках. Скрытое использование биометрических персональных данных без законного разрешения нарушит приватность.

Также следует принимать во внимание ряд других вопросов, в том числе:

- увязку биометрических персональных данных с другой информацией;
- переходные состояния:
 - достижение совершеннолетия,
 - изменение умственных способностей (например, болезнь Альцгеймера),
 - смерть субъекта персональных данных,
 - процедуры отзыва;
- уведомление анонимно зарегистрированных субъектов персональных данных о любых изменениях в использовании биометрических персональных данных.

К планированию и реализации биометрических приложений следует привлекать специалистов по защите биометрических персональных данных, а также разработать и внедрить политику приватности биометрических персональных данных.

5.2.3 Принципы приватности для биометрических приложений

Существует ряд ключевых принципов приватности, которые следует учитывать при внедрении биометрических приложений:

- а) прозрачность. Должна быть обеспечена политика открытости использования биометрических персональных данных, которая включает цели использования данных и указывает ответственное лицо. Любые изменения должны быть известны субъектам персональных данных;

б) согласие. Биометрические данные должны собираться, храниться, использоваться, раскрываться и сохраняться с ведома и согласия субъекта персональных данных, за исключением случаев, когда законодательство предусматривает исключения из этого принципа;

в) участие субъекта персональных данных. Там, где это возможно и целесообразно, субъекту персональных данных должны быть доступны процедуры отказа или согласия;

г) ограничение цели. Цели биометрического приложения должны быть доступны субъектам персональных данных для ознакомления до использования приложения. Обработка биометрических персональных данных должна ограничиваться заявленными целями;

д) ограничение сбора. Сбор биометрических персональных данных должен быть минимальным и достаточным для достижения заявленных целей;

е) ограничение срока хранения. Биометрические персональные данные должны храниться только в течение периода времени, необходимого для заявленных целей. Должны быть определены процедуры безопасного удаления данных, срок хранения которых истек;

ж) соблюдение критериев эффективности. Системный оператор должен обеспечить правильную конфигурацию, функционирование и стабильность биометрического приложения в соответствии с его спецификацией. Работа или сбой системы не должен приводить к несанкционированному доступу, использованию, изменению и раскрытию биометрических персональных данных;

и) права доступа субъекта персональных данных. Субъекту персональных данных должен быть предоставлен соответствующий доступ для проверки правильности биометрических персональных данных и внесения поправок в неверные данные;

к) защита данных. Биометрические приложения должны быть разработаны таким образом, чтобы биометрические персональные данные, в том числе в резервных копиях или архивах, были защищены от несанкционированного доступа, использования, изменения, удаления, раскрытия и хранения;

л) аудит безопасности. Биометрическое приложение должно быть разработано таким образом, чтобы обеспечивать аудит безопасности использования биометрических персональных данных, в том числе их удаления или уничтожения (см. *ГОСТ Р ИСО/МЭК 27017*);

м) передача данных между различными юрисдикциями. Системный оператор должен обеспечить надлежащую защиту биометрических персональных данных, раскрываемых сторонней стороне;

н) автоматические решения. Должен быть предусмотрен механизм вмешательства оператора в случае, если биометрические приложения используются для принятия автоматических решений. Субъекты персональных данных должны быть уведомлены о таких автоматических решениях;

п) подотчетность. Должно быть определено лицо, ответственное за соблюдение законодательства;

р) точность биометрических персональных данных. Биометрическая информация должна быть точной, полной и актуальной настолько, насколько это необходимо для заявленных целей;

с) анонимизация данных. Следует анализировать и контролировать раскрытие биометрических персональных данных для образовательных, статистических или испытательных целей. Ссылки на иную персональную информацию должны быть удалены, если они могут привести к идентификации субъекта персональных данных;

т) встроенная приватность. Следует учитывать приватность на начальных этапах проектирования и на протяжении всего процесса разработки новых продуктов, процессов или услуг, связанных с обработкой биометрических персональных данных;

у) приватность по умолчанию. При наличии выбора способа предоставления персональных данных настройки по умолчанию должны быть наиболее безопасными для приватности.

5.2.4 Дополнительные правовые аспекты

5.2.4.1 Общие положения

В настоящем пункте представлены правовые аспекты помимо тех, которые связаны с приватностью.

5.2.4.2 Электронные транзакции

Биометрические данные могут быть использованы для сценариев электронных транзакций, автономно или в сочетании с ПИН-кодом или паролем. При использовании нескольких факторов аутентификация является многофакторной. В качестве факторов может выступать то, чем обладает субъект, то, кем он является, или то, что он знает, в любой комбинации. Для большинства приложений достаточно двух факторов. В указанном контексте биометрические персональные данные в сочетании с токеном безопасности или учетными данными могут быть рассмотрены как эквивалент рукописной подписи.

