



ПРЕДВАРИТЕЛЬНЫЙ
НАЦИОНАЛЬНЫЙ
СТАНДАРТ
РОССИЙСКОЙ
ФЕДЕРАЦИИ

ПНСТ
876—
2023
(ISO/IEC TR
29144:2014)

Информационные технологии

БИОМЕТРИЯ

Применение биометрических технологий в системах управления идентификационными данными

(ISO/IEC TR 29144:2014, Information technology — Biometrics —
The use of biometric technology in commercial Identity
Management applications and processes, MOD)

Издание официальное

Москва
Российский институт стандартизации
2023

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным бюджетным образовательным учреждением высшего образования «МИРЭА — Российский технологический университет» (ПТУ 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. № 70-пнст

4 Настоящий стандарт является модифицированным по отношению к международному документу ISO/IEC TR 29144:2014 «Информационные технологии. Биометрия. Применение биометрических технологий в системах управления идентификационными данными» (ISO/IEC TR 29144:2014 «Information technology — Biometrics — The use of biometric technology in commercial Identity Management applications and processes», 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 соответствие с ГОСТ Р 1.5—2012 (пункт 3.5).

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

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

5 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, 2014

© IEC, 2014

© 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 Биометрические технологии и IDMS	2
5.1 Общие положения	2
5.2 Биометрия и идентичность	2
5.3 Идентичность и биометрическое распознавание	3
5.4 Биометрические идентификаторы	3
5.5 Роль оператора	3
5.6 Обеспечение целостности базы данных	4
6 Биометрические факторы в IDMS	4
6.1 Общие положения	4
6.2 Сбор и запись биометрических образцов	4
6.3 Привязка биометрических образцов	5
6.4 Изменения имени, псевдонима и идентификационных данных	5
6.5 Изменения состояния	5
6.6 Спуфинг	6
6.7 Другие исключения	6
6.8 Другие актуальные вопросы	6
7 Вопросы реализации	6
7.1 Общие положения	6
7.2 Объединение баз данных	6
7.3 Усовершенствование IDMS на основе токенов и знаний	7
7.4 Ограничения доступа к данным	7
7.5 Приватность	7
7.6 Механизмы предотвращения неправомерного использования систем	8
7.7 Работа системы в условиях многонациональности	8
Приложение ДА (справочное) Сведения о соответствии ссылочных национальных и межгосударственных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном документе	9
Приложение ДБ (справочное) Сопоставление структуры настоящего стандарта со структурой примененного в нем международного документа	10

Введение

Настоящий стандарт содержит рекомендации по внедрению биометрических технологий в системы управления идентификационными данными (IDMS). Следование рекомендациям 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;
- обеспечение интероперабельности;
- обеспечение большей степени независимости внедряемых решений от поставщиков.

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

Применение биометрических технологий в системах управления
идентификационными данными

Information technology.

Biometrics.

The use of biometric technology in identity management systems

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

1 Область применения

Настоящий стандарт устанавливает:

- рекомендации по использованию биометрических технологий в системах управления идентификационными данными;
- элементы, которые необходимо учитывать при внедрении биометрических технологий в системы управления идентификационными данными.

Настоящий стандарт не устанавливает:

- архитектуру и структуру системы управления идентификационными данными;
- бизнес-потребности в биометрической базе данных или процессе;
- перечень биометрических персональных данных для использования в системах управления идентификационными данными;
- законность и приемлемость использования биометрических технологий в определенных юрисдикциях и культурах;
- общую структуру идентификаторов и глобальную идентификацию объектов (например, идентификаторы объектов);
- технические спецификации в отношении использования доверенных биометрических аппаратных и программных средств.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

ГОСТ ISO/IEC 29100 Информационные технологии. Методы и средства обеспечения безопасности. Основы защиты персональных данных

ГОСТ Р 58624.1 (ИСО/МЭК 30107-1:2016) Информационные технологии. Биометрия. Обнаружение атак на биометрическое предъявление. Часть 1. Структура

ГОСТ Р 58624.2 (ИСО/МЭК 30107-2:2017) Информационные технологии. Биометрия. Обнаружение атак на биометрическое предъявление. Часть 2. Форматы данных

ГОСТ Р 58624.3 (ИСО/МЭК 30107-3:2017) Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 3. Испытания и протоколы испытаний

ГОСТ Р ИСО/МЭК 29794-1 Информационные технологии. Биометрия. Качество биометрического образца. Часть 1. Структура

Примечание — При использовании 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 следующий термин с соответствующим определением:

3.1

идентичность (*identity*): Представление (образ) сущности в виде одного или нескольких атрибутов, которые позволяют сущностям быть различимыми в домене.

