ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59515— 2021

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Подтверждение идентичности

(ISO/IEC TS 29003:2018, NEQ)

Издание официальное

Москва
Стандартинформ
2021

Предисловие

1 РАЗРАБОТАН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН), Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО ИАВЦ) и Акционерным обществом «Аладдин Р.Д.» (АО «Аладдин Р.Д.»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 022 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 20 мая 2021 г. № 419-ст

4 Настоящий стандарт разработан с учетом основных нормативных положений международного документа ISO/IEC TS 29003:2018 «Информационные технологии. Методы и средства обеспечения безопасности. Подтверждение идентичности» (ISO/IEC TS 29003:2018 «Information technology — Security techniques — Identity proofing», NEQ)

5 ВВЕДЕН ВПЕРВЫЕ

6 Федеральное агентство по техническому регулированию и метрологии не несет ответственности за патентную чистоту настоящего стандарта. Патентообладатель может заявить о своих правах и направить в национальный орган по стандартизации аргументированное предложение о внесении в настоящий стандарт поправки для указания информации о наличии в стандарте объектов патентного права и патентообладателе

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

Содержание

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Подтверждение идентичности

Information technology. Security techniques. Identity proofing

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт содержит рекомендации по подтверждению идентичности субъектов (физических лиц), определяет уровни подтверждения их идентификационных данных, а также требования для достижения этих уровней.

Положения настоящего стандарта могут быть использованы при разработке и эксплуатации систем управления идентификационными данными и применяются совместно с документами по стандартизации, регламентирующими вопросы идентификации.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 58833—2020 Защита информации. Идентификация и аутентификация. Общие положения

ГОСТ Р 59381 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 1. Терминология и концепции

ГОСТ Р 59382 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 3. Практические приемы

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 следующие термины с соответствующими определениями:

3.1 **вспомогательный атрибут** (supportive attribute): Атрибут, используемый при подтверждении идентичности, но не в качестве идентификационного атрибута.

Издание официальное

3.2 **заявление** (application): Процесс, посредством которого предоставляется информация, используемая для подтверждения идентичности субъекта.

3.3

идентификационная информация (identity information): Совокупность значений атрибутов идентичности, опционально связанных с метаданными.

Примечание — В автоматизированной (информационной) системе физическое лицо присутствует в виде его «цифрового образа», который в том числе характеризуется идентификационной информацией.

[ГОСТ Р 59381—2021, пункт 3.11]

3.4

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.

3 Другие документы, например ITU-T X1252 [1], также определяют различительное использование набора атрибутов.

[ГОСТ Р 59381—2021, пункт 3.13]

3.5 **идентификационный атрибут** (identifying attribute): Атрибут, способствующий однозначной идентификации субъекта в данном домене.

3.6

домен (domain): Среда с определенными граничными условиями, в которых существуют и взаимодействуют субъекты.

[Адаптирован из ГОСТ Р 59381—2021, пункт 3.8]

3.7 **мандат** (credential): Объект или структура данных, которые официально привязывают идентификационные данные с помощью идентификатора или идентификаторов и (факультативно) дополнительных атрибутов, по крайней мере, к одному зарегистрированному аутентификатору, которым обладает и который контролирует пользователь.

Примечание — В отличие от аутентификатора мандат всегда контролируется и поддерживается поставщиком связанных с мандатами услуг (доверенной третьей стороной).

3.8 **официальное свидетельство** (authoritative evidence): Свидетельство, содержащее идентификационный(е) атрибут(ы), управление которыми осуществляет полномочная сторона.

Примечания

1 Это один из типов свидетельств идентичности.

2 Официальное свидетельство для конкретного идентификационного атрибута может быть подтверждающим свидетельством для другого.

3.9 **подтверждающая информация** (proofing information): Информация, собранная для подтверждения идентификационных данных.

3.10 **подтверждающая сторона** (proofing party): Сущность, осуществляющая подтверждение идентификационных данных субъекта.

3.11 **подтверждающее свидетельство** (corroborative evidence): Свидетельство, содержащее идентификационный(е) атрибут(ы), управление которыми не осуществляет полномочная сторона.

Примечания

1 Идентификационные атрибуты в подтверждающем свидетельстве могут не быть такими же актуальными или точными, как в официальном свидетельстве.

2 Это один из типов свидетельств идентичности.

3 Подтверждающее свидетельство для конкретного идентификационного атрибута может быть официальным свидетельством для другого.

3.12 **полномочная сторона** (authoritative party): Сущность, обладающая признанным правом создания или фиксирования идентификационных атрибутов и обязанностью по осуществлению их непосредственного управления.

Примечание — Юрисдикция(и) и/или промышленные круги иногда объявляют сторону полномочной. Возможно, что такая сторона подвергается правовому контролю.

3.13 **свидетельство идентичности** (evidence of identity): Доказательство, обеспечивающее определенную степень уверенности в том, что идентичность действительно соответствует (принадлежит) субъекту.

3.14 **субъект** (subject): Физическое лицо, чьи идентификационные данные подтверждаются.