При использовании биометрических персональных данных для сценария электронных транзакций следует обеспечить надежную безопасность и журнал аудита (см. ГОСТ Р ИСО/МЭК 27002).

5.2.4.3 Степень уверенности в безопасности биометрического приложения

Следует учитывать, что распознавание выборки биометрических персональных данных редко обеспечивает идеальное совпадение характеристик в практических приложениях. Это контрастирует с ПИН-кодом или паролем, где совпадение на сто процентов истинно или ложно, но существует риск того, что ПИН-код или пароль могли быть использованы тем, кто не имеет права его использовать.

Система, защищенная биометрическими персональными данными, подвержена тем же нарушениям безопасности, что и система, защищенная ПИН-кодом или паролем.

5.2.4.4 Ответственность при снижении производительности

Биометрические приложения подвержены снижению производительности в результате технических сбоев, преднамеренного или случайного поведения пользователя, в том числе оператора и субъекта персональных данных, или устаревших биометрических образцов. Неспособность защитить биометрические данные может повлечь за собой ответственность.

5.2.4.5 Принцип недискриминации

Во избежание дискриминации лиц, которые не могут использовать конкретное биометрическое приложение ввиду невозможности предоставить требуемую физическую или поведенческую информацию, следует предусмотреть альтернативные методы проверки личности. Примерами невозможности предъявить физическую или поведенческую информацию является отсутствие пальцев, неспособность говорить или неспособность контролировать движение глаз.

5.2.4.6 Подделка или кража биометрических персональных данных

Следует обеспечить технические меры для предотвращения подделки биометрических данных, например проверку витальности предоставляемых биометрических персональных данных. Системы должны проводить проверку того, что биометрический образец предоставлен физическим лицом, и иметь меры противодействия к атакам воспроизведения или повторного представления биометрического образца. Данные меры позволяют снизить опасения субъектов персональных данных по поводу кражи биометрических персональных данных.

Атаки на биометрическое предъявление подробно рассмотрены в серии национальных стандартов ГОСТ Р 58624.1 — ГОСТ Р 58624.3.

5.3 Доступность для людей с ограниченными возможностями

5.3.1 Общие положения

Биометрическое приложение должно быть доступным для всех субъектов персональных данных. Доступность биометрического приложения зависит от особенностей субъектов персональных данных, использующих биометрическую систему, и от удобства ее использования, включая физическую среду. Для субъектов персональных данных, которые не могут использовать биометрическую систему ввиду постоянных или временных условий, должны быть предусмотрены альтернативные системы.

При проектировании доступных биометрических систем необходимо предусмотреть:

- беспристрастное использование для субъектов персональных данных;
- инклюзивный процесс для субъектов персональных данных с физическими или психологическими ограничениями;
- гибкость в использовании;
- простое и интуитивно понятное использование;
- доступность для понимания с соответствующими дополнительными подсказками;
- использование однозначно интерпретируемых условных обозначений;
- низкая чувствительность к ошибкам;
- необходимость небольших физических усилий при использовании;
- размер и пространство, обеспечивающие удобный доступ и использование;
- использование тактильных, звуковых и визуальных подсказок в пользовательском интерфейсе.

Трудности с доступом могут быть долгосрочными, временными и/или могут возникать без предупреждения, например, в результате острого заболевания, такого как ларингит или боль в горле, стоматологической или глазной хирургии или других физических травм.

Группы субъектов могут быть внутренними или внешними по отношению к организации, реализующей биометрическую систему, или могут быть комбинацией того и другого. Следует определить всех заинтересованных лиц, возможное реагирование групп субъектов на технологию, а также потенциаль-

ные проблемы и решения до внедрения программы. Человеческий фактор касается не только субъекта персональных данных, но также специалистов по внедрению биометрической системы, проектировщиков, техников и специалистов по биометрии, которые могут быть подвержены систематическим ограничениям и ошибкам.

Рекомендуется обеспечить доступность для людей с ограниченными возможностями на основе анализа затрат и выгод таким образом, чтобы снизить необходимость обработки исключений и влияние на других пользователей (операторов и субъектов персональных данных).

