ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59381— 2021

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Основы управления идентичностью

Часть 1

Терминология и концепции

(ISO/IEC 24760-1:2019, NEQ)

Издание официальное

Москва
Стандартинформ
2021

gost.e-ecolog.ru

Предисловие

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

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. № 413-ст

4 Настоящий стандарт разработан с учетом основных нормативных положений международного стандарта ИСО/МЭК 24760-1:2019 «Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 1. Терминология и концепции» (ISO/IEC 24760-1:2019 «Information technology. Security techniques — A framework for identity management — Part 1: Terminology and concepts», NEQ)

5 ВВЕДЕН ВПЕРВЫЕ

*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 (*gost.e-ecolog.ru

© Стандартинформ, оформление, 2021

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

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Идентичность 7
4.1 Общие положения 7
4.2 Идентификационная информация 7
4.3 Идентификатор 8
4.4 Мандат 8
5 Атрибуты 10
5.1 Общие положения 10
5.2 Виды атрибутов 10
5.3 Домен происхождения 10
6 Управление идентичностью 11
6.1 Общие положения 11
6.2 Жизненный цикл идентичности 11
7 Идентификация 13
7.1 Общие положения 13
7.2 Верификация 14
7.3 Внесение в реестр 14
7.4 Регистрация 14
7.5 Подтверждение идентичности 15
8 Аутентификация 16
9 Поддержка 16
10 Реализация 16
11 Обеспечение конфиденциальности персональных данных 17
Библиография 18

Введение

Для функционирования автоматизированных (информационных) систем необходимо собирать и формировать информацию о пользователях, связанными с ними программном обеспечении или оборудовании и принимать решения на основе данной информации. Такие решения, основанные на данных пользователей, могут касаться доступа к приложениям или другим ресурсам.

Для эффективного внедрения и эксплуатации систем, принимающих решения на основе идентификации, комплекс стандартов по основам управления идентичностью определяет общие правила формирования, администрирования и использования данных, помогающих характеризовать физических лиц, организации или компоненты информационной технологии.

Для многих организаций управление идентификационными данными является критичным для обеспечения безопасности процессов организации. Одновременно надлежащее управление важно для защиты персональных данных пользователей.

Комплекс стандартов по основам управления идентичностью определяет базовые концепции управления идентичностью, которое имеет целью обеспечение соответствия между сущностью и набором относящихся к ней идентификационных данных. Степень достижения указанной цели влияет на уверенность в результатах идентификации и аутентификации сущности как субъекта или объекта доступа и, как следствие, определяет корректность управления доступом.

Настоящий стандарт необходимо применять с учетом требований нормативных правовых актов и стандартов Российской Федерации в области защиты информации.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Основы управления идентичностью

Часть 1

Терминология и концепции

Information technology. Security techniques. A framework for identity management.
Part 1. Terminology and concepts

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт определяет термины, относящиеся к управлению идентичностью, основные концепции идентичности и управления идентичностью, а также их взаимосвязь.

Положения настоящего стандарта применимы для любой информационной системы, обрабатывающей идентификационную информацию, и используются совместно с документами по стандартизации, регламентирующими вопросы идентификации.

Настоящий стандарт предназначен для применения путем включения нормативных ссылок на него в соответствии с действующим законодательством и (или) прямого использования устанавливаемых в нем положений.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

ГОСТ Р 59407—2021 Информационная технология. Методы и средства обеспечения безопасности. Базовая архитектура защиты персональных данных

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую 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.

Издание официальное

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **атрибут** (attribute): Характеристика, признак или свойство сущности.

Пример — Возможными атрибутами являются вид сущности, адрес, номер телефона, привилегия, MAC-адрес, имя домена.

3.2 **аутентификация** (authentication): Формализованный процесс верификации, который в случае успеха приводит к подтвержденной (аутентифицированной) идентичности сущности.

Примечания

1 Процесс аутентификации включает в себя проверку верификатором одного или нескольких идентификационных атрибутов, предоставленных субъектом, чтобы определить их достоверность с требуемым уровнем доверия.

2 Аутентификация обычно включает в себя применение политики для достижения требуемого уровня доверия для результата.

3.3 **верификатор** (verifier): Сущность, осуществляющая верификацию.

Примечание — Верификатор может быть той же сущностью или действовать от имени сущности, которая контролирует идентификацию сущностей в конкретном домене.

3.4 **верификация** (verification): Процесс проверки того, что представленные (заявленные) идентификационные данные, связанные с конкретной сущностью, достоверны.

Примечание — Проверка, как правило, включает в себя определение атрибутов, необходимых для распознавания сущности в домене, проверку наличия этих обязательных атрибутов, их правильного синтаксиса, существования в течение определенного периода действия и принадлежности к сущности.

3.5 **внесение в реестр идентичностей** (enrolment): Процесс, в результаты выполнения которого сущность становится известной и учтена в конкретном домене.

Примечание — Внесение в реестр идентичностей обычно включает сбор и проверку идентификационных данных, а также регистрацию идентификационной информации.

3.6 **генератор ссылочных идентификаторов** (reference-identifier generator): Инструментальное средство, используемое при внесении в реестр идентичностей для обеспечения актуального уникального значения для ссылочного идентификатора.

Пример — Система управления базой данных может быть генератором ссылочных идентификаторов, когда она присваивает уникальный номер записи добавляемой в таблицу новой записи и этот номер записи используется как ссылочный идентификатор.

3.7 **полагающаяся сторона** (relying party): Сущность, полагающаяся на проверку идентификационной информации конкретной сущности.

Примечание — Полагающаяся сторона подвергается риску, вызванному неверной идентификационной информацией. Обычно ее связывают доверительные отношения с одним или более органами, предоставляющими идентификационную информацию, необходимую для идентификации субъекта.

3.8 **домен применения (домен)** (domain of applicability): Среда, в которой сущность может использовать набор атрибутов для идентификации и других целей.

Примечание — В общем случае идентичность определяется по отношению к набору атрибутов в конкретном домене.

Пример — Развернутая организацией ИТ-система, позволяющая пользователям регистрироваться, является доменом для зарегистрированного пользовательского имени.

3.9 **домен происхождения** (domain of origin): Домен, в котором было создано значение идентификационного атрибута или которому было присвоено (повторно) его значение.