3.15 **уровень подтверждения идентификационных данных** (level of identity proofing): Достигнутая степень уверенности в подтвержденности идентичности.

4 Концепции подтверждения идентичности

4.1 Подтверждение идентичности

Подтверждение идентичности представляет собой процесс верификации идентификационных атрибутов, вводимых в систему управления идентификационными данными, а также установления того, что идентификационные атрибуты относятся к субъекту, который будет внесен в реестр.

Процесс подтверждения идентичности включает в себя:

- документальное оформление политики подтверждения идентичности, выполняемых процессов и назначенной группы или лица, известных как ответственные разработчики политики подтверждения;
- определение домена подтверждения идентичности, границ и условий, в которых будет осуществляться взаимодействие субъекта и его идентичности;
- определение идентификационных атрибутов, которые нужно собрать и подтвердить;
- определение вспомогательных атрибутов, сбор которых будет осуществляться для выполнения подтверждения идентичности;
- установление уровня подтверждения идентичности, которого требует последующий процесс внесения в реестр;
- реализацию инфраструктуры для осуществления подтверждения идентичности.

Каждый случай подтверждения идентичности включает в себя шаги, направленные на:

- сбор подтверждающей информации;
- определение достоверности собранных идентификационных атрибутов в отношении требований, установленных в разделе 5;
- определение того, что идентификационные атрибуты соответствуют необходимому уровню подтверждения идентичности, который должен быть достигнут;
- привязку (установление связи) заявленных идентификационных атрибутов к субъекту.

4.2 Регистрация (внесение в реестр)

Внесение в реестр представляет собой процесс, посредством которого осуществляется сбор и верификация идентификационной информации, а также ее ввод в систему управления идентификационными данными. При проектировании, реализации и эксплуатации системы подтверждения идентификационных данных следует также учитывать положения ГОСТ Р 59381, ГОСТ Р 59382, а также [1] и [2].

Процесс внесения в реестр должен фиксировать информацию, включая результат подтверждения идентичности.

4.3 Подтверждающая информация

Подтверждающая сторона осуществляет сбор подтверждающей информации, к которой могут относиться как идентификационные атрибуты, так и вспомогательные атрибуты, как приведено в таблице 1. Подтверждающая информация может быть подмножеством информации, необходимой для получения субъектом услуг и/или мандатов.

Таблица 1 — Подтверждающая информация и атрибуты

Типы атрибутов	Объяснение	Примеры атрибутов
Идентификационные атрибуты	Один или несколько атрибутов, которые при их объединении однозначным образом идентифицируют субъекта в данном домене	Псевдоним(ы); имя (имена); дата рождения; место рождения; имя родителя при рождении; биометрические характеристики; адрес(а); номер(а) телефона(ов); адрес(а) электронной почты; время рождения (если известно); национальный идентификационный(е) номер(а)
Вспомогательные атрибуты	Атрибуты, способствующие подтверждению идентичности	Другие имена; взаимоотношения и союзы; номера для ссылок из свидетельства идентичности; уместная информация из представленного свидетельства идентичности

Примечание — Подтверждающая информация не включает в себя атрибуты обладания правом или возможностей. Любая оценка обладания правом или возможностей потенциально ненадежна, если идентификационные данные не подтверждены требуемым уровнем подтверждения идентичности. Характер и точность информации, собранной для определения обладания правом или возможностей (не идентификационных данных) для услуги и/или мандата, выходят за рамки рассмотрения настоящего стандарта.

4.4 Свидетельства идентичности

4.4.1 Общая информация

Свидетельство идентичности используется при подтверждении идентичности для обеспечения уверенности в том, что субъект обладает заявленными идентификационными данными в соответствии с определенным уровнем подтверждения идентичности. Для этого могут использоваться различные каналы, например личное обращение, телефонные каналы связи или аналогичные, обеспечивающие взаимодействие в режиме реального времени. Субъект обращается для получения услуг и/или мандатов, имея определенный уровень подтверждения идентичности. Требования уровней подтверждения идентичности, которые должны выполняться для каждой из целей уровней подтверждения идентификационных данных, определяются в разделе 5.

Свидетельство идентичности может быть официальным либо подтверждающим свидетельством. Свидетельство идентичности обычно включает в себя один или несколько из перечисленных ниже пунктов:

- подтверждающую информацию, предоставляемую субъектом;
- выданное свидетельство, содержащее подтверждающую информацию субъекта или связанное с подтверждающей информацией субъекта;
- базы данных и реестры, содержащие подтверждающую информацию субъекта;
- подтверждающую информацию, предоставленную другими известными источниками.

Любое свидетельство, используемое подтверждающей стороной во время подтверждения идентичности, должно содержать подтверждающую информацию, согласующуюся с информацией заявления и с требованиями, изложенными в разделе 5.

Примечание — Свидетельство идентичности может быть предоставлено в различных видах. Уровень подтверждения идентичности, который может быть достигнут, может зависеть от предоставленного вида.