Примеры ограниченных возможностей субъектов персональных данных приведены далее. Некоторые из этих состояний могут быть временными. Субъект персональных данных может иметь сочетание нарушений, что усилит влияние отдельных нарушений в результате кумулятивного эффекта. Примеры:

а) отсутствие частей тела, необходимых для корректной работы биометрической системы;

Пример — Отсутствие указательного пальца (пальцев) у субъекта персональных данных в системе контроля и управления доступом с использованием указательных пальцев.

б) отсутствие поведенческих признаков, необходимых для корректной работы биометрической системы;

Пример — Отсутствие способности говорить у субъекта персональных данных в системе контроля и управления доступом с голосовым управлением.

в) невозможность использовать части тела, необходимых для корректной работы биометрической системы;

Пример — Крайняя форма артрита у субъекта персональных данных в биометрической системе, использующей геометрию руки на плоской поверхности.

г) невозможность использовать поведенческие особенности, необходимые для корректной работы биометрической системы;

Пример — Система распознавания динамики подписи, разработанная для латинского алфавита, в стране с системой письма, основанной на нелатинском алфавите.

д) неспособность представить требуемую биометрическую модальность в последовательной и предсказуемой форме в конкретных условиях эксплуатации.

Примеры

1 Неконтролируемое движение глазного яблока у субъекта персональных данных в системе распознавания личности по радужной оболочке глаза.

2 Дефект речи (например, заикание) у субъекта персональных данных в системе распознавания диктора по речи.

е) ускоренное изменение физической или поведенческой характеристики в течение определенного периода времени, усложняющее соответствие критериям сравнения для биометрической идентификации или биометрической верификации;

Пример — Субъект персональных данных в состоянии, при котором быстро состарились черты лица, в системе распознавания личности по изображению лица.

ж) невозможность доступа или трудности с физическим доступом к устройству сбора данных или пользовательскому терминалу.

Примеры

1 Субъект персональных данных в инвалидной коляске.

2 Субъект персональных данных, рост которого недостаточен для доступа к устройству сбора данных или пользовательскому терминалу, закрепленному на определенной высоте.

и) неспособность читать ввиду неграмотности, понимать инструкции или вспоминать корректные процедуры для успешной работы с биометрическим приложением;

Пример — Забывание того, какой именно палец был зарегистрирован в автоматической системе контроля и управления доступом, и блокировка после трех попыток.

к) психологические состояния субъекта персональных данных, препятствующие корректному использованию биометрических приложений;

Пример — Обсессивно-компульсивное расстройство у субъекта персональных данных, от которого требуется использовать устройства сбора данных или клавиатуру с физическим контактом.

л) состояния, подобные перечисленным выше и приводящие к несоразмерному использованию ресурсов;

Пример — Пожилые люди, которым требуется более длительный период адаптации к изменению контекста, в ситуации превышения условного времени для аутентификации.

м) невозможность сбора биометрических персональных данных у детей или лиц с отсутствием данных «стандартного» размера.

Пример — Невозможность использования ребенком считывателя геометрии руки из-за положения или размера устройства сбора данных.

Помимо сценариев, когда субъект персональных данных не может использовать биометрическую систему, вероятен сценарий, когда субъект персональных данных отказывается от применения биометрических персональных данных. Системный оператор и/или разработчик может рассмотреть возможность предоставления такого сценария, что может повлиять на преимущества использования и функциональность метода аутентификации.

В некоторых сценариях проблемы могут быть частично устранены путем изменения окружающих условий (например, установка устройств сбора данных с регулируемой высотой или оптимизация условий освещения). Также следует рассмотреть модификацию конструкции биометрической системы.

Разработка доступных биометрических приложений зависит от учета ряда факторов, в том числе:

- является ли использование биометрической системы добровольным или обязательным;
- последствия неблагоприятного результата или ошибки распознавания для субъекта персональных данных (например, личная безопасность, финансовые последствия, социальная изоляция, смущение или изменение качества жизни);
- вероятная демография целевой группы.

5.3.2 Принципы доступности

Следует использовать следующие принципы доступности:

а) инклюзивный дизайн. Биометрические приложения должны быть разработаны таким образом, чтобы максимально возможное количество субъектов целевой группы могло использовать биометрическую систему эффективно и с минимальным дискомфортом. Информационные сообщения могут предоставляться более чем в одной форме, например в визуальной и звуковой;

б) раннее рассмотрение потребностей людей с ограниченными возможностями. При разработке новых биометрических систем или услуг потребности людей с ограниченными возможностями должны учитываться с начала проектирования;

в) испытания. Перед внедрением следует провести испытания биометрической системы на субъектах персональных данных с максимально широким диапазоном возможностей (в отношении зрительных, слуховых, физических, когнитивных и поведенческих возможностей);