Примечания

1 Домен происхождения может быть предоставлен в качестве метаданных для атрибута.

2 Домен происхождения обычно определяет значение и формат значения атрибута.

3 Атрибут может содержать явное значение, которое ссылается на домен происхождения. Например, код страны для номера паспорта в качестве ссылки на страну выдачи, являющейся доменом происхождения идентификационной информации в паспорте.

4 Операционно домен происхождения может быть доступен в качестве источника для атрибута (иногда известного как центр выдачи атрибутов). Источник выдачи атрибутов может работать за пределами фактического домена происхождения. Для одного и того же домена происхождения может существовать несколько центров выдачи атрибутов.

Пример — Домен происхождения номера членства в клубе — это конкретный клуб, присвоивший этот номер.

3.10 **идентификационные данные** (identity data): Совокупность идентификационных атрибутов и их значений, которая связана с конкретной сущностью.

3.11 **идентификационная информация** (identity information): Совокупность значений идентификационных 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.

3.12 **идентификационное утверждение** (identity assertion): Заявление органа идентификационной информации, используемое полагающейся стороной для аутентификации.

Примечание — Идентификационное утверждение может быть криптографическим подтверждением успешной аутентификации, созданным с помощью алгоритмов и ключей, согласованных между сторонами, например, в объединении идентификационных атрибутов.

3.13 **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.

3.14 **кратковременный идентификатор** (ephemeral identifier): Идентификатор с ограниченным сроком действия.

Примечания

1 Как правило, эфемерный идентификатор предоставляется субъекту в качестве криптографического удостоверения личности.

2 Как правило, эфемерный идентификатор может быть проверен только в домене, который его создал, а также в доменах, объединенных с этим доменом.

3.15 **мандат** (credential): Отображение идентичности для цели аутентификации.

Примечания

1 Мандат удостоверяет права и полномочия предъявителя.

2 Мандаты, как правило, создаются для проверки подлинности идентификационной информации, относящейся к сущности, которую она представляет.

3 Идентификационная информация, представленная мандатом, может быть, например, напечатана на удобочитаемом носителе или сохранена в физическом токене.

4 Мандат может быть представлен в виде имени сущности, именем с паролем, PIN-кодом, смарт-картой и т. д.

3.16 **минимальное раскрытие** (minimal disclosure): Принцип управления идентичностью, при котором запрос или передача идентификационной информации третьей стороне ограничивается минимальным набором данных, которые необходимы для конкретной цели.

Примечание — С минимальным раскрытием связан принцип пропорциональности — насколько вмешательство контроля разумно по отношению к деятельности.

3.17 **объединение идентичностей** (identity federation): Соглашение между двумя или более доменами, определяющее, как будет осуществляться обмен и управление идентификационной информацией между доменами.

Примечания

1 Создание объединения идентичностей обычно включает соглашение об использовании общих протоколов и процедур обеспечения конфиденциальности данных, включая защиту персональных данных, и аудита. Соглашение об объединении может определять использование стандартизированных форматов данных и криптографических методов.

2 Соглашение об объединении может быть основой для органов идентификации в каждом из доменов для взаимного признания полномочий на авторизацию.

3.18 **объединенная идентичность** (federated identity): Идентификационные атрибуты для использования во многих доменах.

Примечания

1 Некоторые или все домены, в которых может использоваться объединенная идентичность, могут быть формально представлены в качестве объединения идентичностей. Поставщики идентификационной информации доменов в объединении могут совместно управлять объединенной идентичностью.

2 Объединенная идентичность может быть постоянной или временной.

3.19 **орган идентификационной информации** (identity information authority): Связанная с конкретным доменом сущность, которая может делать доказуемые утверждения о действенности и (или) правильности одного или более значений атрибута в идентификационных атрибутах.

Примечания

1 Орган идентификационной информации обычно связан с доменом, например, доменом происхождения, в которой атрибуты, в отношении которых орган идентификационной информации может делать утверждения, имеют конкретное значение.

2 Деятельность органа идентификационной информации может регулироваться политикой защиты персональных данных.

3 Сущность может объединять функции поставщика идентификационной информации и органа идентификационной информации.

3.20 **орган регистрации** (registration authority): Сущность, связанная с конкретным доменом, ответственная за регистрацию, проверку подлинности и регистрацию личности.

3.21 **первичная идентификация (идентификация)** (identification): Процесс распознания сущности в определенном домене как отличной от других сущностей.

Примечания

1 Процесс идентификации применяет верификацию к предъявленным или наблюдаемым атрибутам.

2 Идентификация обычно является частью взаимодействия между сущностью и сервисами в домене и используется для доступа к ресурсам. Идентификация может происходить многократно, пока сущность известна в домене.

3.22 **подтверждение идентичности** (identity proofing): Верификация на основе свидетельств идентичности, направленная на достижение определенного уровня доверия.

Примечания

1 Подтверждение идентичности обычно выполняется как часть регистрации. Подтверждение идентичности также может потребоваться при сопровождении (поддержании актуальности) зарегистрированной идентификационной информации, например при восстановлении учетной записи пользователя.

2 Обычно проверка подлинности идентичности включает проверку предоставленной идентификационной информации и может включать проверку ее уникальности.

3 Проверка для подтверждения идентификации личности обычно основана на политике регистрации, которая включает в себя спецификацию критериев проверки доказательств личности, которые должны быть ею предоставлены.

4 Проверенная идентификационная информация, полученная при выполнении проверки личности, может быть включена в процесс регистрации и может служить для облегчения дальнейшей идентификации субъекта.

3.23 **подтвержденная идентичность** (authenticated identity): Результат аутентификации в виде подтвержденной идентификационной информации сущности.

Примечания

1 Наличие подтвержденной (аутентифицированной) идентичности в определенном домене означает, что сущность была распознана в этом домене.

2 Подтвержденная (аутентифицированная) идентификационная информация, как правило, содержит данные, полученные в процессе аутентификации, например, достигнутый уровень доверия.

3 Подтвержденная (аутентифицированная) идентичность, как правило, имеет срок действия, ограниченный политикой.

3.24 **поставщик идентификационной информации** (identity information provider): Сущность, предоставляющая доступ к идентификационной информации.