4.4.2 Официальные свидетельства

Субъект может использовать различные идентификационные атрибуты для создания идентификационных данных в различных доменах. Для каждого из идентификационных атрибутов могут быть доступны официальные свидетельства. Идентификационные атрибуты, содержащиеся в данных свидетельствах, при условии их подлинности, считаются правильными и достоверными. При этом официальные свидетельства считаются основой для установления идентичности (т. е. первого подтверждения идентичности, которому подвергается физическое лицо) и/или контролируются законодательством.

4.4.3 Подтверждающие свидетельства

В случаях, когда подтверждающая сторона не имеет доступа к официальным свидетельствам для идентификационного атрибута (или не нуждается в них для требуемого уровня подтверждения идентификационных данных), остаточный риск может быть уменьшен путем верификации подтверждающих свидетельств. Если подтверждающие свидетельства хранят идентификационные атрибуты из официальных свидетельств, атрибуты не признаются в качестве официальных.

4.5 Действующие субъекты

4.5.1 Общая информация

Проверка свидетельства идентичности должна осуществляться с учетом взаимосвязей между субъектом, подтверждающей стороной и, потенциально, верифицирующей стороной. Свидетельство идентичности играет определяющую роль в этом процессе.

4.5.2 Субъект

Субъект или иной заявитель обращается с заявлением о прохождении субъектом подтверждения идентичности подтверждающей стороной. Заявление может быть сделано субъектом заявления либо лицом, действующим от его имени. Для субъекта будет проведено подтверждение идентификационных данных подтверждающей стороной.

4.5.3 Подтверждающая сторона

Подтверждающая сторона устанавливает достоверность заявленных идентификационных атрибутов субъекта в соответствии с требуемым уровнем подтверждения идентичности. Верификация идентификационной информации осуществляется в отношении свидетельства идентичности для каждого идентификационного атрибута.

Подтверждающая сторона делает выбор:

- изучать свидетельство идентичности, содержащее идентификационные атрибуты, и для каждого атрибута определять, принимать ли атрибут;
- либо верифицировать представленные идентификационные атрибуты с помощью поставщика услуг, имеющего санкционированный доступ к свидетельствам для этой цели. Поставщик услуг предоставляет ответ подтверждающей стороне.

Подтверждающая сторона, проводящая верификацию идентификационных данных, полагается на точность и достоверность подтверждающей информации в свидетельстве идентичности, к которому она обращается.

4.5.4 Верификатор

Верификатор — это объект, система, устройство или программное обеспечение, имеющие возможность сформулировать ответ на запрос проверяющей стороны. Верификатором может быть орган идентификационной информации или другие сущности, контролирующие доказательства идентичности. Субъект сам может быть верификатором, если может предоставить доказательства для ответа.

Ответ, предоставленный верификатором, не обязательно включает в себя официальное свидетельство идентичности, но может являться подтверждающей информацией, которая позволит проверяющей стороне вынести решение о том, произошла ли успешная проверка.

4.6 Сила свидетельств идентичности

Если событие подтверждения идентичности не является первоначальным установлением идентичности субъекта, некоторые свидетельства (документы, цифровые идентификационные данные и т. д.) могут быть результатом более раннего формального процесса подтверждения идентичности. Регистрация рождения является примером первоначального события, где отсутствуют предшествующие мероприятия подтверждения идентичности субъекта.

Подтверждающая сторона должна оценить предшествующее событие подтверждения идентичности с целью определения степени возможного принятия свидетельства для текущего события подтверждения идентичности и уровня подтверждения идентификационных данных, а также любого дальнейшего подтверждения идентичности, которое может быть необходимо.

Не все выпущенные свидетельства идентичности могут быть использованы для последующего подтверждения идентификационных данных вне домена их происхождения. Свидетельство может не содержать какую-либо подтверждающую информацию и/или может быть не связано с внешне доступной подтверждающей информацией. Представленные в качестве свидетельства идентичности физические документы могут включать в себя функции защиты от подделки и фальсификации. Там, где это

уместно и осуществимо, верификация идентификационной информации в физическом свидетельстве идентичности включает в себя проверку функций защиты от подделки и фальсификации. Электронные формы свидетельств идентичности могут быть получены таким способом, который позволяет обнаруживать фальсификацию и подделку.

Силу свидетельств определяют следующие три аспекта:

- предпринятое исходное подтверждение идентификационных данных;
- качество и надежность мер защиты для предотвращения подделки, фальсификации и подлога;
- процесс, использованный для их выпуска.

Количество требуемых свидетельств зависит от способности свидетельств идентичности отвечать целям подтверждения идентичности. В случаях, когда требуется несколько свидетельств, можно достичь дополнительного уровня достоверности идентичности, собирая свидетельства идентичности из всей жизни субъекта.