Примечания

1 Сущность может иметь более одного набора относящихся к ней атрибутов.

2 Несколько сущностей могут иметь одинаковый набор атрибутов.

[Адаптировано из ГОСТ Р 59381—2021, пункт 3.13]

4 Сокращения

В настоящем стандарте применены следующие сокращения:

ПИН — персональный идентификационный номер;

IDM — управление идентификационными данными (identity management);

IDMS — система управления идентификационными данными (identity management system);

PIA — оценка воздействия на приватность (privacy impact assessment).

5 Биометрические технологии и IDMS

5.1 Общие положения

В настоящем стандарте представлены рекомендации по использованию биометрических технологий в IDMS. Настоящий стандарт не рассматривает работу IDMS.

5.2 Биометрия и идентичность

Субъект персональных данных может быть описан многими различными атрибутами, и разные наборы этих атрибутов могут формировать разные идентичности.

Идентичность человека может быть уникальной в биометрической системе. Атрибуты, которые являются уникальными, называют «идентификаторами». Такой аспект уникальности часто понимается как сущность идентичности, однако в контексте IDM уникальность является одним из многих аспектов, которые необходимо учитывать. В то время как идентичность является уникальной в одной системе, человек может иметь уникальную, но другую идентичность в другой или других биометрических системах. Набор идентификаторов должен быть достаточным для того, чтобы отличить одного субъекта пер-

сональных данных от другого в конкретной биометрической системе. При совместном использовании биометрических идентификаторов в нескольких системах могут быть сопоставлены данные об одной и той же идентичности в разных биометрических системах.

5.3 Идентичность и биометрическое распознавание

Перед внедрением биометрических технологий в IDMS необходимо определить требуемый процесс распознавания и уровни достоверности идентичности. В соответствии с требованиями распознавания должны быть определены требования к идентичности. Рекомендуется учесть следующие аспекты:

- а) шаблон идентичности, который будет использован субъектом персональных данных;
- б) зависимость доверия к идентичности от уровня активности или предоставленного ранее доступа;
- в) вероятность присвоения другими лицами или использования с разрешения владельца идентификационных документов и токенов;
- г) вероятность изменения информации об имени при вступлении в брак или в программах защиты свидетелей;
- д) вероятность временного изменения биометрических персональных данных субъекта персональных данных;
- е) невозможность сбора определенных биометрических персональных данных, если у субъекта персональных данных они отсутствуют или повреждены в результате травмы или заболевания;
- ж) вероятность изменения поведенческих биометрических персональных данных при каждой попытке.

Управление рисками, а также надлежащие политика и процедуры могут обеспечить приемлемый уровень доверия при использовании системы биометрического распознавания.

5.4 Биометрические идентификаторы

В биометрической системе может быть использован широкий спектр идентификаторов. При подборе идентификатора необходимо учесть, что он должен удовлетворять потребности всех пользователей системы и предоставлять работоспособное решение.

При выборе конкретной биометрической модальности необходимо учитывать следующие факторы:

- стабильность. Биометрические персональные данные должны сохранять достаточное количество биометрических признаков, чтобы минимизировать влияние изменений на производительность системы;
- удобство использования. Удобство и простота использования биометрических персональных данных является ключевым фактором при внедрении и принятии биометрической системы. По возможности датчики должны быть расположены так, чтобы все люди могли их эффективно использовать. Система должна реагировать своевременно и должна быть простой в управлении и обслуживании;
- приватность. В связи с растущим вниманием и осведомленностью общественности о биометрических системах приватность идентификационных данных, хранящихся в биометрической системе, должна иметь первостепенное значение. Все данные должны быть получены с согласия субъекта персональных данных;
- стоимость. Стоимость биометрической системы следует сопоставлять с преимуществами ее внедрения. Если использование конкретного биометрического идентификатора является дорогостоящим и имеет низкий экономический эффект для всей биометрической системы, следует провести поиск других решений;
- уязвимость. Выбранные биометрические модальности должны быть сложными для подделывания, а система и устройства сбора данных должны быть защищены от атак и предупреждать в случае несанкционированного доступа. Рекомендуется использовать соответствующую политику и контроль с участием человека для ослабления атак и уязвимостей.