Примечание — К обычным операциям, осуществляемым поставщиком идентификационной информации, относятся создание и поддержка идентификационной информации для сущностей, известных в конкретном домене. Поставщик идентификационной информации и орган идентификационной информации могут быть одной и той же сущностью.

3.25 **поставщик мандатов** (credential service provider): Доверенная сущность, относящееся к определенному домену, ответственная за управление мандатами, зарегистрированными в данном домене.

Примечание — Возможны случаи, когда поставщик мандатов выступает в качестве эмитента мандатов.

3.26 **псевдоним** (pseudonym): Идентификатор, который содержит минимальную идентификационную информацию, достаточную для того, чтобы дать возможность верификатору установить ее связь с известной сущностью.

Примечания

1 Псевдоним может быть использован для снижения рисков конфиденциальности, связанных с использованием идентификаторов с фиксированными или известными значениями.

2 Псевдоним может быть идентификатором со значением, выбранным человеком или присвоенным случайным образом.

3.27 **регистрация идентичности (регистрация)** (identity registration): Процесс записи идентификационной информации сущности в реестр идентичностей.

3.28 **реестр идентичностей** (identity register): Репозитарий идентичностей.

Примечания

1 Типичный реестр идентичностей индексируется ссылочным идентификатором.

2 Орган идентификационной информации в конкретном домене обычно использует собственный реестр идентичностей. Однако реестр идентичностей может коллективно использоваться связанными доменами, например, в рамках одной и той же организации.

3 Достоверность идентификационной информации в реестре идентичностей определяется политиками подтверждения идентичности, используемыми во время внесения в реестр.

3.29 **свидетельство идентичности** (identity evidence): Информация, которая может поддерживать проверку идентификационной информации и подтверждает, что идентификационные атрибуты и их значения действительно соответствуют (принадлежат) сущности.

Примечания

1 Свидетельства идентичности — это представленная и/или собранная информация, относящаяся к субъекту, который предоставляет идентификационные данные, необходимые для успешной идентификации или аутентификации на определенном (высоком) уровне доверия.

2 В качестве свидетельств идентичности могут рассматриваться, например, результаты верификации заявленных идентификационных данных, документальные подтверждения (официальные документы), в том числе и полученные от субъекта (объекта) доступа, а также другая подтверждающая информация.

3.30 **система управления идентификационными данными** (identity management system): Механизм, включающий политику, процедуры, технологию и другие ресурсы для обслуживания (сбор, верификация, регистрация и т. п.) идентификационной информации, включая соответствующие метаданные.

Примечание — Система управления идентичностью, как правило, используется при идентификации или аутентификации сущностей. Система может быть развернута для поддержки других автоматизированных решений, основанных на идентификационной информации сущности, признанной в домене.

3.31 **слепое подтверждение** (blinded affirmation): Принцип управления идентичностью, при котором третьему лицу не предоставляется идентификационная информация субъекта, за исключением заявления о том, что сущность известна в домене.

Примечания

1 Слепое подтверждение обеспечивает неприкосновенность частной жизни субъекта.

2 Слепое подтверждение может быть реализовано с помощью кратковременного идентификатора или псевдонима.

3.32 **ссылочный идентификатор** (reference identifier): Идентификатор в домене, который должен оставаться неизменным в течение всего срока существования сущности, известной в домене, и не связанным с другой сущностью в течение периода, указанного в политике, после того как сущность перестает быть известной в этом домене.

Примечания

1 Ссылочный идентификатор сохраняется, по крайней мере, в течение существования сущности в домене и может существовать дольше, чем сама сущность, например, для архивных целей.

2 Ссылочный идентификатор для сущности может изменяться в течение срока существования сущности, и в момент изменения прежний ссылочный идентификатор больше не применим к данной сущности.

Пример — Номер водительского удостоверения, который остается неизменным в течение всего срока действия удостоверения, является постоянным идентификатором, который ссылается на дополнительную идентификационную информацию и является эталонным идентификатором. IP-адрес не является ссылочным идентификатором, поскольку он может быть присвоен другим сущностям.

3.33 **субъект** (subject): Сущность, идентификационная информация которой хранится и управляется системой управления идентификационными данными.

Примечание — В контексте защиты персональных данных понятие «субъект» относится к физическому лицу.

3.34 **сущность** (entity): Элемент домена, объективно существующий в соответствии с целью функционирования домена.

Примечания

1 Термин «сущность» следует воспринимать в широком смысле. Сущность может иметь физическое или логическое воплощение. Она может представлять собой физическое или юридическое лицо (учреждение, компания), объект (информация, система, устройство) или группу таких индивидуальных сущностей.

2 Физическое лицо в настоящем документе также является сущностью и имеет единое, целостное существование. Его можно описать множеством различных атрибутов.

Различные наборы этих атрибутов формируют различные идентичности для одного и того же физического лица.

3 С сущностью может быть связан набор атрибутов, используемый в домене.

Пример — Физическое лицо, организация, устройство, группа однородных элементов, физическое лицо как абонент телекоммуникационной услуги, паспорт, сетевая интерфейсная карта, программное приложение, услуга или веб-сайт.

3.35 **уникальный идентификационный атрибут (идентификатор)** (identifier): Атрибут или набор атрибутов, однозначным образом характеризующий уникальность сущности в данном домене.

Примечание — Идентификатор может быть специально созданным атрибутом со значением, уникальным внутри домена.

Пример — Номер полиса обязательного медицинского страхования, адрес электронной почты или универсальный уникальный идентификатор (Universal unique identifier — UUID) могут быть использованы в качестве идентификаторов.

3.36 **управление идентичностью** (identity management): Совокупность процессов управления взаимодействием между сторонами, которые осуществляют обработку идентификационных данных, а также процессов управления жизненным циклом, значениями, наборами, типами и необязательными метаданными атрибутов идентичностей, известных в конкретном домене.

Примечание — Процессы и политики управления идентичностью поддерживают, в том числе, функции органа происхождения идентификационных данных, регулирование взаимодействия между сущностью, для которой осуществляется управления идентичностью, и органом происхождения идентификационных данных.

3.37 **эмитент мандатов** (credential issuer): Субъект, ответственный за предоставление мандатов субъекту в определенном домене.