4.7 Уровни подтверждения идентичности

Уровень подтверждения идентичности для практического применения основан на степени выполнения целей подтверждения идентичности. Целевой уровень подтверждения идентификационных данных будет определяться путем связанной с идентификационными данными оценкой риска последующей предоставляемой услуги и/или мандата. Оценка риска проводится организацией, предоставляющей услугу и/или мандат, и может способствовать проектированию и реализации функции подтверждения идентичности подтверждающей стороной.

В таблице 2 приведены уровни подтверждения идентичности и цели, представляющие значимость каждого из них.

Примечание — С возрастанием уровня подтверждения идентичности требования к процессам для достижения некоторых целей становятся более строгими, как определено в разделе 5.

Таблица 2 — Уровни подтверждения идентичности

Уровень подтверждения идентичности	Описание	Цель
1-й уровень подтверждения идентичности	Низкая уверенность в заявленных или предъявленных идентификационных данных	Идентификационные данные являются уникальными в данном домене, и имеется предположение о существовании идентификационных данных, и субъект предположительно привязан к идентификационным данным
2-й уровень подтверждения идентичности	Средняя уверенность в заявленных или предъявленных идентификационных данных	Идентификационные данные являются уникальными в данном домене, и умеренное установление существования идентификационных данных[1)], и у субъекта есть некоторая привязка к идентификационным данным
3-й уровень подтверждения идентичности	Высокая уверенность в заявленных или предъявленных идентификационных данных	Идентификационные данные являются уникальными в данном домене, и строгое установление существования идентификационных данных[1)], и у субъекта есть значительная привязка к идентификационным данным

[1)] Понятие требует совпадения значений идентификационного атрибута со значениями идентификационного атрибута, указанного в свидетельствах идентичности.

Конкретные реализации процессов подтверждения идентичности будут различаться в зависимости от политики и свидетельств идентичности, доступных для субъекта и подтверждающей стороны. На уровень подтверждения идентификационных данных, который может быть достигнут, будут оказывать влияние надежность и точность свидетельств. В случаях чрезмерного риска, связанного с идентификационными данными, подтверждающая сторона может подтверждать идентификационные данные несколькими способами.

Уровень подтверждения идентификационных данных представляет собой один из элементов, способствующих общему уровню доверия при аутентификации сущности.

Примечание — Подробная информация об уровнях доверия содержится в ГОСТ Р 58833—2020 (см. раздел 7).

Требования к уровню подтверждения идентичности определяет сущность, регулирующая последующие процессы, например внесение в реестр или управление мандатами. Это делается для того, чтобы гарантировать, что связанные с этим риски оценены и соответственно снижены с целью устранения как рисков, связанных с принятием решения о признании идентичности, так и рисков, присущих функционированию услуги.

4.8 Уникальная идентичность на каждого субъекта

В зависимости от цели, для которой осуществляется подтверждение идентичности, может быть необходимым обеспечить уверенность в том, что каждый субъект зарегистрирован только один раз, т. е. каждое физическое лицо имеет уникальную идентичность (набор идентификационных данных) в этом домене.

Для достижения этой цели применимы следующие меры:

- требование документов или информации из официальных свидетельств, которые, как известно, являются единственными для каждого физического лица;
- сравнение биометрического образца субъекта с другими биометрическими образцами в контексте обнаружения и предотвращения дублирования. Собранная биометрическая информация должна быть достаточной и эффективной для исключения дублирования идентификационных данных.

Подтверждающей стороне следует учитывать, является ли субъект живым или покойным. Этот факт необходимо проверять при обнаружении попыток повторного использования идентификационных данных умерших лиц. Если проверка необходима, то для выполнения этой задачи следует использовать верификацию с помощью официальных свидетельств.

В случаях, если определено, что субъект является усопшим, но регистрация (внесение в реестр) все же требуется, соответствующие части подтверждения идентичности должны осуществлять верификацию легитимности заявления и самого заявителя.

5 Требования к подтверждению идентичности

5.1 Политика подтверждения идентичности

Подтверждающая сторона должна осуществлять подтверждение идентичности в соответствии с документально оформленной политикой подтверждения идентичности.

Политика подтверждения идентичности как минимум должна определять:

- уровень(и) подтверждения идентичности, на котором предлагается услуга подтверждения идентичности;
- юрисдикцию, в которой действует и предлагается услуга подтверждения идентичности, и применимое законодательство;
- домен, для которого предпринимается подтверждение идентичности;
- является ли подтверждение идентичности личным или удаленным;
- какие идентификационные атрибуты заявителей требуется предоставлять;
- какие свидетельства идентичности (официальные или подтверждающие) для идентификационных атрибутов должны использоваться при верификации подтверждающей информации;
- каковы возможные результаты операций подтверждения идентичности;
- как результаты процесса подтверждения будут сообщаться заявителю или соответствующим сторонам;

- какие записи о процессах подтверждения будут сохраняться, кем и в течение какого времени, как определено разработчиком политики.

Разработчик политики подтверждения идентичности подтверждающей стороны должен опубликовать политику подтверждения идентичности. В случае публикации документация политики подтверждения идентичности должна содержать дату утверждения.