5.5 Роль оператора

Перед внедрением биометрических технологий в IDMS необходимо определить роль оператора. Решение должно учитывать, как оператор может обрабатывать результаты сравнений, качество изображений и чем требования будут отличаться от автоматизированного процесса сравнения. Следует рассмотреть вопрос о доступе к результатам сравнения и различные решения рабочего процесса для оператора. Необходимо учитывать:

- квалификацию, обучение и компетентность персонала;
- экран дисплея;
- рабочий процесс сравнений;
- обработку исключений;
- качество данных, необходимое для процессов биометрического сравнения.

5.6 Обеспечение целостности базы данных

Следует обеспечить целостность базы данных при внедрении биометрических технологий в IDMS. Рекомендуется внедрить механизм очистки данных.

Несогласованные данные могут быть результатом одной идентичности, имеющей более одного уникального идентификатора, или нескольких идентичностей, имеющих один и тот же идентификатор. Это может произойти из-за человеческой ошибки, системной ошибки, сбоя процесса или мошенничества.

6 Биометрические факторы в IDMS

6.1 Общие положения

В настоящем разделе определены факторы, которые следует учитывать при внедрении биометрических технологий в IDMS.

6.2 Сбор и запись биометрических образцов

Ценность биометрического образца для биометрической системы зависит от его точности и качества, а также от процесса сравнения с набором биометрических контрольных шаблонов.

6.2.1 Сбор биометрических образцов

Должен быть организован процесс сбора биометрических образцов требуемого качества. Эксплуатационные характеристики биометрической системы напрямую зависят от качества биометрических образцов, поэтому важно обеспечить получение биометрического образца с максимально возможным качеством и выполнить оценку качества. При сборе биометрических образцов необходимо учитывать следующее:

- стандарты. Сбор данных должен соответствовать действующим национальным и международным стандартам;
- условия окружающей среды. Следует учитывать условия окружающей среды;
- проверку качества. Необходимо проводить оценку качества во время сбора данных;
- удаленный сбор данных. Рекомендуется учесть возможность сбора биометрических образцов в удаленных местах или местах, которые не входят в штатную работу системы;
- невозможность сбора данных. Следует рассмотреть ситуацию, когда процесс не может быть выполнен.

Дополнительная информация о сборе данных представлена в *ГОСТ Р ИСО/МЭК 29794-1* и в национальных стандартах на форматы обмена.

6.2.2 Стабильность и повторяемость процесса

При внедрении биометрических технологий в IDMS следует обеспечить стабильный и воспроизводимый процесс сбора данных. Все биометрические модальности подвержены изменчивости из-за ряда факторов, в том числе связанных с окружающей средой, например освещения, температуры, шума и эргономики устройств сбора данных. Рекомендуется учитывать все воздействующие факторы и снижать риски. Изменчивость вызывается также аспектами человеческого поведения и состояния, такими как положение, выражение лица, состояние кожи, состояние здоровья и *возрастными изменениями*.

6.2.3 Хранение и срок использования биометрических записей

Качество биометрических персональных данных может ухудшиться со временем. Старение является проблемой для большинства биометрических модальностей. Как правило, с увеличением времени с момента регистрации увеличивается число ошибочных сравнений.

6.2.4 Стабильность биометрических записей

На стабильность биометрической записи могут повлиять человеческие факторы, такие как эмоции, усталость, состояние здоровья и наличие стресса.

6.3 Привязка биометрических образцов

6.3.1 Общие положения

Следует оценить целостность привязки биометрических образцов к идентичности. При поступлении данных из нескольких источников могут быть определены разные уровни достоверности для источника биометрических образцов и идентификационных данных.

Доверие к информации и ограничения на обработку идентификационной информации должны быть четко описаны в соглашении для IDMS, в особенности для данных из других систем. Рекомендуется определять уровень доверия с учетом полного процесса биометрического распознавания.