4 Идентичность

4.1 Общие положения

Идентичность — это информация, используемая для представления сущности в автоматизированной (информационной) системе в виде данных, подлежащих хранению или обработке. Цель конкретного домена, обслуживаемого системой — определить, какие атрибуты, описывающие сущность, должны использоваться в ее идентичности. Постоянно сохраняемая идентичность является основой для идентификации субъекта. Если хранящаяся идентификационная информация не является идентификатором, то от субъекта может потребоваться дополнительная информация для его идентификации.

Идентичность может быть частично или полностью заменена мандатом, выданным субъекту. Если идентичность представлена таким мандатом, то идентификатор этого мандата может быть включен в зарегистрированную идентичность.

Этот документ рассматривает любой набор атрибутов, описывающих конкретную сущность, как идентичность для этой сущности. В некоторых доменах постоянно сохраняемая идентификационная информация для разных сущностей может быть одинаковой. В этом случае дополнительная информация используется при идентификации для распознавания сущности как отдельной, где это необходимо. В некоторых случаях [1] явной целью идентификации является способность идентификационной информации отличать объекты друг от друга в той мере, в какой это необходимо для приложений в определенном домене.

У сущности может быть много идентификационных атрибутов, связанных с одним и тем же доменом и каждый из них связан, по крайней мере, с одним доменом. Некоторые идентификационные атрибуты сущности могут не быть уникальными в домене.

Если идентичность не является уникальной в определенном домене, она может служить для различения группы сущностей в этом домене, которые имеют одну или несколько общих характеристик, от других сущностей, которые не имеют такой характеристики.

Идентичность сущности служит для того, чтобы сделать известной соответствующую информацию о сущности при ее взаимодействии с услугами и/или при доступе к ресурсам, предоставляемым доменом. Домен определяет тип и диапазон допустимых значений атрибутов, которые будут использоваться для идентификации или других целей.

Примечание — В некоторых случаях термин «частичная идентичность» может быть использован для обозначения определенного набора атрибутов, взятых из большего набора атрибутов, которые, в отличие от этого, могут быть названы полной идентичностью — всеми доступными атрибутами — сущности в домене. Предпочтительным термином в этом документе является идентичность.

Домен должен использовать систему управления идентификационными данными, соответствующую комплексу стандартов по основам управления идентичностью, для управления идентификационной информацией сущностей, которые он планирует распознавать.

4.2 Идентификационная информация

Информация, относящаяся к конкретной сущности в домене, называется идентификационной информацией.

Если данная идентификационная информация в достаточной степени отличает сущность от других в контексте ее использования, то эта идентификационная информация позволяет различить и их идентичности.

Если комбинация значений, содержащихся в идентификационной информации, уникальна в данном домене, то эта идентификационная информация может являться идентификатором сущности.

При создании новой идентичности сущности в домене поставщик идентификационной информации домена может задавать значения для обязательных атрибутов новой идентичности. Новые атрибуты могут состоять из:

- информации, необходимой для обеспечения взаимодействия между доменом и сущностью, для которой создается идентичность;
- информации, необходимой для будущей идентификации сущности, включая описание характеристик физического существования сущности;
- информации, необходимой для будущей аутентификации идентичности сущности;
- одного или нескольких ссылочных идентификаторов.

Новая идентификационная информация может быть получена из идентификационной информации сущности, созданной в текущем или в другом домене. Формирование новой информации может включать копирование, подбор или создание псевдонима. При формировании необходимо удостовериться, что созданная идентификационная информация однозначно относится к сущности.

Идентификационная информация может быть связана с метаданными, определяющими, например, ее происхождение, область использования и период действия. Метаданные идентификационной информации могут быть сами идентификационной информацией и могут быть включены в число идентификационных атрибутов, с которыми они связаны.

Идентификационная информация и связанные с ней метаданные могут меняться. В соответствующих политиках должны быть определены процедуры и условия для изменения, обновления и создания идентификационной информации. Политики могут включать ведение записей для аудита. Кроме того, политики могут включать ряд задач и действий, относящихся к жизненному циклу идентичности (см. 6.2), включая:

- запрос и получение информации из внешних источников;
- верификацию и подтверждение действительности;
- уточнение и классификацию;
- регистрацию (внесение в реестр);
- активацию;
- архивирование;
- удаление.

4.3 Идентификатор

Уникальный атрибут или атрибуты идентичности, используемые в качестве идентификатора, могут быть: доступны сущности исключительно для использования в домене происхождения или пригодны для использования в доменах, отличных от домена происхождения.

Идентификатор может быть создан в домене происхождения, может быть результатом наблюдения или может основываться на представленных идентификаторах.

Примечания

1 В некоторых случаях, например, в технологии единого входа, идентификатор может создаваться с целью использования и вне домена происхождения.

2 В некоторых случаях одного лишь идентификатора может быть недостаточно, чтобы отличить сущность от другой сущности в домене, отличном от домена происхождения. В этом случае другому домену, в зависимости от сценариев использования идентификатора, может потребоваться дополнительная идентификационная информация. Примером этого может служить библиотечная карточка с номером в качестве идентификатора, который также предоставляет регулярный доступ в музей, где в случае проведения в музее выставки, доступной с определенного возраста, запрашивают эту дополнительную информацию.

4.4 Мандат

Мандаты могут существовать в различных форматах:

- как информация, известная только субъекту и системе управления идентификационными данными, например пароль, PIN-код, парольная фраза;
- как общедоступная информация, известная заявителю и, возможно, другим субъектам, например имя пользователя;
- в виде цифровой записи, содержащей идентификационную информацию;

- в качестве документа с напечатанной идентификационной информацией, возможно машиночитаемой;
- как портативное процессорное устройство, например смарт-карта, с идентификационной информацией, хранящейся в его (постоянной) памяти;
- как сочетание этих форматов.

Примечания

1 Для физических лиц мандаты могут быть представлены в виде физических объектов, принадлежащих лицу, личность удостоверяется мандатом. Мандаты косвенно представляют домен идентичности, в которым они созданы, например, для секрета как среды, в которой секрет может быть проверен.