5.2 Определение уровня подтверждения идентичности

Для обеспечения уверенности в достоверности идентификационных данных на требуемом уровне подтверждения идентичности следует успешно подтвердить существование идентификационных данных и осуществить привязку идентификационных данных к субъекту на уровне подтверждения, соответствующем требуемому. Подтверждение идентификационных данных требует, чтобы каждые идентификационные данные были уникальными в своем домене (в соответствии с 5.3).

В таблице 3 показано, как определяется результирующий уровень подтверждения идентичности.

Таблица 3 — Определение уровня подтверждения идентичности

Привязка идентификационных данных	Существование идентификационных данных		
	Идентификационные данные существуют на 1-м уровне подтверждения идентичности	Идентификационные данные существуют на 2-м уровне подтверждения идентичности	Идентификационные данные существуют на 3-м уровне подтверждения идентичности
Идентификационные данные привязаны на 1-м уровне подтверждения идентичности	1-й уровень подтверждения идентификационных данных	1-й уровень подтверждения идентификационных данных	1-й уровень подтверждения идентификационных данных
Идентификационные данные привязаны на 2-м уровне подтверждения идентичности	1-й уровень подтверждения идентификационных данных	2-й уровень подтверждения идентификационных данных	2-й уровень подтверждения идентификационных данных
Идентификационные данные привязаны на 3-м уровне подтверждения идентичности	1-й уровень подтверждения идентичности	2-й уровень подтверждения идентичности	3-й уровень подтверждения идентичности

5.3 Уникальность идентичности

Подтверждающая сторона должна проверять предоставляемые субъектом идентификационные атрибуты, чтобы оценивать факт дублирования и идентификационных атрибутов, управление которыми уже осуществляется для других субъектов в данном домене. Любой обнаруженный факт дублирования будет разрешаться в соответствии с политикой подтверждения идентичности. В таблице 4 приведены требования к уровню подтверждения идентичности относительно ее уникальности.

Примечание — Дублирование идентичности может определяться либо как полное дублирование всех атрибутов, либо как дублирование части атрибутов. Политика подтверждения идентификационных данных должна определять идентификационные атрибуты, например тип и число, которых, вероятно, достаточно для уникальности. Если обнаруживается, что первоначально предоставленные идентификационные данные не являются уникальными либо подтверждение идентичности выполнено с отрицательным результатом, то необходимо получить дополнительную информацию от субъекта. Политика подтверждения идентичности указывает, какие дополнительные атрибуты следует получать или генерировать, если таковые имеются.

Таблица 4 — Требования к уровню подтверждения идентичности относительно ее уникальности

Цель	1-й уровень подтверждения идентичности	2-й уровень подтверждения идентичности	3-й уровень подтверждения идентичности
Идентификационные данные являются уникальными	Идентификационные данные в данном домене должны быть проверены на предмет дублирования	То же, что на 1-м уровне подтверждения идентичности	То же, что на 1-м уровне подтверждения идентичности

5.4 Существование идентичности

Для 1-го уровня подтверждения идентичности подтверждающая сторона должна принимать идентификационные данные такими, как они предоставляются, не осуществляя никакой проверки. Для 2-го уровня подтверждения идентичности подтверждающая сторона должна проверять существование идентификационных данных в подтверждающих свидетельствах; для 3-го уровня подтверждения идентичности подтверждающая сторона должна проверять существование идентификационных данных в официальных свидетельствах.

Если на 2-м и 3-м уровнях подтверждения идентичности идентификационные данные не могут быть подтверждены в свидетельстве идентичности, подтверждающая сторона должна применять документально оформленный процесс особых ситуаций согласно политике подтверждения, чтобы попытаться определить существование идентичности. Такие меры в процессе особых ситуаций должны быть пропорциональны уровню подтверждения идентичности и должны принимать во внимание усилия, требуемые для их выполнения, в сравнении с прекращением рассмотрения заявления. Когда такие проверки не являются убедительными, рассмотрение заявления должно быть в любом случае прекращено.

В таблице 5 приведены требования к уровню подтверждения идентичности относительно существования идентичности, подтвержденного в свидетельствах.

Таблица 5 — Требования к уровню подтверждения идентичности относительно существования идентичности, подтвержденного в свидетельствах

Цель	1-й уровень подтверждения идентичности	2-й уровень подтверждения идентичности	3-й уровень подтверждения идентичности
Существование идентичности в свидетельствах	Существование идентификационных атрибутов в свидетельствах идентичности не проверяется	Подтверждающая сторона должна верифицировать существование идентификационных атрибутов в подтверждающих свидетельствах	Подтверждающая сторона должна верифицировать существование идентификационных атрибутов в официальных свидетельствах

В случаях, когда для подтверждения идентичности требуются дополнительные вспомогательные атрибуты, подтверждающая сторона должна их верифицировать. Этот процесс должен давать информацию либо о достоверной верификации, либо о неуспешной верификации (которая также включает в себя информацию о несоответствиях).