г) обучение. Субъектам с ограниченными возможностями следует предложить обучение для повышения эффективности использования биометрической системы;

д) выбор. Рекомендуются обеспечить субъекту персональных данных выбор биометрических приложений для использования, если его ограниченные возможности не позволяют ему использовать конкретную биометрическую технологию;

е) альтернативный метод. Если выбор различных биометрических технологий недоступен, а ограниченные возможности не позволяют субъекту персональных данных использовать конкретную биометрическую технологию, то следует предусмотреть альтернативный метод. По возможности использование альтернативного метода не должно приводить к снижению уровня обслуживания или функциональности по отношению к субъекту персональных данных;

ж) повторная регистрация. При невозможности дальнейшего использования биометрической системы рекомендуется повторить процесс регистрации субъекта персональных данных для обновления данных;

и) обучение персонала. Персонал, работающий с биометрическими системами, должен быть обучен работе с людьми с ограниченными возможностями;

к) согласие. В биометрической системе не следует хранить сведения об инвалидности субъекта персональных данных без его информированного согласия;

л) равенство. Права субъекта персональных данных с ограниченными возможностями должны быть такими же, как и у субъекта персональных данных, не являющегося лицом с ограниченными возможностями.

5.4 Здоровье и безопасность

5.4.1 Общие положения

У некоторых людей могут возникать опасения по поводу использования биометрических методов, которые усугубляются дезинформацией в средствах массовой информации. Такие опасения и представления будут влиять на производительность, что сведет к минимуму преимущества биометрических технологий для общества. Даже готовность использовать устройства сбора данных может зависеть от степени предполагаемого вмешательства технологий в отношении здоровья и безопасности.

При применении биометрических технологий возникают два аспекта здоровья и безопасности:

- прямое медицинское воздействие биометрических технологий, т. е. потенциальный риск для организма, связанный с использованием технологий. Как правило, такие опасения субъектов персональных данных не отражают реальность использования этих устройств и не имеют под собой научных оснований. Тем не менее для успешного внедрения биометрических приложений требуется, чтобы субъекты персональных данных были проинформированы о любом возможном риске, который может возникнуть в результате использования устройств сбора данных. Примеры:

- физический контакт с рабочей поверхностью устройства сбора данных, приводящий к вероятности передаче инфекций;
- освещение видимым или невидимым светом и последующее вероятное повреждение органа чувств;

- косвенное медицинское воздействие, связанное с возможным раскрытием информации о состоянии здоровья, полученной во время сбора биометрических персональных данных. Такая информация не нужна непосредственно для биометрического процесса, но при определенных обстоятельствах, дополнительной обработке или анализе может свидетельствовать об экстраординарном состоянии субъекта персональных данных. Субъекты персональных данных могут быть обеспокоены тем, что медицинская информация, полученная из таких данных, повлияет на их страхование жизни и ситуацию с трудоустройством, особенно если биометрическая информация передается или доступна между организациями.

5.4.2 Решение

Разработчик и системный оператор биометрического приложения должны учесть следующие принципы:

- устройства сбора данных должны соответствовать стандартам здоровья и безопасности, где это применимо, и ссылаться на эти стандарты. Субъекты персональных данных должны быть проинформированы о любых потенциальных последствиях для здоровья и безопасности;

- в определенных средах, где присутствуют инфекции или вредные вещества, следует принимать меры предосторожности, чтобы снизить риск перекрестного загрязнения до приемлемого уровня.

5.4.3 Частные случаи

Некоторые субъекты персональных данных могут испытывать особую психологическую или физическую чувствительность при использовании того или иного метода. Системные операторы должны знать о влиянии такой чувствительности на производительность биометрических приложений. По возможности системные операторы должны быть готовы урегулировать подобную ситуацию.

Следует учитывать особые условия в лечебных учреждениях, где медицинский персонал не может использовать отпечатки пальцев в биометрических системах из-за требований гигиены рук. Частные случаи с особыми условиями включают в себя предприятия общественного питания, обрабатывающие производства, фармацевтические предприятия, пункты пограничного и миграционного контроля, и карантинные объекты, где возможен контакт с лицами, не прошедшими оценку состояния здоровья. На внедрение биометрических технологий может повлиять требование носить защитную одежду по профессиональным, санитарно-гигиеническим или климатическим причинам, что обусловит использование бесконтактных технологий.

5.5 Удобство использования

5.5.1 Общие положения

Удобство использования биометрического приложения, обязательного или добровольного, является ключевым условием оптимальной производительности.