2 Если мандат не является уникальным, для аутентификации необходима дополнительная информация, такая, например, как имя пользователя или биометрический образец. Эта информация может быть предоставлена с помощью отдельного мандата.

3 Физические мандаты могут быть уникальными в домене происхождения. Например, паспорт однозначно идентифицирует физическое лицо как гражданина страны (домена).

4 Мандат также можно рассматривать как самостоятельную сущность с определенным идентификатором, например паспорт, идентифицируемый уникальным номером паспорта.

Мандаты могут содержать информацию, облегчающую проверку содержащихся в них идентификационных данных на заданном уровне доверия. Соответствующие методы проверки будут зависеть от приложения и формы используемых мандатов и могут включать в себя:

- ссылку на домен происхождения, например имя или URL-адрес;
- ссылку на издателя мандата, например имя или URL-адрес;
- секретную информацию, известную только субъекту, например пароль;
- физические характеристики, которые трудно скопировать, такие как:
  - водяной знак;
  - голограмма;
  - физически неклонируемая функция;
- секретный криптографический ключ;
- криптографический открытый ключ;
- сертификат открытого ключа;
- описание параметров криптографических ключей;
- ссылку на спецификацию проверки подлинности или уровень гарантии содержащейся в ней идентификационной информации, например международный стандарт.

Примечание — Информация в мандатах, предназначенная для поддержки проверки, позволяет доверенной третьей стороне утверждать физическую целостность мандата или логическую целостность содержащихся в них идентификационных данных. Эта вспомогательная информация позволяет верификатору получить уверенность в любой информации, которую он получает из мандата. Верификатор может использовать дополнительную информацию, например, полученную из домена, в котором были выданы мандаты, для определения целостности мандатов и содержащейся в них информации.

Для информации в мандатах, которая используется в процессе верификации идентификационной информации, относящейся к физическому лицу, должна быть обеспечена защита конфиденциальности в соответствии с нормативными правовыми актами.

Мандаты могут дополнительно поддерживать криптографические методы для аутентификации и защиты конфиденциальности идентификационной информации, которую они представляют.

Мандаты могут выступать в качестве идентификатора сущности в домене, в котором они выданы. Мандаты могут использоваться в качестве идентичности сущности для регистрации в другом домене.

Мандаты должны быть связаны с организацией, которую они представляют, и любая содержащаяся в них идентификационная информация должна быть верной на момент ее выдачи. Домен, в котором мандаты выдаются в физической форме, может связать каждый мандат с уникальным идентификатором, и эта комбинация может быть записана в реестр. Реестр идентичностей должен быть реализован в соответствии с [2].

Примечание — Для усиления защиты конфиденциальности реестр идентичностей может быть отделен от реестра мандатов в домене выдачи.

Принципы управления мандатами описаны в [3].

5 Атрибуты

5.1 Общие положения

Идентификационный атрибут описывает состояние, внешний вид или другие качества сущности, связанный с данным доменом. Каждый атрибут имеет собственную семантику, определяющую интерпретацию значений, которые может принимать атрибут. Семантика атрибута может быть явным образом определена, например, путем ссылки на международный стандарт для оборудования, чтобы установить его значение.

Атрибут имеет вид, значение и операционный контекст. У атрибута может быть название, которое может использоваться для ссылки на него. В зависимости от использования значения атрибута его операционным контекстом является домен происхождения или домен применимости.

Для атрибутов должны быть четко определены и документированы семантики и синтаксис.

Примечание — Для автоматизированной (информационной) системы, реализующей управление идентичностью рекомендуется для каждого элемента данных, представляющего атрибут, явно указать его внутреннее и внешнее представление (синтаксис) и способы его обработки (семантика).

5.2 Виды атрибутов

Атрибуты можно классифицировать, относя их к одному или более видам, включающим (но не ограничивающимся) следующее:

- информация о физическом существовании, такая как:
  - биографические детали;
  - домашний или рабочий адрес;
  - работодатель;
  - трудовой стаж;
  - местоположение устройства;
- информация, описывающая развитие сущности с течением времени, такая как:
  - уровень образования;
  - оценки компетентности;
  - награды;
  - установленные приложения;
  - конфигурация устройства;
  - информация, свойственная сущности, такая как, например, биометрия;
- информация, присвоенная сущности, такая как:
  - цифровая подпись;
  - номер карточки социального страхования;
  - номер документа о гражданстве;
  - номер паспорта;
  - серийный номер производителя;
  - сетевой (MAC) адрес;
  - криптографический ключ;
- ссылка на источник идентификационной информации о сущности, такой как:
- паспорт;
- диплом об образовании;
- официальный акт о регистрации организации;
- свидетельство о регистрации транспортного средства.

Примечание — Классификация атрибутов здесь приводится в качестве примера. Некоторые атрибуты можно классифицировать, относя их ко многим видам.

5.3 Домен происхождения

Домен происхождения атрибута может обеспечивать метаданные для атрибута, чтобы указывать:

- диапазон значений атрибута;
- уникальность значений атрибута;
- шифрование значения атрибута;
- время создания или верификации атрибутов или идентификационных атрибутов;

- время истечения срока атрибутов или идентификационных атрибутов;
- метод установления значения атрибутов или идентификационных атрибутов;
- метод верификации значения атрибутов;
- механизм получения физическим лицом удобочитаемого представления значения атрибута.

Домен происхождения атрибута или любая информация, определяемая доменом происхождения, может быть явным образом определена как часть значения атрибута, например, со ссылкой на документ спецификации системы или применимые стандарты.

Примечания

1 Явно определенный домен происхождения может быть детализирован как часть значения атрибута или определен, когда потребуется, например, в процессе обнаружения.

2 Указанные доменом происхождения свойства атрибута могут быть указаны с однозначной ссылкой, например, унифицированный идентификатор ресурса, на документацию системы, которая включена в определение вида атрибута.

3 Значение атрибута, включающее метаданные, можно назвать составным.

6 Управление идентичностью

6.1 Общие положения

Домен может использовать структуру управления идентичностью для поддержки соответствия между сущностью и ее идентичностью, например, с помощью аутентификации.

Управление идентичностью охватывает жизненный цикл идентификационной информации от первоначального внесения в реестр идентичностей до архивирования или удаления.