Примечание — Информация о силе свидетельств идентичности содержится в 4.6. Более подробная информация о процессах верификации и обнаружении мошенничества содержится в приложении А.

5.5 Привязка идентичности к субъекту

Для 1-го уровня подтверждения идентичности подтверждающая сторона должна признавать привязку субъекта к идентификационным данным, не осуществляя никакой проверки. Для 2-го и более высокого уровня подтверждения идентичности подтверждающая сторона должна установить привязку субъекта к идентификационным данным. Точность идентификационных данных не означает, что субъект представлен этими идентификационными данными или связан с ними. Например, физическое лицо может предъявлять идентификационные данные кого-то другого.

Если на 2-м и более высоком уровне подтверждения идентичности субъект не может быть привязан к идентификационным данным, подтверждающая сторона должна применять документально оформленный процесс особых ситуаций согласно политике подтверждения. Такие меры в процессе особых ситуаций должны быть пропорциональны уровню подтверждения идентичности.

Требования к уровню подтверждения идентичности относительно привязки идентичности к субъекту приведены в таблице 6.

Настоящий стандарт определяет применение следующих механизмов привязки идентификационной информации с использованием в качестве «факторов»:

- знание: привязка устанавливается для субъекта с использованием информации, не являющейся общедоступными сведениями. Привязка может включать верификацию относительно свидетельств идентичности, отличных от предоставленных свидетельств;

- владение: привязка устанавливается для субъекта, представляющего физические свидетельства, содержащие идентификационную информацию, которая будет верифицироваться относительно свидетельства идентичности.

- биометрия: привязка устанавливается путем сопоставления биологической или поведенческой характеристики, наблюдаемой подтверждающей стороной, с эталонной биометрической информацией, которая, как известно, соответствует субъекту. Привязка может включать технологию автоматического распознания или ручное сравнение (например, осуществляемое вручную сравнение лица с фотографией или осуществляемое вручную квалифицированным экспертом сравнение отпечатков пальцев с эталонными отпечатками пальцев) со свидетельством идентичности.

Таблица 6 — Требования к уровню подтверждения идентичности относительно привязки идентичности к субъекту

Цель	1-й уровень подтверждения идентичности	2-й уровень подтверждения идентичности	3-й уровень подтверждения идентичности
Идентичность привязана к субъекту	Привязка к идентификационным данным не проверяется	Подтверждающая сторона должна проверять привязку к идентификационным данным, используя один фактор	Подтверждающая сторона должна проверять привязку к идентификационным данным, используя два или более факторов

Примечание — Информация о силе свидетельств идентичности содержится в 4.6.

Подтверждающая сторона должна включать в свою оценку риска рассмотрение атак выдачи одного физического лица за другое физическое лицо и применять защитные меры для снижения соответствующих рисков до приемлемого уровня.

Примечание — Привязка идентичности к субъекту явным образом не упоминается в [1], но существует требование снижения вероятности кражи идентификационной информации и выдачи одного физического лица за другое физическое лицо.

Приложение А
(справочное)

Несоответствия в идентичности и обнаружение мошенничества

А.1 Введение

Свидетельство для подтверждения идентичности может быть физическим и нефизическим.

Источниками для выявления несоответствий в идентичности могут выступать правоохранительные органы, а также источники известных подделанных или похищенных свидетельств идентичности.

А.2 Выявление несоответствий в свидетельствах идентичности

В случае использования свидетельства идентичности в нем могут быть представлены действительные и ложные элементы. В таблице А.1 приведены категории установления того, является ли свидетельство истинным или ложным.

Таблица А.1 — Результаты проверок свидетельств идентичности

Выполняемые проверки и объекты контроля	Свидетельство идентичности			
	Действительное	Похищенное/проданное	Фальсифицированное	Поддельное/фальшивое
Идентификационные данные	Действительные	Действительные	Действительные или ложные[1)]	Действительные или ложные[2)]
Проверка физических свидетельств	Пройдена	Пройдена	Не пройдена	Не пройдена
Привязка к субъекту	Пройдена	Не пройдена	Пройдена	Пройдена
Верификация совместно с выдающей стороной	Пройдена	Пройдена или не пройдена[3)]	Не пройдена	Пройдена или не пройдена[4), 5)]
Подтверждение	Пройдено	Вероятно, слабое	Вероятно, слабое	Вероятно, слабое

[1)] Фальсифицированное не означает, что идентификационные данные неверны, может быть так, что в свидетельство вставлены подлинные идентификационные данные.

[2)] Поддельное или фальшивое свидетельство может содержать действительную или ложную идентификационную информацию. Действительная информация будет давать результат «пройдено» при верификации.

[3)] Где это возможно, должна проводиться верификация совместно с выдающей стороной за национальными границами.

[4)] Зависит от того, сообщалось ли о пропаже свидетельства.

[5)] Если существует двойник, то в обращении находятся два варианта одного и того же свидетельства: одно действительное, другое поддельное. Верификация совместно с выдающей стороной будет показывать результат «пройдено», пока не будет обнаружен подлог и не будут приняты меры. Этот риск может уменьшить криптографическая привязка свидетельства.