В настоящем подразделе представлены некоторые аспекты удобства использования биометрических приложений. Список не является исчерпывающим, и кроме того, в сценариях необходимо учитывать вопросы удобства использования в зависимости от конкретного биометрического метода.

Влияние аспектов удобства значительно различается в зависимости от конкретной используемой биометрической технологии и приложения, в котором она развернута.

Старение субъекта персональных данных влияет на эффективность биометрической верификации при сравнении с неизменным биометрическим шаблоном. Способность субъектов персональных данных использовать биометрическое приложение также может ухудшаться с возрастом.

5.5.2 Удобство использования и контекст использования

5.5.2.1 Общие положения

Производительность биометрических приложений зависит от физической среды, в которой они работают. Проблемы могут быть вызваны экстремальными климатическими условиями, загрязнением пылью или химическими веществами, потребностью в защитной одежде, защитой от вандализма, уровнями искусственного или естественного освещения, положением и ориентацией устройства сбора данных, а также наличием других аксессуаров и приспособлений в помещении. Производительность биометрических приложений зависит от качества зарегистрированного биометрического образца, что требует приемлемых условий регистрации биометрического образца. Для разных биометрических модальностей требуются различные параметры окружающей среды.

Следует предоставить четкие инструкции, документацию для субъектов персональных данных и гарантии в отношении использования данных и аспектов технологии, связанных со здоровьем и безопасностью.

5.5.2.2 Климатические условия

Экстремальные климатические условия, такие как температура или влажность, могут создавать проблемы для чувствительных устройств сбора данных. На открытом воздухе это может включать воздействие тумана, дождя или снега и приводить к образованию льда или конденсата на устройстве сбора данных, таком как объектив камеры. От субъектов персональных данных может потребоваться снять перчатки, головные уборы, шарфы или солнцезащитные очки. Экстремальные температуры могут привести к тому, что биометрический образец станет более сухим или влажным в зависимости от окружающей среды. Высокая температура окружающего воздуха может вызвать потение субъекта персональных данных и затруднить сбор биометрических персональных данных.

Примечание — В ГОСТ Р 58273 определены требования к планированию и выполнению испытаний эксплуатационных характеристик биометрической системы на воздействие условий окружающей среды.

5.5.2.3 Загрязнение

Загрязнение пылью или химическими веществами может потребовать крайне высокую активность по техническому обслуживанию для предотвращения коррозии устройств и содержания их в чистоте. Это является актуальным для инженерных или промышленных зон, а также мест приготовления еды, в которых присутствует большое количество частиц масла от жарки пищи. В некоторых средах может потребоваться специальный корпус для устройств сбора данных.

5.5.2.4 Общественные места

Устройства сбора данных в общественных местах могут подвергаться вандализму, в том числе нападению с применением тяжелого или острого предмета или распылению краски. Сбор биометрических персональных данных или распознавание диктора могут быть осложнены высоким уровнем окружающего шума от людей, машин, систем громкой связи или дорожного движения. Высокий уровень окружающего шума может помешать пользователям и субъектам персональных данных слышать устные инструкции, в особенности слепым или слабовидящим субъектам, которые полагаются на речевые инструкции.

В общественных местах рекомендуется использовать кабины или киоски с контролируемыми условиями окружающей среды для обеспечения требуемого уровня распознавания.

5.5.2.5 Расположение

При активном участии субъекта персональных данных расположение устройств сбора данных имеет важное значение. Расположение устройства сбора данных должно быть четко обозначено зна-

ками. Рекомендуется использовать умные знаки с подсветкой, чтобы предупредить слепых и других людей с ограниченными возможностями о присутствии знака. Рекомендуется использовать текстурированные полы для направления слепых и слабовидящих людей к устройству сбора данных.

Расположение устройства сбора данных должно позволять фактической операции сбора биометрических персональных данных находиться в поле зрения оператора биометрической системы.

Расположение устройства сбора данных должно предотвращать фоновые помехи во время сбора биометрических персональных данных и позволять осуществлять помощь детям со стороны взрослых или лицам с ограниченными возможностями со стороны лица, осуществляющего уход.

В биометрических приложениях могут возникнуть трудности при расположении устройства сбора данных, например в автомобильной системе, в которой пассажиры в машине должны подтвердить свои биометрические персональные данные. При распознавании лица водителя необходимо учитывать разницу в высоте транспортного средства.

При выборе подходящей биометрической системы для помещения, где большая часть людей имеют временные травмы, например для отделения неотложной (экстренной) медицинской помощи больницы, необходимо проанализировать характер и частоту травм до разработки и внедрения биометрического приложения.

5.5.2.6 Пропускная способность и плотность субъектов персональных данных

Для эффективной работы биометрической системы следует учитывать пиковую пропускную способность в месте разворачивания биометрической системы, управление очередями, количество необходимых устройств сбора данных, а также требуемое время и его вариабельность. Следует учитывать характер плотности субъектов персональных данных при выборе биометрической системы для внедрения.

При высокой пропускной способности рекомендуется использовать бесконтактные биометрические системы.

5.5.2.7 Положение

Важными факторами являются положение и ориентация устройств сбора данных. Устройства сбора данных должны быть доступны для субъектов персональных данных и располагаться в стационарном месте. Должно быть разработано руководство по положению с указанием стоящего или сидящего положения субъекта персональных данных, а также должны быть учтены различия в росте и охвате субъекта персональных данных. Рекомендуется обеспечить обратную связь с субъектом персональных данных по ориентации, размещению или громкости в случае голосовой системы.

5.5.2.8 Информация и обучение

Следует обеспечить доступность руководств пользователя вблизи общедоступных устройств сбора данных. Должны быть отображены номер или адрес горячей линии в случае сбоя или неуспешного использования биометрической системы субъектом персональных данных. Перед использованием биометрической системы в деловой или домашней среде необходимо провести обучение пользователей перед выполнением основных задач. Персонал, проводящий регистрацию, должен пройти специальное обучение для надлежащей регистрации данных.

5.5.2.9 Простота использования

Пользовательский интерфейс устройства сбора данных, требующего активного участия субъекта персональных данных, должен быть интуитивно понятным. Если субъект персональных данных должен представить свои биометрические персональные данные, предъявить токен, например смарт-карту, или ввести идентификационный номер или номер счета, то следует обеспечить логичную последовательность действий. Это может потребовать исследовать ожидания субъектов персональных данных и использовать соответствующие стандарты. Инструкции должны быть предоставлены в визуальной и звуковой форме, рекомендуется использовать графические, визуальные и/или звуковые подсказки. От субъекта персональных данных может потребоваться предпринять какие-либо действия для указания готовности предоставить свои биометрические персональные данные. Следует использовать обратную связь с указанием результата и, при необходимости, предложением повторной попытки. В некоторых средах биометрические персональные данные могут собираться пассивно и без необходимости активного участия субъекта персональных данных, например распознавание лица при чтении субъектом экрана. В таком случае субъект должен быть осведомлен о проведении биометрического распознавания.

5.5.2.10 Поддержка

Следует предоставлять пользовательскую поддержку, особенно в случаях, когда работа устройства сбора данных осуществляется без оператора. В случае возникновения проблем с представлением

биометрических персональных данных или какой-либо другой работой устройства сбора данных должна быть доступна служба поддержки, позволяющая субъекту обратиться за помощью либо удаленно, либо на месте. В качестве альтернативы субъект персональных данных должен иметь возможность вызывать другую процедуру, например дверной звонок или телефон в системе доступа в здание. Следует предоставить субъекту персональных данных доступ к процедуре отмены в случае травмы или действия, которое не позволяет ему предоставить биометрические персональные данные. Должна быть предусмотрена процедура отмены для использования в чрезвычайных ситуациях.

5.5.2.11 Дополнительные вопросы

Уровни искусственного или естественного освещения могут повлиять на скорость биометрического распознавания некоторых биометрических методов и удобство использования биометрической системы. Также следует учитывать вибрацию и движение рабочей среды системы.

5.6 Социальные, культурные и этические аспекты биометрии

Технические ограничения любой конкретной биометрической технологии не должны приводить к дискриминации какой-либо этнической или социальной группы.

5.6.1 Различия

Могут существовать культурные, социальные и этические различия в разных культурах, влияющие на биометрические приложения. Например, в большинстве культур в настоящее время принимают фотографические доказательства личности и, следовательно, принимают биометрическое распознавание лиц. В некоторых культурах люди могут возражать против прикосновения к общим поверхностям, таким как биометрические сканеры отпечатков пальцев или геометрии рук.

5.6.2 Многонациональные среды

При внедрении биометрического приложения для использования в многонациональной группе пользователей, например для учета рабочего времени и посещаемости, образы соответствующих культурных групп должны быть включены во все информационные и учебные материалы.

5.6.3 Анонимность

В разных культурных и прикладных контекстах стремление людей к анонимности варьируется, поэтому биометрические приложения должны обеспечивать гибкость в отношении степени анонимности. Например, в некоторых биометрических приложениях не обязательно знать персональные данные субъекта персональных данных. Может потребоваться только подтверждение прав или предотвращение множественной регистрации.

5.6.4 Одежда, украшения и традиции

В некоторых культурах люди могут неохотно использовать биометрические технологии, поскольку считают, что это серьезно подрывает их культурные, социальные и этические обычаи или убеждения.

Например, биометрическое приложение распознавания лиц может противоречить культуре, в которой нормальным поведением является ношение чадры или головных платков. Может быть непрактичным или неприемлемым биометрическое приложение, на производительность которого отрицательно влияют культурные или социальные украшения тела (например, макияж, татуировки, украшения, одежда или растительность на лице).

5.6.5 Обязательное участие

Некоторые биометрические приложения могут требовать обязательного участия. Например, регистрация и использование биометрического приложения может быть необходимым условием для получения работы или входа в безопасное место. Степень приемлемости будет зависеть от культурной и социальной демографии.

Тщательное рассмотрение культурных, социальных и этических аспектов биометрии следует проводить до внедрения биометрических приложений.

5.7 Принятие

5.7.1 Общие положения

Решающим аспектом успешного результата внедрения биометрического приложения является принятие биометрических систем субъектами персональных данных. По мере расширения использования биометрии важно оценить меняющееся мнение общественности о технологии, ее приложениях и обеспечении защиты приватности. Общая производительность биометрического приложения будет низкой, если субъекты персональных данных не принимают биометрическую систему, вне зависимости от того, является ли использование биометрической системы обязательным или добровольным.

Даже в рамках обязательной биометрической системы субъекты персональных данных могут отвергнуть систему своим поведением, не направленным на сотрудничество, что со временем приведет к существенному снижению вероятности распознавания. Следует определить положительные и отрицательные факторы принятия. Взаимодействие между пользователем и биометрическим приложением является эффективным только тогда, когда приводит к эффективному выполнению желаемой задачи. Такое взаимодействие происходит в контексте, который включает не только физическое и организационное, но и культурное окружение.

Опасения субъектов персональных данных могут быть логически обоснованными или субъективными. Несмотря на то, что техническим специалистам понятнее работа с первой группой, необходимо анализировать и менее осязаемые аспекты.

Факторы принятия биометрического приложения могут включать следующее:

- приватность/защиту данных;
- удобство;
- надежность и производительность;
- правовые условия, ориентированные на потребителя;
- простота использования;
- соотношение цены и качества;
- жизненный цикл;
- инвазивность;
- здоровье и гигиена;
- пол субъекта;
- религия, этика и культура.

Максимальное принятие достигается, когда биометрическое приложение приносит наибольшую ощутимую пользу субъекту персональных данных. Если субъект персональных данных не видит никакой выгоды от использования биометрической системы, то желание использовать ее и, следовательно, общее принятие приложения снизится. Чем менее ощутима польза для субъекта персональных данных, тем меньше он готов принять на себя потенциальные риски, связанные с использованием биометрического приложения.

Повышается степень принятия биометрического приложения, если оно:

- соответствует производственным задачам и задачам безопасности, которые должны выполнять субъекты персональных данных, т. е. биометрическое приложение интегрировано в рабочий процесс;
- работает с высокой производительностью (высокая скорость, низкий процент ошибок) на всех этапах использования (установка, регистрация, ежедневное использование, непредвиденные обстоятельства);
- имеет доверие к безопасности, безопасному хранению биометрических персональных данных и неиспользованию их для других целей.

Также фактором принятия является прозрачность биометрической системы для субъекта персональных данных. Позитивное отношение к биометрии может быть усилено за счет более широкого освещения биометрических технологий в средствах массовой информации. Чем больше человек знает о биометрической системе и ее деталях, преимуществах и рисках, тем больше он сможет доверять биометрической системе. Следует учесть, что доверие к оператору биометрической системы может влиять на доверие субъекта персональных данных к самой системе.

Положительное отношение к биометрии коррелирует с простотой, скоростью и удобством в течение длительного периода времени.

При внедрении биометрических технологий необходимо принять ряд компромиссных решений, например между снижением приватности субъекта персональных данных и повышением безопасности. Для разных групп субъектов персональных данных данный компромисс находится в различных точках, поэтому разработчик и оператор биометрического приложения должен учитывать различные группы пользователей. Группирование субъектов персональных данных может проводиться:

- по возрасту;
- полу;
- образованию;
- профессии;
- компетентности;
- культуре;
- этнической принадлежности;

- обязанностям по уходу, например родители детей школьного возраста и лица, ответственные за пожилых и уязвимых лиц;
- социально-экономическому распределению и происхождению;
- отношению к власти и взаимодействию с правоохранительными органами.

В разных культурах отношение к биометрии и разным уровням информации будет отличаться. Культурные различия могут быть даже сильнее, чем гендерные или возрастные различия. Могут быть различия в оценке приватности, а также в рейтинге производительности и безопасности.

5.7.2 Приватность и принятие

Гарантии или принципы приватности являются решающими факторами приемлемости для субъектов персональных данных биометрической системы. Максимально возможная прозрачность способна уменьшить опасения по поводу приватности. Это должно включать информацию до начала использования, цель использования, а также информацию о способах использования, передачи и обработки биометрических персональных данных. Опасения людей включают возможную комбинацию с другими личными идентификаторами и риск отслеживания передвижения людей.

Возможность субъекта персональных данных проверить корректность биометрических персональных данных повышает доверие к биометрической системе.

Комплексная концепция безопасности должна требовать, чтобы используемые биометрические персональные данные рассматривались как персональные данные, и были предусмотрены механизмы для защиты этих данных.

5.7.3 Надежность, производительность и принятие

К снижению принятия может привести отсутствие уверенности в точности и надежности биометрических технологий (например, высокая вероятность ложного недопуска и неудовлетворительный пользовательский интерфейс). Для некоторых социальных групп и культур страх является нормальной психологической реакцией на неизвестность. Высокая вероятность ложного недопуска может привести к снижению приемлемости в зависимости от цели приложения.

5.7.4 Рекомендуемые действия

Рекомендуется провести следующие действия для повышения принятия биометрической системы:

- а) пилотное испытание биометрического приложения и определение факторов приемлемости для групп потенциальных субъектов персональных данных;
- б) исследование контингента пользователей конкретного приложения для решения проблем соответствующих субъектов персональных данных;
- в) дополнительное испытание и перепроектирование в случае использования биометрической системы, первоначально разработанной для других целевых групп субъектов персональных данных;
- г) повторная регистрация по мере старения субъектов персональных данных;
- д) нахождение компромисса между уменьшением числа ложных недопусков и снижением безопасности. Следует пояснить субъектам персональных данных связь между ложным допуском и ложным недопуском;
- е) предоставление информации и инструкции по использованию, понятных для нетехнических специалистов и, в зависимости от количества пользователей, на разных языках;
- ж) испытания принятия, во время которых группе субъектов персональных данных предлагается ознакомиться с биометрическим приложением в контексте приложения;
- и) обучение и продвижение предполагаемого использования биометрии имеют решающее значение для устранения логически обоснованных и субъективных опасений субъектов персональных данных;
- к) проверка отсутствия влияния целевых условий окружающей среды (температуры, влажности и т. д.) на частоту ложного недопуска;
- л) меры предосторожности в отношении риска перекрестного заражения.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных национальных стандартов
международным стандартам, использованным
в качестве ссылочных в примененном международном стандарте

Таблица ДА.1

Обозначение ссылочного межгосударственного стандарта	Степень соответствия	Обозначение и наименование ссылочного международного стандарта
ГОСТ ISO/IEC 2382-37—2016	IDT	ISO/IEC 2382-37:2012 «Информационные технологии. Сло- варь. Часть 37. Биометрия»
П р и м е ч а н и е — В настоящей таблице использовано следующее условное обозначение степени соот- ветствия стандарта: - IDT — идентичный стандарт.		

**Приложение ДБ
(справочное)**

**Сопоставление структуры настоящего стандарта со структурой
примененного в нем международного стандарта**

Таблица ДБ.1

Структура настоящего стандарта	Структура международного стандарта ISO/IEC TR 24714:2023
Приложение ДА Сведения о соответствии ссылочных национальных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте	—
Приложение ДБ Сопоставление структуры настоящего стандарта со структурой примененного в нем международного стандарта	—
—	Приложение А Примеры для рассмотрения межведомственных и социальных аспектов в биометрических приложениях
—	Библиография
Примечание — Сопоставление структуры настоящего стандарта со структурой примененного в нем международного стандарта приведено, начиная с приложения А, т.к. предыдущие разделы идентичны.	

УДК 336.77:002:006.354

ОКС 35.240.15

Ключевые слова: информационные технологии, биометрия, социальные аспекты, доступность, удобство использования

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

Сдано в набор 28.11.2023. Подписано в печать 11.12.2023. Формат 60×84%. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 2,10.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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