Структура управления идентичностью включает органы управления, политики, процессы, данные, технологии и стандарты, которые могут включать:

- приложение(я), реализующее(ие) реестр идентичностей;
- аутентификацию идентичности;
- установление происхождения идентификационной информации;
- установление связи межу идентификационной информацией и сущностью;
- поддержку идентификационной информации;
- обеспечение целостности идентификационной информации;
- предоставление мандатов и услуг для упрощения аутентификации сущности как уже известной;
- уменьшение риска хищения идентификационной информации или злоупотребления ей.

6.2 Жизненный цикл идентичности

На рисунке 1 показан жизненный цикл идентичности. Первоначально идентификационная информация о сущности отсутствует и сущность неизвестна. После удаления всей идентификационной информации о сущности она опять становится неизвестна.

Примечание — С точки зрения управления идентичностью, неизвестная сущность не существует.

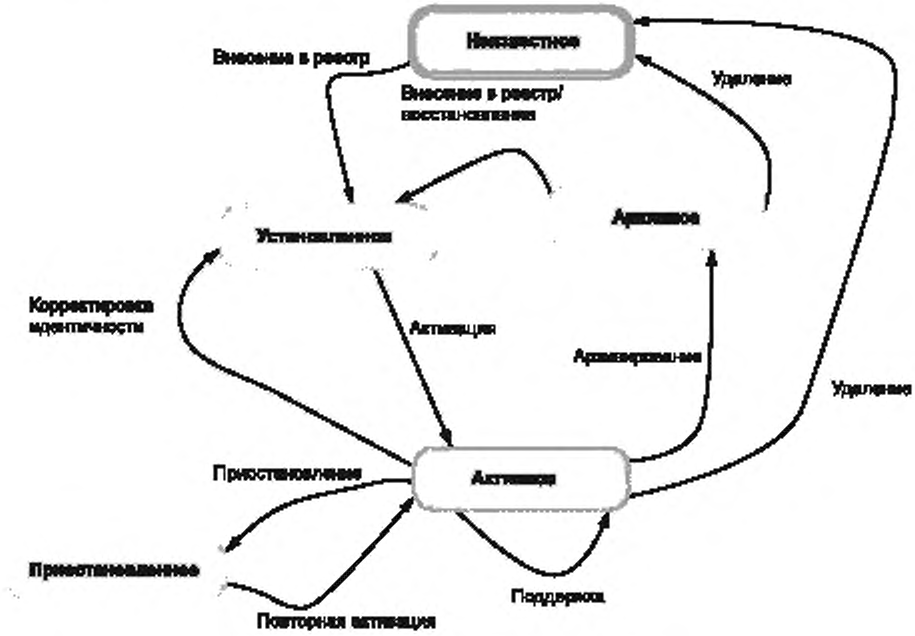

Рисунок 1 — Жизненный цикл идентичности

Определяются следующие состояния в жизненном цикле идентичности:

- неизвестное: в реестре идентичностей нет никакой информации, которая может использоваться для идентификации сущности, которая, следовательно, является неизвестной.

- установленное: требуемая идентификационная информация верифицирована во время процесса внесения в реестр (см. 7.3), создана дополнительная информация, например, ссылочный идентификатор, информация зарегистрирована (см. 7.4).

- активное: идентификационная информация имеется, что позволяет сущности взаимодействовать с сервисами и использовать ресурсы, доступные в домене применения, например, сущности может быть дано право инициировать активный сеанс в системе.

- приостановленное: имеется идентификационная информация, специально указывающая на то, что сущность не может использовать ресурсы домена.

- архивное: идентификационная информация для сущности все еще имеется, даже если сущность больше не существует в данном домене. Архивная информация недоступна для распознания сущности, за исключением повторного внесения в реестр. При повторном внесении сущности в реестр архивная информация может быть использована для установления новой идентичности для сущности, которая может включать в себя часть архивной информации (восстановление).

В управлении жизненным циклом могут существовать следующие переходы:

- внесение в реестр — включает подтверждение идентичности (верификацию) и регистрацию идентичности с верифицированной и созданной идентификационной информацией (см. 8.3);

- активация — добавление идентификационной информации к информации, хранящейся в реестре идентичностей для сущности, специально для того, чтобы дать возможность сущности иметь доступ к ресурсам и взаимодействовать с предоставляемыми доменом сервисами;

- поддержка — обновление идентификационной информации сущности, хранящейся в реестре идентичностей (см. раздел 10);

- корректировка идентификационных атрибутов — обновление информации сущности в реестре идентичностей, при котором новая информация вызывает модификацию информации активации;

- приостановление — маркирование некоторой идентификационной информации сущности, хранящейся в реестре идентичностей, как временно недоступной для использования. Приостановление может достигаться путем устранения прав доступа, выраженных в хранящейся идентификационной информации;

- повторная активация — возврат после приостановления;
- удаление — полное удаление идентификационной информации в зарегистрированной идентичности;
- архивирование — частичное устранение идентификационной информации сущности из реестра идентичностей, так чтобы информация была пригодна только для статистической обработки или могла быть только доступна как относящаяся к сущности при дополнительной информации, предоставляемой сущностью;
- внесение в реестр/восстановление — это процесс внесения в реестр, при котором некоторую идентификационную информацию, используемую в качестве подтверждения идентичности, получают из реестра идентичностей.

7 Идентификация

7.1 Общие положения

Идентификация определяет, что представленные идентификационные данные содержат информацию, необходимую для установления того, что:
- сущность уже известна в данном домене;
- сущность оценивается, чтобы стать известной в домене.

Идентификация может использовать идентификационную информацию, связанную с конкретной сущностью, для определения:
- существуют ли уже идентичность для сущности;
- соответствует ли сущность известной, представленной или наблюдаемой идентификационной информации;
- связана ли однозначно сущность с идентичностью.

После идентификации домен может активно отличать сущность и ее взаимодействие с доменом от любой другой сущности, которую он также идентифицировал.

Примечание — В настоящем стандарте идентификация представляется с точки зрения домена. Во взаимной идентификации обе стороны могут являться как сущностью, так и доменом.

Идентификация включает связывание совокупности атрибутов как с сущностью, так и с идентичностью. Значение этих атрибутов может быть:
- определено путем наблюдения;
- предоставлено сущностью;
- извлечено из реестра идентичностей;
- предоставлено другим источником;
- присвоено во время процесса идентификации.