Физическая проверка свидетельства включает в себя:

а) проверку всей информации в заявлении в отношении свидетельств упущений, ошибок и противоречий;

б) проверку каждого элемента на предмет его физической структуры, качества материала, качества печати, функций защиты, печатей и подписей. Этим можно выявить:

1) любые признаки фальсификации (в случае, если подлинный элемент был изменен), например внесены изменения в фотографии или напечатанные данные, или документ разобран и собран заново, или страницы не синхронизируются (например, в паспорте),

2) любые признаки поддельного или фальшивого документа. Многие элементы имеют функции защиты, которые трудно подделать, и требуются экспертные знания или специальные аппараты для обнаружения подделок. Проверки без таких навыков и аппаратов, вероятно, не смогут обнаружить поддельный элемент свидетельств;

в) проверки должны осуществлять квалифицированные специалисты, обладающие навыками, инструментальными средствами и способностями обнаружения поддельных или фальсифицированных свидетельств.

А.3 Выявление несоответствий при верификации

Во время процесса верификации проверка подтверждающей информации может основываться на определенных предоставляемых свидетельствах или механизме самозаявления. В любом случае противоположные показания могут включать в себя:

а) полностью противоречивую информацию, представленную в заявлении или свидетельстве;

б) частично противоречивую информацию, представленную в заявлении или свидетельстве. Это может быть указанием на ошибки клавиатурного ввода или такие события, как смена фамилии, которые должны быть исключены, прежде чем трактовать их как потенциальное мошенничество;

в) ответ верификации, указывающий на существование сообщения о потере или хищении свидетельства:

1) ответ верификации, указывающий на отсутствие у свидетельства активного статуса (например, приостановлено, утратило силу с истечением срока, аннулировано и т. д.).

2) другие факторы (например, геолокация, время и т. д.).

А.4 Биометрическое распознавание

Для обеспечения уверенности в уникальности идентичности субъектов, зарегистрированных в данном домене, и подлинности субъектов, осуществляющих транзакции в данном домене, могут быть получены и сохранены биометрические данные. Во время подтверждения идентичности могут быть рассмотрены биометрические данные в источнике идентификационных данных с целью обнаружения попыток субъекта сделать заявки на множественные регистрации с различными идентификационными данными или сделать заявку на регистрацию с идентификационными данными другого субъекта.

Биометрическая аутентификация обычно включает в себя сравнение вида «один к одному», полученного от субъекта биометрического образца с хранящимся биометрическим эталоном для заявленных субъектом идентификационных данных. Обнаружение множественных попыток регистрации требует поиска вида «один — множество» для базы данных регистрации, сравнивая полученный от субъекта биометрический образец с биометрическими эталонами всех предыдущих регистраций субъекта. Поиски вида «один — множество» накладывают более строгие требования на точность используемой биометрической технологии и могут требовать использования многих биометрических образцов или модальностей.

В случаях, когда культурные особенности затрудняют сбор и подтверждение определенных биометрических характеристик, могут быть рассмотрены альтернативные биометрические и небиометрические варианты. Полагающаяся сторона и правовые требования могут быть такими, что для достижения доверия необходим компромисс с культурными особенностями.

Биометрическое распознавание, как и другие технологии распознавания и верификации, может подвергаться ошибкам. В случае биометрических данных ошибки распознавания бывают двух форм: ошибочное совпадение (когда субъект ошибочно распознается как кто-то другой) и ошибочное несовпадение (когда распознавание субъекта заканчивается неудачей). Последнее применимо только в том случае, если субъект зарегистрирован и, соответственно, может быть распознан. Следует отметить, что возможны презентационные атаки на биометрический продукт, используемый в системе.

Биометрическое распознавание не может использоваться изолированно или вместо верификации других идентификационных атрибутов. Любые противоположные показания, вызванные несовпадением, будут исследованы специалистами в сфере биометрического сравнения прежде, чем будут направлены для расследования мошенничества в отношении идентификационных данных.

А.5 Собеседование

Собеседование обычно проводится в личном присутствии и осуществляется по трем причинам:

- чтобы исключить возможность мошенничества среди заявителей;
- чтобы выявить аномальное поведение;
- чтобы осуществить привязку субъекта к заявленным идентификационным данным и поддерживающему свидетельству идентичности.

Процедуры собеседования будут зависеть от национальных норм защиты данных и предписаний соответственной страны.

Методы собеседования должны быть достаточными для удовлетворения трем вышеуказанным причинам помимо разумных сомнений. В данном разделе представлено руководство по типовым методам передовой практики в этой сфере. Когда собеседование проводится удаленным образом, важно, чтобы действия субъекта были независимым образом засвидетельствованы и зафиксированы для целей собеседования, либо от субъекта требуется осуществление потокового видео с места действия. Потоковое видео с места действия включает в себя установление видеосвязи между лицом, проводящим опрос, и субъектом; затем опрашивающее лицо просит субъекта выполнить серию действий, приводящих к получению видео с места действия, которое можно сравнивать с известными изображениями.

Взаимодействие в режиме реального времени между субъектом и опрашивающим лицом, представляющим услугу подтверждения идентификационных данных, можно использовать как средство верификации и осуществления привязки идентификационных данных к субъекту, если существуют какие-либо подозрения относительно

достоверности свидетельства или заявления. Собеседование с субъектом предоставит возможность исследовать привязку субъекта к заявленным идентификационным данным. Опрос субъекта о подробностях заявления и любых потенциальных расхождениях между представленными свидетельствами и заявлением должен дать ответы, которые могут помочь в подтверждении или отрицании привязки. Это может происходить в результате использования дополнительной подтверждающей информации, предоставленной субъектом, или на основании оценки поведения субъекта во время собеседования.

Персональная верификация может происходить удаленно или на месте, в зависимости от подозрений или требующих верификации свидетельств.

Опрашивающее лицо должно:

- быть компетентным в сфере соответствующих методов проведения собеседования;
- быть компетентным в сфере соответствующих методов проверки документов;
- использовать соответствующее оборудование для проверки документов;
- использовать информацию, не являющуюся общедоступной и известную, по-видимому, только истинному субъекту, для установления привязки субъекта к идентификационным данным;
- осуществлять взаимодействие в среде и условиях, которых требует национальное законодательство.

Для идентификации мошеннических заявлений опрашивающее лицо должно:

- использовать информацию из заявления и других источников (например, банков) для поддержки опроса;
- опрашивать заявителя об информации, содержащейся в поддерживающих документах, и там, где это возможно, взаимосвязанной информации, известной подтверждающей стороне, которой нет в документах (например, информация о банковском счете, связанном с представленным для поддержки заявления счетом за коммунальные услуги);
- регулировать свои методы и задавать одни и те же вопросы в разные моменты собеседования и разными способами для обеспечения непредсказуемости опроса;
- задавать вопросы о семейных отношениях, событиях прошлого и перемещениях, а также о ключевых жизненных событиях;
- оценивать поведение субъекта. В некоторых случаях личное собеседование является очень эффективным для сдерживания мошенничества. Для обеспечения учета и достоверности процесса подтверждения идентичности опросы могут быть засвидетельствованы или записаны на видео с четкой аудио- и видеозаписью, позволяющей однозначным образом идентифицировать субъекта;
- обеспечивать более тщательное сравнение физической внешности субъекта с фотоизображением для установления любых несоответствий. Это может также включать оценивание других физических характеристик.

Другие аспекты собеседования, которые могут оказывать положительное или отрицательное воздействие на способность обнаружения мошенничества, включают в себя следующее:

а) опрашиваемый субъект обычно не может иметь сопровождение;

б) случаи, когда требуется перевод (подтверждающая сторона может предоставить переводчика для увеличения достоверности);

в) случаи, когда заявитель не способен общаться в связи с физической или умственной недееспособностью и приходит с представителем, обеспечивающим уход (подтверждающая сторона может также предоставить квалифицированное лицо, обеспечивающее уход, или медицинский персонал для обеспечения уверенности в том, что собеседование осуществляется корректным образом, без предубеждения или нанесения ущерба здоровью заявителя). В таких обстоятельствах собеседование должно проводиться в личном присутствии, а не удаленно;

г) в случае наличия культурных особенностей могут быть приняты меры для удовлетворения таких потребностей, как обеспечение приватности, проведение собеседования и сбора биометрических данных лицами того же пола;

д) в случае собеседования с несовершеннолетними (как определено в национальном законодательстве) необходимо сопровождение представителя (как определено национальным законодательством);

е) если собеседование осуществляется удаленным образом:

1) будет осуществляться достаточный дополнительный мониторинг доверенными лицами и/или надежными системами наблюдения и видеозапись для предотвращения мошенничества или искажения фактов,

2) до собеседования могут проводиться дополнительные верификационные проверки для установления степени риска, связанного с заявителем, и вероятности того, что он может попытаться «подорвать» собеседование. Если такой риск велик, должно происходить собеседование в личном присутствии.

Если в конце собеседования опрашивающее лицо предполагает, что не все требования в полной мере удовлетворены, и/или заявление не содержит достаточной информации, то оно должно направить заявление на дальнейшее рассмотрение.

Библиография

[1] ISO/IEC 24760-2:2015 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 2. Базовая архитектура и требования (Information technology — Security techniques — A framework for identity management — Part 2: Reference architecture and requirements)

[2] ISO/IEC 29115:2013 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к аутентификации сущности (Information technology — Security techniques — Entity authentication assurance framework)

УДК 006.34:004.056:004.056.5:004.056.53:006.354 ОКС 35.030

Ключевые слова: атрибут, идентификатор, идентификационная информация, идентификационный атрибут, идентификация, идентификационные данные, подтверждение идентичности

Технический редактор *В.Н. Прусакова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 24.05.2021. Подписано в печать 28.05.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 2,10.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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