Пример соглашения может быть следующим:

- А: всегда согласовано. Нет сомнений в подлинности, достоверности и компетентности источника данных. Система или организация, предоставляющая информацию, является надежной. При проведении проверки оборудование и процедуры демонстрируют высокое качество;

- В: преимущественно согласовано. Информация была получена ранее из источника и в целом оказалась согласованной;

- С: иногда согласовано. Некоторая информация, полученная из источника, оказалась согласованной, но источнику нельзя доверять без подтверждения;

- D: не согласовано. Информация получена из источников, которые в прошлом представили информацию, оказавшейся в целом противоречивой или непроверяемой;

- Е: не проверено. Информация получена из источника, который ранее не использовался. Информация не обязательно является несогласованной, но к ней следует относиться с осторожностью и найти подтверждение согласованности.

6.3.2 Подтверждение данных

При привязке биометрических образцов к субъекту персональных данных следует учесть степень, с которой отдельная часть информации может быть подтверждена ссылкой на другие источники.

6.3.3 Обработка данных

Может быть использован набор ограничений на обмен данными, указывающих, как и кому может быть предоставлена информация.

6.3.4 Прочность связи данных

Рекомендуется проводить оценку того, насколько сильно предполагаемый идентификатор привязан к субъекту персональных данных. Может быть использована следующая шкала оценки прочности связи:

- 1: отделение метки или токена от человека невозможно обнаружить;
- 2: отделение обнаруживается при внимательном рассмотрении, например, путем сравнения фотографии с лицом владельца;
- 3: отделение обнаруживается на пользовательском терминале, например, при поднесении карты с соответствующим ПИН-кодом или паролем к устройству;
- 4: отделение определяется автоматически;
- 5: отделение невозможно.

6.3.5 Удаление данных

Биометрические образцы, относящиеся к идентичности, могут быть удалены из системы из-за требований юрисдикции или законодательства. Удаление данных из системы должно осуществляться в соответствии с законодательством.

6.4 Изменения имени, псевдонима и идентификационных данных

В связи с тем, что человек по различным причинам может изменить свое имя, биометрические образцы должны быть связаны не с именем, а с уникальным идентификатором в IDMS, что позволит обновлять идентичность без изменения биометрического идентификатора. Порядок и процессы для внесения изменений должны определяться политикой IDMS.

6.5 Изменения состояния

Человек может изменить ключевые параметры, используемые для идентификации, такие как национальность, место работы, место жительства, образование и квалификация, и их следует рассматривать как фиксированные только во время транзакции или наблюдения.

Аналогично изменению имени, биометрические образцы должны быть связаны только с уникальным идентификатором в IDMS, что позволит обновлять идентичность без изменения биометрического идентификатора. Порядок и процессы для внесения изменений должны определяться политикой IDMS.

При внедрении биометрических технологий в IDMS следует учитывать, как будет работать процесс сопоставления с метаданными. Например, если для уменьшения размера галереи результатов сравнения используется дата рождения, и дата рождения была изменена, то процесс сравнения следует повторить.

6.6 Спуфинг

Биометрические технологии подвержены спуфинговым атакам и атакам на биометрическое предъявление, поэтому следует иметь эффективные меры противодействия. По мере развития и увеличения темпов внедрения биометрических технологий количество и сложность атак продолжает расти. Для обеспечения целостности системы необходимо проводить научные исследования и разработки для проверки биометрических уязвимостей и мер противодействия. Меры противодействия имеют ограниченный жизненный цикл, поэтому регулярное и независимое от поставщиков испытание эффективности системы имеет такую же ценность, как и выбор правильного оборудования.

Дополнительная информация представлена в *ГОСТ Р ИСО/МЭК 29794-1*, *ГОСТ Р 58624.1*, *ГОСТ Р 58624.2*, *ГОСТ Р 58624.3* и в национальных стандартах на форматы обмена.

6.7 Другие исключения

При внедрении биометрических технологий в IDMS следует учитывать вероятность подделки предъявляемых документов, удостоверяющих личность. Биометрия является единственной надежной прямой связью между документом и его законным владельцем. Например, если отображаемый портрет на документе был подменен, то биометрическое сравнение легитимного фотографического изображения законного владельца продемонстрирует это, отражая, что предъявитель подделал документ.

При разработке рекомендуется учесть другие исключения, например неопознанных больных с амнезией или беспризорных детей.

6.8 Другие актуальные вопросы

6.8.1 Удобство использования и доступность

Следует обеспечить удобство использования и доступность в каждой биометрической транзакции.

6.8.2 Отсутствие идентификационных записей

Следует учесть, что у лиц, мигрирующих в новую страну или юрисдикцию, может полностью отсутствовать какой-либо зарегистрированный цифровой профиль в новой юрисдикции, а записи, хранящиеся в предыдущей юрисдикции, могут быть недоступными.

6.8.3 Законные представители

Законные представители, имеющие законные полномочия действовать от имени другого лица, такие как действующая доверенность, могут идентифицировать себя сами по себе, а также в качестве агента для других субъектов персональных данных.

7 Вопросы реализации

7.1 Общие положения

В настоящем разделе определены вопросы реализации, которые следует учитывать при внедрении биометрических технологий в IDMS.

7.2 Объединение баз данных

При объединении двух баз данных, каждая из которых содержит данные об отдельных людях, необходимо обеспечить корректную идентификацию и объединение записей, данные которых содержатся в обоих наборах. Необходимо обеспечить, чтобы данные одного человека не были объединены ошибочно с данными другого человека. Это особенно актуально, когда базы данных имеют очень большое количество общих полей, и некоторые из таких общих элементов похожи или идентичны. При наличии биометрической метки в каждой записи двусмысленность устраняется при условии, что две системы используют одну и ту же биометрическую модальность и один и тот же экземпляр — напри-

мер, один и тот же палец или глаз. Рекомендуется учесть потенциальную степень гармонизации между организациями аналогичного типа, которые могут быть вовлечены в слияние в будущем.

Если две базы данных объединяются на основе биографического содержания при отсутствии сопоставимых биометрических персональных данных в обеих системах, то следует пометить каждый элемент данных достаточным количеством метаданных, чтобы обеспечить последующее разделение записей в базе данных при обнаружении записей, которые были объединены некорректно.

Объединение баз данных, содержащих идентификационную информацию, может вызвать проблемы с приватностью (см. 7.5). При использовании биометрических персональных данных для объединения записей могут возникнуть проблемы с приватностью и безопасностью (см. 7.6).

При объединении данных следует учитывать надежность данных в зависимости от источника данных и целостности процесса регистрации.

7.3 Усовершенствование IDMS на основе токенов и знаний

При внедрении биометрических технологий в IDMS, в которой ранее использовались токены, такие как карта, или знание пароля или ПИН-кода, одним из последствий может быть злоупотребление системой. В системе могут быть зарегистрированы лица, имеющие несколько токенов или паролей, или один токен или пароль могут использоваться несколькими лицами. При обнаружении подобных злоупотреблений потребуются процессы для исправления записей прошлых периодов.

7.4 Ограничения доступа к данным

В отдельных случаях данные могут быть ограничены или скрыты из-за ограничений доступа пользователя или оператора. В этом случае данные остаются в биометрической системе и будут продолжать использоваться для сравнения.

Например, система распознавания лиц может маскировать или заменять совпадающее изображение лица абстрактным значком в галерее изображений, но при выборе для непосредственного сравнения может отображать рейтинг и решение системы.

7.5 Приватность

Использование методов обеспечения приватности на ранних этапах разработки системы снизит потенциальное воздействие на частную жизнь. Следует провести PIA для определения того, как система и инициирование программ сбора новых данных могут повлиять на частную жизнь и возможное неправомерное использование.

К биометрическим технологиям следует применять следующие принципы обеспечения приватности (см. ГОСТ ISO/IEC 29100):

- прозрачность: уведомление человека о сборе, использовании, распространении и хранении биометрических персональных данных;
- индивидуальное участие: вовлечение человека в процесс использования биометрических персональных данных и оформление согласия на обработку биометрических персональных данных (включая сбор, использование, распространение и хранение). Обеспечение механизмов для надлежащего доступа, исправления и возмещения ущерба в отношении использования организацией биометрических персональных данных;
- спецификация цели: указание полномочий, разрешающих сбор биометрических персональных данных, и цели использования биометрических персональных данных;
- минимизация данных: сбор только тех биометрических персональных данных, которые необходимы для достижения указанной цели, и хранение биометрических персональных данных только в пределах срока, необходимого для достижения указанной цели;
- ограничения в отношении использования: использование биометрических персональных данных исключительно для указанных целей. Обмен биометрических персональных данных только с целью, совместимой с целью сбора биометрических персональных данных;
- качество и целостность данных: точность, актуальность, своевременность и полноту биометрических персональных данных;
- безопасность: защита биометрических персональных данных на всех носителях с помощью соответствующих мер безопасности от таких рисков, как потеря, несанкционированный доступ или использование, уничтожение, модификация или непреднамеренное или ненадлежащее раскрытие;

- подотчетность и аудит: проверка фактического использования биометрических персональных данных на предмет соответствия принципам и применимым требованиям защиты приватности.

При внедрении биометрических технологий в IDMS следует учесть следующие аспекты:

а) биометрические образцы неудовлетворительного качества из-за возраста, метода сбора данных или рода занятий субъекта персональных данных (например, отпечатки пальцев низкого качества у каменщиков). Следует предусмотреть отмену сбора определенных биометрических персональных данных, если у субъекта персональных данных они отсутствуют или повреждены в результате травмы или заболевания;

б) открытый сбор. Субъекты персональных данных должны знать, что собираются их биометрические персональные данные. Сбор биометрических персональных данных не должен быть скрытым;

с) надежные меры защиты данных: шифрование при хранении и передаче. Рекомендуется передавать биометрические персональные данные и биографические данные по отдельности;

д) беспрепятственное исправление несоответствия (например, супруги предоставили свои отпечатки пальцев и биографические данные, но отпечатки пальцев мужа хранятся вместе с биографическими данными жены и наоборот);

е) восстановление. Если субъект персональных данных заявил, что информация неверна, то следует предоставить возможность ее просмотра и исправления.

Следует обеспечивать приватность с начала разработки системы сбора биометрических персональных данных. Должна быть проведена оценка воздействия на приватность, которая затрагивает следующие области:

- сбор информации;
- использование информации;
- хранение информации;
- обмен информацией (внутренний и внешний);
- уведомление;
- индивидуальный доступ, восстановление и исправление;
- безопасность;
- технологии.

7.6 Механизмы предотвращения неправомерного использования систем

Экономическое обоснование внедрения биометрических технологий в IDMS часто обусловлено необходимостью уменьшить количество случаев мошенничества. Добавление биометрических технологий может ограничить масштабы мошенничества, связанного, например, с использованием украденных документов или клонированных карт.

7.7 Работа системы в условиях многонациональности

При работе организации в разных культурных и политических областях необходимо учитывать факторы:

- культуры;
- законов;
- приватности;
- отрасли;
- расовые различия.

**Приложение ДА
(справочное)**

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

Таблица ДА.1

Обозначение ссылочного межгосударственного стандарта	Степень соответствия	Обозначение и наименование ссылочного международного стандарта
ГОСТ ISO/IEC 2382-37—2016	IDT	ISO/IEC 2382-37:2012 «Информационные технологии. Словарь. Часть 37. Биометрия»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта: - IDT — идентичный стандарт.		

**Приложение ДБ
(справочное)**

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

Таблица ДБ.1

Структура настоящего стандарта	Структура международного документа ISO/IEC TR 29144:2014
Приложение ДА Сведения о соответствии ссылочных национальных и межгосударственных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном документе	—
Приложение ДБ Сопоставление структуры настоящего стандарта со структурой примененного в нем международного документа	—
—	Библиография
П р и м е ч а н и е — Сопоставление структуры настоящего стандарта со структурой примененного в нем международного документа приведено начиная с приложения ДА, т. к. предыдущие разделы идентичны.	

УДК 336.77:002:006.354

ОКС 35.240.15

Ключевые слова: информационные технологии, биометрия, система управления идентификационными данными

Редактор *Е.В. Якубова*
Технический редактор *И.Е. Черепкова*
Корректор *С.И. Фирсова*
Компьютерная верстка *М.В. Малеевой*

Сдано в набор 29.11.2023. Подписано в печать 11.12.2023. Формат 60×84%. Гарнитура Ариал.
Усл. печ. л. 1,86. Уч.-изд. л. 1,58.

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