Идентификация может сопровождаться установлением прав субъекта на доступ к ресурсам и взаимодействие с услугами, предоставляемыми доменом, для последующей авторизации (см. 6.2).

В системе, где доступ к ресурсам или взаимодействие с услугами сопряжены с рисками, связанными с идентификацией, требуемый уровень доверия к идентификации должен быть определен на основе типа и уровня риска идентификации для ресурса, а также типа взаимодействия с услугой, для которой могут быть установлены права доступа (см. раздел 8).

Идентификация может осуществляться для одной цели, характерной для домена, или для многих различных целей. Идентификация может быть частью многих процессов управления идентичностью.

Процесс идентификации должен быть определен с помощью следующих принципов:
- риск (должна осуществляться оценка рисков, связанных с использованием идентификационных атрибутов сущности, и их обработка в необходимой степени, чтобы они были допустимыми).

Примечания

1 Различные уровни доверия к идентификации могут быть связаны с различными уровнями риска, связанного с доступом к различным ресурсам и взаимодействием с различными сервисами.

2 Оценка рисков включает рассмотрение качества доступной информации и средств для установления ее правильности.

3 Выбор приемлемых вариантов уменьшения риска включает обеспечение того, чтобы расходы были пропорциональны риску;

- качество информации (идентификационная информация должна верифицироваться для обеспечения уверенности в применимости для целей использования);
- минимальность (для идентификации физических лиц следует собирать не больше идентификационной информации, чем это необходимо).

7.2 Верификация

Новая идентификационная информация должна быть верифицирована. Верификация может также осуществляться в отношении идентификационной информации, извлеченной из реестра идентичностей или полученной от поставщика идентификационной информации.

Верификация идентификационной информации должна обеспечивать уверенность в том, что она:
- присутствует в утвержденном формате;
- содержит значения, соответствующие критериям, характерным для домена или цели идентификации;
- была создана в рамках требуемого периода действия;
- исходит из надежного источника.

Примечание — Верификация может также предоставлять входные данные для идентификации, а ее результат может быть характерным для определенных обстоятельств, например, места и времени данного процесса.

Верификация может также устанавливать, что атрибут относится к физическому существованию сущности, например, сопоставлять биометрический образец сущности с биометрическим образцом, содержащимся в ее идентификационных атрибутах.

Верификация может устанавливать, что все представленные атрибуты относятся к одной и той же сущности и согласуются с ее физическим существованием.

Верификация может включать подтверждение действительности не требуемых для процесса идентификации атрибутов, которые могут использоваться во время взаимодействия с сервисами или доступа к ресурсам, предоставляемым доменом после идентификации, например, языковое предпочтение или учетный номер.

7.3 Внесение в реестр

Внесение в реестр может привести к созданию одной или нескольких идентичностей для зарегистрированной сущности. В частности, может быть создан ссылочный идентификатор. Созданная идентификационная информация регистрируется как идентичность сущности, зарегистрированной в домене. Идентификационная информация, выбранная из свидетельства идентичности, также может быть зарегистрирована с данной идентичностью в момент регистрации.

Значение уникального(ых) атрибута(ов) в созданной идентичности может быть выбрано сущностью или назначено системой управления идентификационными данными, например, на основе эталонного идентификатора, созданного при регистрации объекта.

Внесение в реестр может включать в себя сбор биометрических данных в качестве идентификационной информации для зарегистрированного субъекта.

Если сущность определяет значение идентификатора, созданного во время регистрации, система управления идентификационными данными должна обеспечить его уникальность.

Примечание — Физический объект, например, членский билет, может содержать идентификатор, созданный во время внесения в реестр.

7.4 Регистрация

Система управления идентификационными данными может вносить в реестр идентичностей идентификационную информацию для сущностей, которые она намерена распознавать. Внесение в реестр включает в себя начальную регистрацию идентификационной информации.

Примечание — После регистрации сущность становится известной в домене и начинается жизненный цикл ее идентичности.

Регистрация может иметь конкретную или неограниченную длительность. Нормативные правовые акты могут накладывать ограничения на фактическую длительность регистрации, включая условия того, когда и как может заканчиваться неограниченная регистрация.

Если этому не препятствуют правовые требования, неограниченная регистрация должна завершаться по сделанному сущностью или от лица сущности запросу об удалении. При удалении всей идентификационной информации для сущности сущность должна быть удалена из реестра идентичностей. Однако, если определено в соответствующей политике, домен может сохранять некоторую идентификационную информацию для архивных или аудиторских целей, и в этом случае идентичность будет находиться на архивном этапе жизненного цикла (см. 6.2). В частности, ссылочный идентификатор может сохраняться, чтобы предотвратить его повторное использование в качестве ссылки на другую сущность.

Идентичность сущности, хранящаяся в реестре, должна иметь ссылочный идентификатор, являющийся уникальным среди всех хранящихся идентичностей. Ссылочный идентификатор должен иметь одно и то же значение на протяжении периода регистрации конкретной идентичности.

Ссылочный идентификатор может быть предназначен для использования исключительно внутри домена, где действует система управления идентификационными данными.

Примечание — Если ссылочный идентификатор не используется исключительно внутри домена, он может быть доступен для использования в качестве атрибута в идентичности, представляемой сущностью для идентификации в другом домене.

Идентификационная информация, хранящаяся в реестре идентичностей, может включать в себя несколько ссылочных идентификаторов.

Ссылочный идентификатор может использоваться для указания конкретной идентичности сущности в домене.

7.5 Подтверждение идентичности

7.5.1 Общие положения

Целью проверки подлинности идентичности является установление определенного уровня уверенности в том, что:

- выбранные атрибуты для сущности имеют определенное значение;
- эти атрибуты на самом деле относятся к определенной сущности;
- в домене неизвестна никакая другая сущность, которой принадлежат те же атрибуты.

Примечания

1 В домене, где постоянно хранимая идентификационная информация не является уникальной, может потребоваться только создание идентичности сущности, которая еще не идентифицирована. В этом случае система управления идентификационными данными может хранить дополнительную постоянную информацию, не связанную с идентификационной информацией, для поддержки того, что идентичность для проверяемой сущности уникальна.

2 Орган регистрации несет ответственность за подтверждение идентичности.

7.5.2 Свидетельства идентичности

Свидетельства идентичности используются для установления значений атрибутов при регистрации сущности в домене. Мандаты, выданные в домене, могут использоваться в качестве свидетельства идентичности в другом домене. Эти мандаты могут быть представлены сущностью. В качестве альтернативы они могут быть получены от поставщика идентификационной информации в другом домене, где сущность известна на основе информации, предоставленной сущностью.

Если при проверке выявляется, что нескольких мандатов из одного и того же или разных доменов, в которых каждый из мандатов обеспечивает уровень доверия, меньший, чем требуется, то для достижения требуемого уровня доверия к идентичности сущности в значении атрибута и в установлении значения, относящегося к конкретной сущности, может быть применено агрегирование атрибутов.

Орган идентификационной информации для домена, в котором были выданы мандаты, может поддерживать проверку идентификационной информации во время проверки подлинности идентичности с помощью:

- предоставления некоторого аутентифицированного набора допустимых значений атрибутов, например списка названий улиц или районов;
- формата публикации и другие физические или логические свойства действительных мандатов, выданных конкретным доменом;
- политики публикации, применяемой к проверке подлинности, и обслуживанию идентификационной информации;

- предоставления открытого ключа в инфраструктуре открытых ключей, совместно используемой с проверяющим центром регистрации, для проверки цифровых подписей, используемых для аутентификации мандатов или данных, представленных им;
- предоставления онлайн-сервиса для проверки представленных атрибутов для сущности, известной в своем домене;
- предоставления онлайн-сервиса для получения дополнительных атрибутов для сущности, известной в своем домене.

8 Аутентификация

Успешная аутентификация сущности в домене с конкретным уровнем доверия дает полагающейся стороне уверенность в правильности и применимости результата верификации. Уровни доверия определяются в соответствии с ГОСТ Р 58833.

Соответствующая требованиям настоящего стандарта система управления идентификационными данными должна определять для каждого из своих процессов аутентификации:

- политики верификации идентификационной информации;
- механизмы установления достоверности и правильности аутентифицированной идентичности;
- срок действия аутентифицированной идентичности;
- механизмы учета и аудита; этапы обработки и (промежуточные) результаты обработки.

Примечание — Аутентификация аналогична модели безопасности контроля периметра, где строгая проверка на входе дает разрешение на доступ в определенную область деятельности в течение определенного периода времени.

9 Поддержка

Система управления идентификационными данными может осуществлять поддержку зарегистрированной ею идентификационной информации посредством изменения одного или более значений атрибутов идентичности.

Система управления идентификационными данными должна специфицировать механизмы для обеспечения целостности и точности хранимых атрибутов. Механизмы должны поддерживать хранящуюся в реестре идентичностей информацию как точное представление идентичности.

Орган идентификационной информации должен предоставлять наиболее точные данные, доступные для идентичности, посредством процесса, в котором реализованы меры защиты.

10 Реализация

Система управления идентификационными данными может быть.

- централизованной — полностью централизованная система имеет единый реестр идентичностей и единую точку контроля за внесением в реестр и доступом к хранящейся идентификационной информации;
- распределенной — система управления идентификационными данными может иметь много реестров идентичностей и много точек контроля за внесением в реестр и доступом к зарегистрированной идентификационной информации.

Примечание — Более централизованная система обычно демонстрирует меньшую сложность, но более жесткую структуру.

- ориентированной на пользователя — система управления идентификационными данными является ориентированной на пользователя, если она позволяет сущностям играть активную роль в управлении идентификационной информацией, хранящейся в реестре идентичностей (см. 7.4);
- объединенной — объединение дает возможность системе управления идентификационными данными, не содержащей требуемую идентификационную информацию в своем реестре, полагаться на идентификационную информацию из другой системы управления идентификационными данными и выпущенные ею свидетельства идентичности. В этом случае система управления идентификационными данными действует как орган идентификационной информации.

В ситуациях взаимодействия сущностей со многими доменами объединение идентичностей предназначено для:

- содействия подтверждению идентификационных данных;
- содействия аутентификации;
- содействия внесению в реестр;
- улучшению опыта пользователей.

Примечание — Объединение идентичностей применимо для сущностей (и доменов), взаимодействующих с другими доменами в сети Интернет.

11 Обеспечение конфиденциальности персональных данных

Система управления идентификационными данными, соответствующая требованиям настоящего документа, должна обеспечивать выполнение законодательных и нормативных требований для обеспечения конфиденциальности персональных данных взаимодействующих с ней физических лиц. Проект такой системы должен определять любую чувствительную, с точки зрения необходимости защиты, информацию, обрабатываемую ею.

Система управления идентификационными данными, соответствующая требованиям настоящего стандарта, должна предоставлять связанные с обеспечением конфиденциальности персональных данных возможности для:

- реализации механизмов, включая политики, процессы и технологию, для минимального раскрытия;
- аутентификации сущностей, использующих идентификационную информацию;
- минимизации возможности связывания идентичностей;
- записи и аудита использования идентификационной информации;
- защиты от непреднамеренного создания рисков нарушения конфиденциальности, например, связанных с неадекватной защитой идентификационной информации в журналах и аудиторских журналах;
- внедрения политики выборочного раскрытия информации;
- осуществления политики привлечения физического лица для получения согласия на обработку его персональных данных.

Требования, касающиеся обращения с чувствительной, с точки зрения защиты персональных данных, содержатся в ГОСТ Р 59407.

Библиография

[1] ITU-T Recommendation X.1252 — Кибербезопасность. Управление идентичностью. Базовые термины и определения (Cyberspace security — Identity management — Baseline identity management terms and definitions)

[2] ИСО/МЭК 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)

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

УДК 006.354:004.056.5:006.354 ОКС 35.030

Ключевые слова: методы и средства обеспечения безопасности, управление идентичностью, идентификационная информация, поставщик идентификационной информации

Технический редактор *И.Е. Черепкова*
Корректор *И.А. Королева*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 24.05.2021. Подписано в печать 31.05.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 2,79. Уч.-изд. л. 2,51.

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.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru