ЕВРАЗИЙСКИЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ
(EACC)
EURO-ASIAN COUNCIL FOR STANDARDIZATION, METROLOGY AND CERTIFICATION
(EASC)

М Е Ж Г О С У Д А Р С Т В Е Н Н Ы Й
С Т А Н Д А Р Т

ГОСТ ИСО/МЭК 24760-2— (проект, окончательная редакция)

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Основы управления идентичностью

Часть 2

Базовая архитектура и требования

(ISO/IEC 24760-2:2015, IDT)

Издание официальное

Минск
Евразийский совет по стандартизации, метрологии и сертификации
202

Предисловие

Евразийский совет по стандартизации, метрологии и сертификации (ЕАСС) представляет собой региональное объединение национальных органов по стандартизации государств, входящих в Содружество Независимых Государств. В дальнейшем возможно вступление в ЕАСС национальных органов по стандартизации других государств.

Цели, основные принципы и основной порядок проведения работ по межгосударственной стандартизации определены ГОСТ 1.0 «Межгосударственная система стандартизации. Основные положения» и ГОСТ 1.2 «Межгосударственная система стандартизации. Стандарты межгосударственные, правила и рекомендации по межгосударственной стандартизации. Правила разработки, принятия, обновления и отмены».

Сведения о стандарте

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН), Закрытым акционерным обществом «Аладдин Р.Д.» (ЗАО «Аладдин Р.Д.») и Обществом с ограниченной ответственностью «Информационно – аналитический центр» (ООО ИАВЦ) на основе собственного аутентичного перевода стандарта, указанного в пункте 4

2 ВНЕСЕН Межгосударственным техническим комитетом по стандартизации МТК 22 «Информационные технологии»

3 ПРИНЯТ Евразийским советом по стандартизации, метрологии и сертификации (протокол № от 202.. г.)

За принятие стандарта проголосовали:

Краткое наименование страны по МК (ИСО 3166) 004–97	Код страны по МК (ИСО 3166)044–97	Сокращенное наименование национального органа по стандартизации

4 Настоящий стандарт идентичен проекту международного стандарта ISO/IEC 24760-2:2019 «Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 2. Базовая архитектура и требования» (ISO/IEC 24760-2:2015 «Information technology — Security techniques — A framework for identity management — Part 2: Reference architecture and requirements»).

ISO/IEC 24760-2:2015 разработан подкомитетом ПК 27 «Информационная безопасность, кибербезопасность и защита конфиденциальности» Совместного технического комитета СТК 1 «Информационные технологии» Международной организации по стандартизации (ИСО) и Международной электротехнической комиссии (МЭК).

Перевод с английского языка (en).

Сведения о соответствии межгосударственных стандартов ссылочным международным стандартам приведены в дополнительном приложении ДА.

Степень соответствия — идентичная (IDT).

5 ВВЕДЕН ВПЕРВЫЕ

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории указанных выше государств публикуется в указателях национальных стандартов, издаваемых в этих государствах, а

также в сети Интернет на сайтах соответствующих национальных органов по стандартизации.

В случае пересмотра, изменения или отмены настоящего стандарта соответствующая информация будет опубликована на официальном интернет-сайте Межгосударственного совета по стандартизации, метрологии и сертификации в «Межгосударственные стандарты».

Содержание

Введение

Для функционирования автоматизированных (информационных) систем необходимо собирать и формировать по установленным правилам информацию о пользователях, связанном 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.

Реагируя на потребность эффективной и результативной реализации систем, принимающих основанные на идентификационных данных решения, настоящий стандарт определяет архитектуру выпуска, администрирования и использования данных, помогающих характеризовать физических лиц, организации или компоненты информационной технологии, действующие в их интересах.

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

Комплекс стандартов ИСО/МЭК 24760 определяет основные понятия и операционные основы управления идентичностями с целью реализации управления информационными системами таким образом, чтобы информационные системы могли выполнять деловые, договорные, нормативные и правовые обязательства.

Настоящий стандарт определяет базовую архитектуру системы управления идентификационными данными, которая включает основные элементы архитектуры и их взаимосвязи. Данные элементы архитектуры описываются по отношению к моделям реализации управления идентификационными данными. Кроме того, в документе определены требования к проектированию и реализации системы управления идентификационными данными, чтобы она могла отвечать целям причастных сторон, участвующих в развертывании и эксплуатации этой системы.

Настоящий стандарт является основой для реализации других документов по стандартизации, связанных с обработкой идентификационной информации, таких как:

ИСО/МЭК 29100 Информационные технологии. Методы и средства обеспечения безопасности. Основы защиты персональных данных;

ИСО/МЭК 29101 Информационные технологии. Методы и средства обеспечения безопасности. Эталонная архитектура защиты персональных данных;

ИСО/МЭК 29115 Информационные технологии. Методы и средства обеспечения безопасности. Основы доверия к аутентификации сущности;

ИСО/МЭК 29146 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом.

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

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

Дата введения — 20…—… —…

1 Область применения

Настоящий стандарт:

– представляет собой руководство по реализации управления идентификационными данными;

– определяет требования для реализации и эксплуатации архитектуры управления идентификационными данными.

Настоящий стандарт подходит для любой информационной системы, обрабатывающей или хранящей информацию, связанную с идентификационными данными.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты. Для датированных документов используются только указанные издания. Для недатированных документов используются последние издания с учетом внесенных в них изменений.

ИСО/МЭК 24760-1, Information technology — Security techniques — A framework for identity management — Part 1: Terminology and concepts (Информационные технологии.

Методы и средства обеспечения безопасности. Основы управления идентичностью — Часть 1: Терминологии и концепции)

ИСО/МЭК 29115, Information technology — Security techniques — Entity authentication assurance framework (Информационные технологии. Методы и средства обеспечения безопасности. Основы доверия к аутентификации сущности)

3 Термины и определения

Для целей настоящего документа используются термины по ИСО/МЭК 24760-1, а также следующие:

3.1 **документально оформленный проект** (**documented design**): Официальное описание архитектурных (структурных), функциональных и операционных аспектов системы.

Примечания

1 Документально оформленный проект представляет собой документацию, созданную для выполнения функции руководства по реализации автоматизированной (информационной) систем.

2 Документально оформленный проект обычно включает описание конкретной архитектуры автоматизированной (информационной) систем.

3.2 **орган управления идентификационными данными** (identity management authority): Сущность, отвечающая за создание и обеспечение соблюдения операционных политик системы управления идентификационными данными (3.3).

Примечание — Орган управления идентификационными данными обычно поручает осуществление проектирования, реализации и развертывания системы управления идентификационными данными.

Пример – Исполнительное высшее руководство компании, развертывающее систему управления идентификационными данными в поддержку предоставляемых ею услуг.

3.3 **система управления идентификационными данными** *(*identity management system, IMS): Механизм, включающий в себя политики, процедуры, технологию и другие ресурсы для поддержки идентификационной информации, в том числе метаданных.

Примечание – Управления идентификационными данными обычно используется для осуществления идентификации или аутентификации сущностей. Оно может использоваться для поддержки других автоматических решений на основе идентификационной информации сущности, признанной в домене применения, для системы управления идентификационными данными.

3.4 **субъект** (principal, subject): Сущность, к которой относится идентификационная информация в системе управления идентификационными данными (3.3).

Примечание – В контексте требований защиты персональных данных понятие субъект относится к физическому лицу.

3.5 **признание недействительности** *(*invalidation): Процесс, осуществляемый в системе управления идентификационными данными (3.3), чтобы обозначить определенный атрибут как недействительный для будущего использования когда он больше не имеет силы для конкретной сущности.

Примечания

1 Признание недействительности атрибутов может быть частью обновления значений атрибутов, например, при изменении адреса.

2 Признание недействительности обычно происходит для атрибута, который определен как не имеющий больше силы, до наступления конца периода действия, ранее связанного с ним.

3 Для признания недействительности атрибутов, являющихся мандатами, обычно используется термин «аннулирование».

4 Признание недействительности, как правило, происходит сразу же после определения того, что атрибут больше не имеет силы для конкретной сущности.

3.6 **регулятивный орган** (regulatory body): Орган, уполномоченный законодательным, правовым нормативным актом или соглашением осуществлять надзор за функционированием систем управления идентификационными данными (3.3).

3.7 **причастная сторона** *(*stakeholder): Лицо, группа, организация или их аналоги, имеющие заинтересованность в системе.

[Источник: ИСО/МЭК 42010]

4 Обозначения и сокращения

IMS Система управления идентификационными данными (Identity management system)

ИКТ Информационно – коммуникационные технологии (Information and Cjmmunication Technology)

ПДн- Защита персональных данных (Personal identifiable information)

5 Базовая архитектура

5.1 Общие сведения

В данном разделе описываются элементы архитектуры системы менеджмента идентификационных данных и их взаимосвязи.

Документально оформленный проект архитектуры системы управления идентификационными данными должен быть основан на ИСО/МЭК 42010[1].

Примечание — Базовая архитектура и описание архитектуры, определенные в настоящем стандарте, основаны на ИСО/МЭК 42010.

Документально оформленный проект архитектуры системы управления идентификационными данными должен определять систему в контексте ее развертывания на основе причастных сторон и действующих субъектов, определенных в настоящем документе. Действующие субъекты бизнес уровня являются причастными сторонами. Некоторые причастные стороны не взаимодействуют с системой. Документально оформленный проект должен рассматривать требования для причастных сторон, являющихся и не являющихся действующими субъектами. Документально оформленный проект должен исчерпывающим образом описывать действующих субъектов.

Документально оформленный проект системы управления идентификационными данными, соответствующий требованиям настоящего стандарта, должен использовать соответствующий язык описания архитектуры, а также компоненты и функции базовой архитектуры с использованием терминов, определенных в настоящем стандарте.

[1] При разработке настоящего стандарта использован ГОСТ Р 57100-2016/ISO/IEC/IEEE 42010:2011.

5.2 Элементы архитектуры

5.2.1 Обзор

Элементы базовой архитектуры включают следующее:

- причастные стороны (см. 5.3.1);
- действующие субъекты (см.5.3.2);
- представления (см. 5.3, 4.4);
- модели (см. 5.3.3, 5.3.4, 5.3.5, 5.4.1, 5.4.3);
- компоненты (см. 5.4.1);
- процессы (см. 5.4.2);
- потоки информации и действия (см. 5.4.2).

5.2.2 Точки зрения

5.2.2.1 Общие сведения

Документально оформленный проект системы управления идентификационными данными должен включать контекстное представление и функциональное представление. Он может также включать физическое представление. Документально оформленный проект может содержать другие виды представлений, например, информационное представление.

Примечание — Необходимый минимальный набор точек обзора описывает взаимодействия системы с ее средой, а также внутренние компоненты и взаимодействия системы.

Описание представления должно быть сфокусированным. Диаграммы в описаниях представления должны сопровождаться текстом, определяющим показанные элементы.

Примечание — Описание точек обзора в этом подразделе основано на [5].

5.2.2.2 Контекстная точка зрения

Определение. В документально оформленном проекте контекстная точка обзора описывает взаимосвязи, зависимости и взаимодействия между системой и ее средой (физические лица, системы и внешние сущности, с которыми взаимодействует данная система).

Проблемные вопросы. Сфера действия и функции системы; идентичность, природа и характеристики внешних сущностей и используемых услуг и данных; идентичность, функции, природа и характеристики внешних интерфейсов, другие внешние взаимозависимости; влияние системы на ее окружающую среду; и общая полнота, согласованность и последовательность.

Модели. Контекстная точка зрения может содержать контекстную модель, варианты использования и сценарии взаимодействия. Контекстная модель представляет собой неформальную диаграмму, которая показывает обсуждаемую систему в виде «черного ящика» с интерфейсами, высокоуровневыми взаимодействиями и зависимостями от внешних сущностей (см. 5.3.3).

Моменты, требующие внимания. Недостающие или неверные внешние сущности, недостающие явные зависимости, слишком широкие или неточные описания интерфейсов, ненадлежащий уровень детальности, сползание сферы действия, неявный или предполагаемый контекст или сфера действия, чрезмерно усложненные взаимодействия, злоупотребление жаргоном.

5.2.2.3 Функциональная точка зрения

Определение. В документально оформленном проекте с функциональной точки зрения описываются главные функциональные элементы с операционными функциями, интерфейсами и основными взаимодействиями.

Проблемные вопросы. Функциональные возможности, внешние интерфейсы, внутренняя структура и философия функционального проектирования.

Модели. Функциональная точка зрения может содержать компонентную модель, физическую модель или инфраструктурную модель.

В документально оформленном проекте функциональная точка зрения должна идентифицировать стандарты и руководства, применяющиеся к каждой из описываемых ею функций.

Руководство по определению функциональной точки зрения представлено в 5.4.

5.3 Контекстное представление

5.3.1 Причастные стороны

5.3.1.1 Общие сведения

В настоящем стандарте признаются следующие прямые и косвенные причастные стороны [стороны обмена идентификационными данными], имеющие первостепенную значимость:

- субъект;
- орган управления идентификационными данными;
- орган идентификационной информации;
- полагающаяся сторона;
- регулятивный орган;
- аудитор;
- представитель или защитник субъектов персональных данных.

Каждая причастная сторона выполняет отдельную функцию в системе управления идентификационными данными. Эти функции подразумевают конкретные обязанности и ответственность. За исключением регулятивных органов и представителей субъектов, причастные стороны взаимодействуют с системой управления идентификационными данными и, соответственно, присутствуют в базовой архитектуре в качестве действующих субъектов (см. 5.3.2).

Вопросы, имеющие отношение к причастным сторонам в управления идентификационными данными, описываются в дальнейших подразделах и должны рассматриваться при проектировании, реализации и эксплуатации системы.

5.3.1.2 Субъект

Проблемные вопросы, имеющие отношение к субъекту в системе управления идентификационными данными, включают в себя:

- правильность собираемой, обрабатываемой и хранимой идентификационной информации;
- обеспечение защиты персональных данных;
- сведение к минимуму идентификационной информации, собираемой, обрабатываемой и хранимой системой управления идентификационными данными;

– сведение к минимуму использования идентификационной информации системой управления идентификационными данными в домене ее применения;

– ошибки идентификации, включая ошибочный отказ в доступе и ошибочное предоставление доступа, а также обнаружение и обработка ошибок;

– осведомленность об обмене идентификационной информацией с третьими сторонами и предоставление согласия на него;

– правильное представление собираемой, обрабатываемой или хранимой идентификационной информации;

– корректность операций предоставления услуг и доступа к предоставляемым ресурсам на основе атрибутов, представленных в конкретной ситуации;

– сбор, обработка и хранение идентификационной информации происходят только при наличии его осознанного согласия;

– беспристрастная трактовка его взаимодействий с системой;

– легко понятный, эффективный и соответствующий пользовательский интерфейс.

Примечание — Относящиеся к субъекту вопросы, связанные с услугами третьих сторон с использованием идентификационной информации, полученной из системы управления идентификационными данными, не являются вопросами, относящимися к системе управления идентификационными данными, и, соответственно, выходят за рамки сферы рассмотрения настоящего стандарта.

5.3.1.3 Орган управления идентификационными данными

Проблемные вопросы, имеющие отношение к органу управления идентификационными данными в системе управления идентификационными данными, включают следующее:

– определение целей управления идентичностью для домена(ов), обслуживаемого системой управления идентификационными данными*;*

– спецификация политик для поддержки целей управления идентичностью для домена (-ов), обслуживаемого системой управления идентификационными данными*;*

– выполнение целей системы управления идентификационными данными в отношении субъектов и потребителей идентификационной информации;

– обеспечение того, чтобы предоставляемая каждым субъектом идентификационная информация на определенным уровне доверия была точной и относилась к данному принципалу;

– соответствие требованиям нормативных правовых актов.

5.3.1.4 Орган идентификационной информации

Проблемные вопросы, имеющие отношение к органу идентификационной информации в системе управления идентификационными данными, включают следующее:

– правильность идентификационной информации;

– выполнение требований полагающихся сторон;

– обеспечение соответствия требованиям нормативных правовых актов*;*

– выполнение обязательств перед субъектами.

5.3.1.5 Полагающаяся сторона

Проблемные вопросы, имеющие отношение к полагающейся стороне в системе управления идентификационными данными, включают следующее:

– конфиденциальность, доступность и целостность идентификационной информации и ее применимость к субъекту;

– предоставление точной идентификационной информации, относящейся к соответствующим принципалам, на требуемом уровне доверия;

– эффективные, документально оформленные и безопасные интерфейсы;

– соответствие требованиям нормативных правовых актов, относящимся к ее операциям;

– наличие эффективного механизма и процедур проведения аудита.

5.3.1.6 Регулятивный орган

Проблемные вопросы, имеющие отношение к регулятивному органу – как к внешней независимой организации – в системе управления идентификационными данными, включают следующее:

– надлежащее документальное оформление операционных политик;

– правильность функционирования, в частности, применения операционных политик;

– надлежащую подотчетность и аудит операций системы;

– соответствие операционной политики и операционных практических приемов правовым и нормативным требованиям;

– эффективную отчетность по операциям системы, включая эффективность мер защиты информации, инциденты и меры, принятые для предотвращения инцидентов;

– эффективное реагирование на инциденты, которые нарушают защиту персональных данных или обладают потенциалом ее нарушения.

Примечание — Аудиторы как действующие субъекты в системе управления идентификационными данными (см. 5.3.2.9) при контроле операций системы управления идентификационными данными (см. 5.4) могут представлять интересы регулятивных органов.

5.3.1.7 Представитель субъектов

Представитель субъектов – это лица или группы лиц гражданского общества, защищающие права субъектов.

Представители субъектов – это лица, назначенные субъектом или выбранные организацией для представления прав субъектов в плане защиты прав и свобод при обработке его персональных данных.

Проблемные вопросы, имеющие отношение к представителям субъектов, включают следующее:

– обеспечение прозрачности, уведомлений, соответствия и защиты от сложного юридического языка;

– обеспечение доступа к услугам населения.

Примечания

1 Представители потребителей и граждан участвуют в признанных общественных процессах со многими задействованными причастными сторонами, таких как управление и установление качественных практических приемов и требований, которым должны отвечать сущности, предоставляющие товары и услуги потребителям и гражданам.

2 Представители потребителей и граждан выбираются, инструктируются и в случае необходимости обучаются для обеспечения уверенности в их участии путем разумного и обоснованного обсуждения, основанного на качественных свидетельствах, где это представляется возможным.

5.3.2 Действующие субъекты

5.3.2.1 Общие сведения

Действующий субъект взаимодействует с системой управления идентификационными данными с целью участия в операциях управления идентичностями. Сущность может взаимодействовать с одной и той же системой управления идентификационными данными как несколько различных действующих субъектов. Документально оформленный проект должен определять все взаимодействия любого действующего субъекта, поддерживаемые системой.

Документально оформленный проект должен описывать взаимодействия действующего субъекта с точки зрения функций, с которыми связаны взаимодействия. В случаях, когда взаимодействующий с системой управления идентификационными данными действующий субъект должен быть аутентифицирован, прежде чем будет разрешено продолжать взаимодействия, документально оформленный проект должен определять основу для аутентификации (например, аутентификация на основе сущности; аутентификация на основе роли и т.д.), метод аутентификации и уровень доверия, необходимый для каждого взаимодействия, как определено в ИСО/МЭК 29115[2].

Примечание — Одна из целей определения действующих субъектов в проекте системы управления идентификационными данными заключается в возможности описания всех намеченных взаимодействий с системой.

Документально оформленный проект может распознавать следующих действующих субъектов:

- субъект;
- орган управления идентификационными данными;
- орган регистрации;
- полагающаяся сторона;
- поставщик идентификационной информации;
- орган идентификационной информации;
- проверяющая сторона;
- аудитор.

[2] Настоящий стандарт разработан с учетом национального стандарта РФ ГОСТ Р 58833, а также проекта ГОСТ Р Защита информации. Идентификация и аутентификация. Уровни доверия к результатам аутентификации

Документально оформленный проект должен определять уровень доверия, необходимый для идентификации и аутентификации сущностей, делающих запрос о предоставлении доступа к идентификационной информации, содержащейся в системе управления идентификационными данными, как определено в ИСО/МЭК 29115. Уровень доверия может различаться для разных видов информации и разных видов предоставляемого доступа, т.е. для чтения, записи и т.д. Авторизация может быть реализована, как определено в ИСО/МЭК 29146.

5.3.2.2 Субъект

Субъект – это действующий субъект, который предоставляет идентификационную информацию для установления и подтверждения достоверности идентификационных данных в рамках процессов управления идентичностью. Субъект имеет следующие обязанности:

– как сущность, обращающаяся с запросом о регистрации в домене применения – предоставлять точную идентификационную информацию для внесения в реестр в качестве нового субъекта;

– как уже зарегистрированный пользователь системы – подавать запрос о распознании системой управления идентификационными данными и получать одобрение для доступа к услугам или использования доступных в домене применения ресурсов, связанных с системой управления идентификационными данными;

– как объект наблюдения при получении идентификационной информации – способствовать наблюдению.

Примечание — Что касается объекта наблюдения, полученная идентификационная информация является анонимной, пока не установлена ее связь с субъектом.

Субъект может использовать систему управления идентификационными данными для следующих целей:

– подавать запрос о распознании посредством информации в системе управления идентификационными данными и получать одобрение для доступа к услугам или использования доступных в домене применения ресурсов, связанных с системой управления идентификационными данными;

– быть информированным, как физическое лицо, об относящейся к нему идентификационной информации, которая содержится в системе управления идентификационными данными;

фикационными данными, и подавать запрос об исправлении любых ошибок в идентификационной информации.

Примечание — В определенных надлежащим образом условиях от имени принципала может действовать юридически уполномоченный представитель.

5.3.2.3 Орган управления идентификационными данными

Орган управления идентификационными данными связан с доменом применения, обладая обязанностями и возможностями определения и корректирования целей для управления идентичностями в этом домене и установления политик управления для выполнения этих целей.

Орган управления идентификационными данными использует политики, чтобы регулировать использование зарегистрированной идентификационной информации. Политики могут определять уровни услуг, которые будут предоставляться, включая уровень доверия, который может обеспечиваться системой управления идентификационными данными. Политики могут также определять способы получения авторизации для доступа и модификации идентификационной информации в непредвиденных обстоятельствах.

Орган управления идентификационными данными должен определять цели управления идентичностями для домена применения, обслуживаемого системой управления идентификационными данными, действующей под его управлением. Орган управления идентификационными данными должен определять политики для достижения целей управления идентичностями для соответственного домена применения.

Обязанности органа управления идентификационными данными включают следующее:

– создание, модификация или аннулирование операционных политик;

– обеспечение соответствия политик и функционирования системы управления идентификационными данными требованиям нормативных правовых актов;

– запрос и утверждение модификации механизмов для установления требуемого уровня доверия к аутентификации сущности с целью доступа к идентификационной информации и функциям управления системой;

– реагирование на инциденты;

– утверждение изменений типов информации, зафиксированных в реестре идентичностей;

– инициирование регулярных аудитов;

– оценивание отчетов о результатах аудита, в частности, посвященных эффективности политик.

Орган управления идентификационными данными может вступать в официальный союз с одним или несколькими другими органами управления идентификационными данными с целью формирования «объединения».

Примечание — Цель объединения органов управления идентификационными данными состоит в том, чтобы расширить домен применения для субъектов, охватывая другие домены применения. Это расширение достигается при строго контролируемом совместном использовании идентификационной информации.

В объединении каждый орган управления идентификационными данными данных должен:

– обеспечивать уровень доверия к идентификационной информации, соответствующий указанному требованию любого другого члена объединения;

– поддерживать управление доступом к идентификационной информации, содержащейся в его системе управления идентификационными данными;

– удостоверяться в том, что уровень доверия, реализуемый любым другим членом объединения при санкционировании доступа к идентификационной информации в объединенных системах управления идентификационными данными, соответствует его требованиям в отношении доступа к собственной идентификационной информации;

– оперировать общими политиками обмена информацией;

– определять политики для поддержания своей уверенности в достигаемом уровне доверия к аутентификации идентификационных данных.

Примечания

1 Обычно в объединении некоторые политики управления идентификационными данными, особенно касающиеся санкционирования доступа, будут частью соглашения между органами управления идентификационными данными участвующих доменов.

2 Политики управления идентификационными данными, используемые во многих доменах применения, могут устанавливаться межгосударственными стандартами.

3 Изменения структуры, организации и степени объединения могут зависеть от внешних ограничений, таких как правовые или нормативные требования или разрешение контролирующих органов.

4 Члены объединения могут договориться о делегировании операционных обязанностей органа управления идентификационными данными данных общему оператору, называемому «органом объединения».

5.3.2.4 Орган регистрации идентификационных данных

Орган регистрации идентификационных данных – это действующий субъект в системе управления идентификационными данными, обладающий обязанностями и возможностями установления и обеспечения соблюдения операционных политик, связанных со сбором, фиксированием и обновлением идентификационной информации в реестре идентичностей.

Политики регистрации идентификационных данных должны идентифицировать различные типы модификации идентификационной информации, а также операционные условия и условия, связанные с обеспечением безопасности, при которых такие модификации разрешены. Эти политики должны определять процедуры достижения уровня доверия к собранной идентификационной информации.

Обязанности органа регистрации идентификационных данных включают следующее:

– модификация, создание или аннулирование операционных политик;

– утверждение изменений типов информации, зафиксированных в репозитории;

– утверждение модификации идентификационной информации, зафиксированной в репозитории.

5.3.2.5 Полагающаяся сторона

Полагающаяся сторона – это действующий субъект, полагающийся на идентификационную информацию конкретного принципала, предоставленную системой управления идентификационными данными. Полагающаяся сторона использует проверенную информацию для предоставления доступа к находящимся под ее контролем услугам и ресурсам.

Обязанности полагающейся стороны включают следующее:

– обработку и хранение идентификационной информации в соответствии с установленными органом управления идентификационными данными политиками, в особенности в отношении защиты персональных данных;

– определение необходимого уровня доверия к идентификационной информации, используемой для управления доступа, соразмерного ценности конкретных ресурсов и услуг;

– предоставление информации о своих взаимодействиях с системой управления идентификационными данными для аудиторских целей.

5.3.2.6 Орган идентификационной информации

Орган идентификационной информации – это действующий субъект в системе управления идентификационными данными, предоставляющий официальный статус идентификационной информации, предоставляемой полагающимся сторонам. Орган идентификационной информации предоставляет идентификационную информацию сущностей, известных в данном домене. С операционной точки зрения орган идентификационной информации может быть поставщиком услуг, задействованным для предоставления официальных метаданных, связанных с идентификационной информацией. Метаданные могут дополняться информацией, предназначенной для установления их подлинности, например, путем аутентификации данных.

Домен применения может поддерживать один или несколько органов идентификационной информации. Орган идентификационной информации может отличаться от органа управления идентификационными данными. Независимый поставщик услуг может выполнять функции органа идентификационной информации.

Примечание — Делегирование полномочий по предоставлению идентификационной информации независимому поставщику услуг обычно включает соглашение об уровне услуг.

Процедуры установления сущности в качестве органа идентификационной информации выходят за рамки сферы рассмотрения настоящего стандарта.

Документально оформленный проект системы управления идентификационными данными должен определять политики вместе с процедурами и критериями для определения уровня доверия к информации, которая может быть получена от конкретного органа идентификационной информации. В этих политиках должны учитываться следующие критерии:

– качество подтверждения идентификационных данных;
– уровень доверия к информации, зафиксированной при внесении в реестр;
– качество генератора ссылочных идентификаторов (см. 5.4.2.3);
– качество поддержки идентификационной информации;

– характер процедур, используемых для получения значений атрибутов;

– синтаксис и семантика атрибутов;

– обеспечение безопасности системы управления идентификационными данными;

– качество защищенных протоколов связи, используемых для предоставления.

Документально оформленный проект системы управления идентификационными данными должен определять политики добавления, удаления и оценивания органа идентификационной информации, применимые для поддержки функционирования системы управления идентификационными данными. Эти политики должны рассматривать вопрос поддержки требуемого уровня доверия в случае замены конкретного органа идентификационной информации на другого.

Если система управления идентификационными данными поддерживает такое использование, документально оформленный проект системы управления идентификационными данными должен определять политики устранения разногласий в идентификационной информации для одной и той же сущности, которая была одновременно получена от двух разных органов идентификационной информации.

5.3.2.7 Поставщик идентификационной информации

Поставщик идентификационной информации – это действующий субъект в системе управления идентификационными данными, который предоставляет идентификационную информацию для конкретной сущности.

Основные обязанности поставщика идентификационной информации включают следующее:

– сбор идентификационных данных, в том числе содержащих персональные данные, у субъектов;

– обеспечение уверенности в том, что сбор персональных данных соответствует действующему законодательству и политикам системы;

– информирование субъекта о персональных данных, сбор которых будет осуществляться, об использовании этих персональных данных и любых третьих сторонах, которым будет передаваться персональные данные;

– получение согласия субъекта на сбор персональных данных;

– перевод необходимых идентификационных данных в идентификационную информацию, которая используется системой управления идентификационными данными для идентификации субъектов;

– перевод идентификационной информации в формат идентификационной записи и хранение записи в реестре идентификационных данных системы управления идентификационными данными;

– поддержка идентификационной информации в реестре идентификационных данных с целью отражения изменений, которые могут происходить в идентификационных данных субъектов;

– извлечение идентификационной информации из реестра идентичностей и предоставление ее полагающимся сторонам;

– обеспечение минимизации идентификационной информации, передаваемой другим сторонам, путем удаления чувствительной, с точки зрения безопасности персональных данных, информации, если это специально не требуется и не санкционировано в целях обработки стороной, которой предоставляется идентификационная информация.

Примечание — Несмотря на то, что за установление и утверждение политик, относящихся к вышеупомянутым вопросам, отвечает орган управления идентификационными данными, за их реализацию и функционирование отвечает поставщик идентификационной информации.

Документально оформленный проект системы управления идентификационными данными должен определять политики наблюдения, вычисления, генерации и предоставления идентификационной информации, которые определяют уровень доверия к процессу, соизмеримый с уровнем доверия к результирующей идентификационной информации. В ИСО/МЭК 29003 представлено руководство по процессам получения идентификационной информации.

Поставщик идентификационной информации может также создавать метаданные, описывающие идентификационную информацию, которые могут включать следующее:

– описание типов идентификационных атрибутов, значения которых составляет идентификационную информацию;

– формат(-ы) названий атрибутов и значений атрибутов, подходящий(-е) для отображения на экране;

– подробности структуры и формата идентификационной информации, используемых системой управления идентификационными данными для хранения и передачи;

– дата и время создания идентификационной информации;

– дата и время истечения срока действия идентификационной информации;

– ссылка на источник идентификационной информации;

– криптографические данные, используемые для обеспечения защиты конфиденциальности и целостности хранящейся и передаваемой идентификационной информации и любых связанных с ней метаданных.

Поставщик идентификационной информации может создавать мандат, который будет использоваться при аутентификации субъекта – держателя мандата. Мандат может содержать криптографические данные, созданные органом идентификационной информации. Мандат может иметь форму физического токена, содержащего идентификационную информацию в удобочитаемом виде.

Выпуск физических мандатов выходит за рамки сферы рассмотрения настоящего стандарта.

5.3.2.8 Проверяющая сторона

Проверяющая сторона – это действующий субъект в системе управления идентификационными данными, отвечающий за установление точности, достоверности и действительности идентификационной информации, относящейся к конкретной сущности.

Деятельность проверяющей стороны может включать проверки с использованием предоставляемых сущностью свидетельств идентичности. Если свидетельство идентичности поддерживается мандатом, проверяющая сторона должна устанавливать временную действительность идентификационной информации, которую содержит мандат.

Система управления идентификационными данными может содержать много дополняющих друг друга проверяющих сторон. Во избежание неоднозначности в документально оформленном проекте необходимо следующее:

– действующий субъект, специализирующийся на проверке с использованием предоставленных свидетельств идентичности, должен классифицироваться как «проверяющая сторона для процесса подтверждения»;

– действующий субъект, специализирующийся на установлении того, что сущность является той сущностью, как было ею заявлено в ходе процесса аутентификации, должен классифицироваться как «проверяющая сторона для процесса аутентификации»;

– действующий субъект, в основном использующий официальную идентификационную информацию, предоставленную внешней системой управления идентификационными данными, должен классифицироваться как «пользователь утверждения».

Примечание — Проверяющая сторона для процесса подтверждения связана с процессом подтверждения идентификационных данных во время внесения в реестр. Ее правильное функционирование обеспечивает основу для правильного функционирования системы управления идентификационными данными.

5.3.2.9 Аудитор

Роль аудитора заключается в подтверждении соответствия функционирования системы управления идентификационными данными документально оформленным политикам и процедурам, а также правовым и иным налагаемым внешним требованиям. Аудитор в большинстве случаев сообщает свои заключения органу управления идентификационной информации, но может быть обязан сообщать свои заключения о соответствии правовым и налагаемым внешним требованиям и регулятивному органу, а также иным внешним органам.

Примечание — Аудит обычно включает изучение и анализ записей об операциях и транзакциях системы и, соответственно, зависит от доступности таких записей.

Вопросы, имеющие отношение к аудитору, включают следующее:

– документирование политик функционирования системы управления идентификационными данными;

– доступность записей об управлении идентификационными данными на всех уместных этапах транзакций управления идентичностями, включая сбор, хранение, использование, передачу и утилизацию идентификационной информации;

– однозначные и достижимые критерии проведения аудитов.

Обязанности аудитора включают следующее:

– в качестве представляющего отчеты лица – периодическая подготовка отчетов, описывающих операции, осуществляемые системой управления идентификационными данными, особенно в отношении соответствия операционным политикам;

– в качестве лица, осуществляющего мониторинг – своевременное получение отчетов о конкретных операциях, осуществляемых системой управления идентификационными данными, с целью осуществления оценки, соответствуют ли операции применимым политикам, и доведение органу управления идентификационными данными о любых несоответствиях;

– в качестве консультанта – предоставление органу управления идентификационными данными рекомендаций о возможных усовершенствованиях операционных политик и обеспечения их соблюдения;

– в качестве надзорного органа – предоставление отчетов внешним сторонам, в том числе регулятивным органам, о соответствии операций применимым политикам, правилам и предписаниям.

5.3.3 Контекстная модель

На рисунке 1 изображена контекстная модель системы управления идентификационными данными, показывающая причастные стороны, являющиеся и не являющиеся действующими субъектами, как определено в настоящем стандарте.

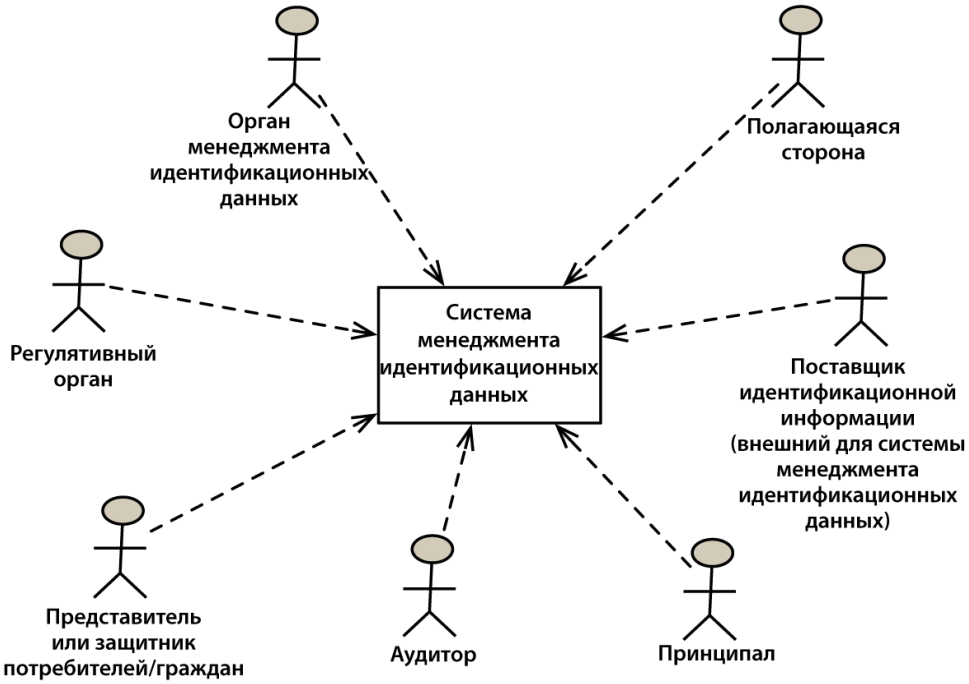

Рисунок 1 – Контекстная модель управления идентификационными данными

Документально оформленный проект должен определять конкретные представления причастных сторон и действующих субъектов, определенных в 5.3.1 и 5.3.2, соответственно. Документально оформленный проект может добавлять дополнительные причастные стороны или действующих субъектов. Он может определять причастные стороны и действующих субъектов, которые идентифицированы на рисунке, с несколькими различными представлениями.

5.3.4 Модель вариантов использования

5.3.4.1 Общие сведения

Модель вариантов использования определяет взаимодействия действующих субъектов с системой управления идентификационными данными. Она идентифицирует функциональные требования.

Рисунок 2 иллюстрирует простой вариант использования с действующими субъектами, взаимодействующими с системой управления идентификационными данными, которая используется полагающейся стороной для управления доступом к услугам и ресурсам в ее домене применения. Расширенные варианты использования и связанные с ними диаграммы компонентов, охватывающие основные аспекты системы управления идентификационными данными, включены в приложение В.

На рисунке 2 изображены:

– субъект, устанавливающий взаимосвязь с системой управления идентификационными данными, находящейся под контролем органа управления идентификационными данными;

– субъект, предоставляющий идентификационную информацию полагающейся стороне с целью получения доступа к ресурсам;

– полагающая сторона, делающая запрос об аутентификации субъекта;

– полагающаяся сторона, запрашивающая атрибуты аутентифицированного принципала;

– полагающаяся сторона, предоставляющая доступ к ресурсам, находящимся под ее контролем;

– субъект, получающий доступ к ресурсам, находящимся под контролем полагающейся стороны.

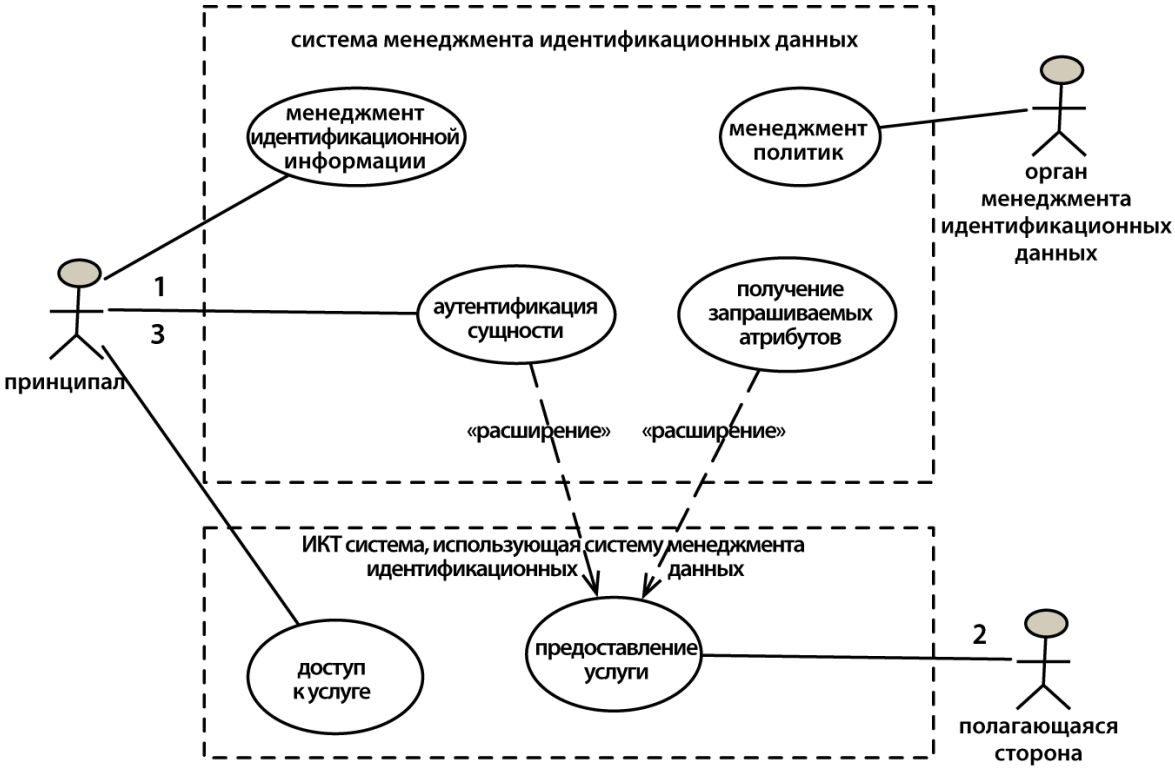

Рисунок 2 – Базовый вариант использования идентификационной информации

Диаграмма типового варианта использования на рисунке содержит административную деятельность (управление идентификационными данными, управление политиками) и деятельность, связанную с доступом к ресурсам, которая включает получение идентификационной информации и аутентификацию.

Для того, чтобы облегчить описание функциональных требований из вариантов использования, вариант использования и функциональное представление могут представлять действующих субъектов как сущностей, принадлежащих разным сообществам. Сообщество представляет общие интересы в вопросе эксплуатации системы управления идентификационными данными. Сообщества включают:

- пользователей организации;
- привилегированных пользователей (администраторов);
- пользователей, не относящихся к организации.

Сущности, не являющиеся физическими лицами, тоже могут запрашивать доступ к ресурсам автоматизированной (информационной) системы, который потребует аутентификации сущности. Сущности, не являющиеся физическими лицами, могут включать устройства, а также логические сущности, такие как сервисы и программные средства.

5.3.4.2 Варианты использования, связанные с сотрудниками

Сотрудники организации используют систему для извлечения информации. Согласие на обработку информации и доступ к ней является явным.

На основе порученных служебных обязанностей сотрудники ожидают от системы управления идентификационными данными точной идентификационной информации и доступа к идентификационной информации. С точки зрения сотрудников, информация должна быть получена точным образом, подтверждающим о целостности ее происхождения и поддержки.

5.3.4.3 Варианты использования, связанные с работодателем (оператором)

У работодателя есть обязанности по осуществлению управления компонентами системы. Во взаимодействиях с системой управления идентификационными данными работодатель может рассматриваться таким же образом как сотрудник. (см. 5.3.4.2)

С точки зрения работодателя идентификационная информация должна поддерживаться и обрабатываться только при наличии согласия.

5.3.4.4 Варианты использования, связанные с принципалом

В вариантах использования, связанных с субъектом, наиболее важна однозначная идентификация. Доступ к информации осуществляется либо субъектом, либо по поручению субъекта, либо коммерческими сторонами с явного согласия.

Варианты использования, связанные с применением системы для целей функционирования, отличных от тех, которые идентифицированы в документально оформленном проекте., описывают риски — злоупотребления идентификационной информацией в системе управления идентификационными данными и возможные способы их уменьшения. Для решения этих вопросов варианты использования, связанные с целевым потребителем, обычно описывают аспект обеспечения соответствия правовым и нормативным требованиям.

Вариант использования, связанный с субъектом, может описывать конкретный процесс повторного внесения сущности в реестр с целью повторного установления ее идентификационных данных, который включает процессы обновления любой идентификационной информации, хранящейся у полагающихся сторон.

С точки зрения субъекта, доступ к идентификационной информации должен осуществляться безопасным образом, предотвращающим любую утечку информации. Поскольку информация собирается с конкретной целью, любое иное использование должно происходить с согласия субъекта. Должна обеспечиваться защита информации от риска искажения и разглашения.

5.3.4.5 Варианты использования, связанные с устройством

Варианты использования, связанные с устройством, описывают использование устройств как субъектов в системе управления идентификационными данными. Устройства обычно действуют от имени или под контролем других сущностей, которые могут являться или не являться субъектами. В вариантах использования, связанных с устройством, должны рассматриваться риски утраты физического контроля или компрометации целостности устройства.

С точки зрения устройства, должна обеспечиваться защита идентификационной информации от риска искажения или разглашения.

5.3.5 Модель соответствия и управления

Модель соответствия и управления показывает концептуальные механизмы, которые могут использоваться для выполнения нормативных и иных внешних ограниче-

ний, налагаемых на систему управления идентификационными данными. Это включает следующие обязательные условия:

– обеспечение уверенности в точности получаемой идентификационной информации контролируемых сущностей на соответствующем уровне доверия не только при инициализации, но и в течение полного срока действия идентификационной информации субъекта;

– обеспечение уверенности в уникальности идентификационной информации, относящейся к конкретному субъекту;

– обеспечение уверенности в точном получении идентификационной информации;

– обеспечение уверенности в том, что доступ к различным видам идентификационной информации ограничивается пользователями с санкционированным доступом к данному виду информации и аутентифицированным на соответствующем уровне доверия;

– обеспечение уверенности в том, что доступ к идентификационной информации фиксируется и доступен для аудита;

– предотвращение обработки идентификационной информации и доступа к ней без согласия принципала в рамках локальных, региональных и федеральных норм;

– соблюдение локальных, региональных и глобальных предписаний и выполнение требований соответствия и управления.

5.4 Функциональное представление

5.4.1 Компонентная модель

5.4.1.1 Общие сведения

Документально оформленный проект системы управления идентификационными данными может интерпретировать описанные ниже компоненты. В приложении В представлена диаграмма, показывающая компоненты системы управления идентификационными данными и их взаимодействия. Документально оформленный проект определяет каждый компонент, необходимый для выполнения операционных требований для концепций, идентифицированных в его архитектурных представлениях.

Документально оформленный проект системы управления идентификационными данными должен описывать операционные элементы системы, в том числе причастные

стороны, действующие субъекты, структуры данных, функциональные компоненты и интерфейсы. Определяемые структуры данных должны включать следующее:

– криптографические ключи (при наличии) и свойства, сервисы обнаружения и политики, а также другие возможности и требования;

– синтаксис и семантику данных идентификационных атрибутов, а также, где это применимо, правила преобразования в эквивалентные представления идентификационных данных в других системах;

– структуры данных, используемые в транзакциях, такие как аутентификационные запросы, утверждения и сеансовые ключи.

5.4.1.2 Сущность

Сущность – это действующие субъекты в системе управления идентификационными данными, которые получают доступ к услугам и ресурсам, доступным в домене применения.

Требования, определяющие доступ к услугам и ресурсам, доступным в домене применения, рассматриваются в ИСО/МЭК 29146.

5.4.1.3 Реестр идентичностей

Назначение реестра идентичностей состоит в предоставлении официальных ссылок на идентификационную информацию в домене системы управления идентификационными данными. Реестр идентичностей может быть реализован различными способами, например, он может быть централизованным или распределенным. Некоторая идентификационная информация в реестре идентичностей может также храниться в устройстве, которым владеет сама сущность, например, на смарт-карте.

Документально оформленный проект системы управления идентификационными данными должен определять механизм управления доступом к идентификационной информации, содержащейся в реестре идентичностей (см. 6.2).

Идентификационная информация, определяющая идентичность сущности, может храниться в реестре идентичностей в одной или нескольких записях. Разбиение идентификационной информации на несколько записей может основываться на ряде факторов, которые могут включать:

– различия условий доступа, например, для реализации минимального раскрытия информации;

– различия длительности хранения идентификационной информации в реестре идентификационных данных;

– различия места хранения, например в централизованном репозитории и/или на персональном устройстве.

Структура хранения данных для идентификационной информации и методы реализации реестра идентичностей выходят за рамки сферы рассмотрения настоящего стандарта.

5.4.2 Процессы и сервисы

5.4.2.1 Документация

Описание компонентов и операций в документально оформленном проекте должно быть основано на терминологии, представленной в таблицах в данном пункте.

Документально оформленный проект должен включать UML диаграммы для описания процессов.

Примечание — Диаграммы, представленные в приложении С настоящего стандарта, могут быть использованы в качестве шаблона.

Документально оформленный проект может определять реализацию с использованием компонентов, которые выполняют подмножество процессов в приведенных таблицах.

5.4.2.2 Процессы управления идентификационной информацией

5.4.2.2.1 Общие сведения

Обработка информации в системе управления идентификационными данными включает (но не ограничивается) следующие процессы:

– предоставление идентификационной информации;

– обработка идентификационной информации;

– предоставление доступа к обработке идентификационной информации.

Примечание — Приведенные процессы относятся к идентификационной информации, присутствующей в реестре идентификационных данных. Процессы ввода идентификационной информации здесь не описываются (см. ИСО/МЭК 29003).

В таблице 1 представлен обзор обмена информацией в системе управления идентификационными данными, который связан с описываемыми в данном подразделе процессами.

Таблица 1 – Обзор обмена информацией в процессах управления идентификационной информацией

Процесс	**Действующие субъекты**			
	Источник		**Получатель**	
	Элемент архитектуры	**Деятельность**	**Элемент архитектуры**	**Деятельность**
Обработка идентификационной информации	Поставщик идентификационной информации	Применяет операции обработки информации	Поставщик идентификационной информации	Сохраняет результаты
			Реестр	Хранит результаты обработки, возможно обновляя информацию одних или нескольких идентификационных атрибутов
Предоставление права на обработку идентификационной информации	Орган управления идентификационными данными	Информирует об обработке идентификационной информации. Требует авторизации для операций обработки	Принципал	Предоставляет право или отказывает в праве на операции обработки информации
	Принципал	Запрашивает информацию об обработке идентификационных данных	Орган управления идентификационными данными	Предоставляет запрашиваемую информацию
Предоставление	Полагающаяся сторона	Делает запрос об услугах	Орган управления	Разрешает услугу

Окончание таблицы 1

Процесс	Действующие субъекты			
	Источник		Получатель	
	Элемент архитектуры	Деятельность	Элемент архитектуры	Деятельность
		предоставления	ционными данными	предоставления или отказывает в ней, определяет условия
			Поставщик идентификационной информации	Фиксирует полагающуюся сторону как получателя услуги предоставления
	Поставщик идентификационной информации	Передает идентификационную информацию	Полагающаяся сторона	Применяет обновленную информацию к своему процессу обслуживания
	Орган идентификационной информации	Дополняет идентификационную информацию утверждением об уровне доверия	Полагающаяся сторона	Подтверждает действительность утверждений и соответствие ее требованиям для уровня доверия

5.4.2.2.2 Поддержка идентификационной информации

Предоставление идентификационной информации представляет собой процесс предоставления обновленной идентификационной информации, относящейся к субъектам, когда созданы идентификационные данные или ранее предоставленная информация больше не верна. Управление доступом к идентификационной информации осуществляется путем разрешений, которые даются полагающейся стороне.

Документально оформленный проект должен определять процедуры и условия для инициирования предоставления полагающейся стороне.

5.4.2.2.3 Предоставление идентификационной информации

Обработка идентификационной информации должна осуществляться в соответствии с политиками. Обработка идентификационной информации может генерировать новую идентификационную информацию посредством доступа к идентификационной информации, относящейся к одному или более субъектам.

5.4.2.2.4 Предоставление права доступа к обработке идентификационных данных

Управление доступом к идентификационной информации для обработки идентификационной информации и к генерируемой информации должно осуществляться в соответствии с применимыми политиками.

5.4.2.3 Специальные процессы управления идентификационной информацией

5.4.2.3.1 Общие сведения

В этом подразделе определяются дополнительные процессы, характерные для различных реализаций системы управления идентификационными данными. Они включают следующее:

– аудит;
– генерация ссылочных идентификаторов; и
– признание недействительности.

В таблице 2 представлен обзор обмена информацией в системе управления идентификационными данными, который связан с описываемыми в данном подразделе процессами.

Таблица 2 – Обзор обмена информацией в специальных процессах управления идентификационной информацией

Процесс	**Действующие субъекты**			
	Источник		**Получатель**	
	Элемент архитектуры	**Деятельность**	**Элемент архитектуры**	**Деятельность**
Аудит	Орган управления идентификационными данными	Определяет действия, подлежащие регистрации, и инциденты, о которых следует сообщать	Все действующие субъекты	Включают определения в реализацию процесса
	Принципал	Регистрирует жалобы	Аудитор	Расследует

Продолжение таблицы 2

Процесс	Действующие субъекты			
	Источник		Получатель	
	Элемент архитектуры	Деятельность	Элемент архитектуры	Деятельность
				жалобы
	Орган управления идентификационными данными	Поддерживает контрольный журнал действий, связанных с управлением		Проверяет контрольные журналы и инциденты
	Реестр идентификационных данных	Поддерживает контрольный журнал операций доступа к данным		
	Поставщик идентификационной информации	Поддерживает контрольный журнал запросов идентификационной информации и мероприятий предоставления информации		
	Орган идентификационной информации	Поддерживает контрольный журнал предоставляемых утверждений об обеспечении доверия Сообщает об инцидентах		
	Аудитор	Представляет отчет о заключениях. Рекомендует изменения	Орган управления идентификационными данными	Корректирует политики и процедуры с целью реализации любых рекомендованных изменений
Генерация ссылочных идентификаторов	Поставщик идентификационной информации	Запрашивает ссылочный идентификатор	Генератор ссылочных идентификаторов	Генерирует ссылочный идентификатор
	Принципал	Предоставляет	Генератор	Подтверждает

Окончание таблицы 2

Процесс	Действующие субъекты			
	Источник		Получатель	
	Элемент архитектуры	Деятельность	Элемент архитектуры	Деятельность
		идентификационную информацию, которая будет использоваться в качестве ссылочного идентификатора	ссылочных идентификаторов	пригодность предоставленной идентификационной информации в качестве ссылочного идентификатора. Генерирует ссылочный идентификатор
	Генератор ссылочных идентификаторов	Предоставляет сгенерированный ссылочный идентификатор	Поставщик идентификационной информации	Связывает ссылочный идентификатор с другой идентификационной информацией
Признание недействительности идентификационной информации	Аудитор	Представляет отчет о заключениях. Рекомендует изменения	Орган управления идентификационными данными	Утверждает признание недействительности
	Принципалы	Идентифицирует ошибки	Поставщик идентификационной информации	Исправляет информацию
	Поставщик идентификационной информации	Информирует об изменениях	Принципалы	Подтверждают и признают действительным уведомление об изменениях
			Полагающаяся сторона	Подтверждает уведомление об изменениях

5.4.2.3.2 Аудит

С течением времени действующие субъекты и компоненты должны подвергаться аудиту для проверки правильности функционирования в своей роли в системе управления идентификационными данными:

– реестр идентификационных данных и генератор ссылочных идентификаторов должны постоянно подвергаться аудиту для проверки точности их мер защиты целостности;

– поставщик идентификационной информации должен регулярно подвергаться аудиту для проверки точности его процедур контроля при предоставлении идентификационной информации;

– орган идентификационной информации должен регулярно подвергаться аудиту для проверки точности его процедур контроля при осуществлении управления идентификационной информацией.

Аудиторы могут сертифицироваться посредством аккредитованного процесса контроля их проверок действующих субъектов и компонентов системы управления идентификационными данными.

5.4.2.3.3 Генерация ссылочных идентификаторов

В рамках регистрации идентификационных данных создается ссылочный идентификатор, который связывается с идентификационной информацией соответствующей сущности. Генератор ссылочных идентификаторов активируется с помощью любой необходимой доступной идентификационной информации и создает значение идентификатора. Ссылочный идентификатор фиксируется вместе с другой идентификационной информацией в реестре идентичностей.

5.4.2.3.4 Признание недействительности

Документально оформленный проект системы управления идентификационными данными может определять условия и процедуры признания недействительности идентификационной информации.

Примечание – Признание недействительности идентификационной информации означает признание недействительности любых доказуемых утверждений, например, с помощью криптографии, о достоверности идентификационной информации, которая могла быть записана пользователем этой информации. На практике удаление доказуемого утверждения приводит к аннулированию информации.

Дополнительно могут приниматься во внимание следующие условия:

– было обнаружено, что свидетельство идентичности неверно оценено как действительное либо мошенническим образом, либо посредством неверных процедур;

– были обнаружены ошибки при присвоении или распознании атрибутов;

– произошли изменения политик, связанных с внесением в реестр или идентификацией;

– идентификационная информация субъекта была использована кем-то другим, так что требуется повторное установление новой совокупности идентификационной информации.

Механизм признания недействительности, если таковой поддерживается, должен осуществляться в соответствии с политикой признания недействительности. Эта политика должна рассматривать следующее:

– условия и механизмы признания недействительности;

– уровень доверия для сообщений о признании недействительности;

– условия и механизмы информирования субъекта о признании недействительности атрибута в каких-то его идентификационных данных;

– механизм реагирования на запросы о недействительном статусе атрибута.

5.4.2.4 Дополнительные функции

5.4.2.4.1 Общие сведения

Документально оформленный проект системы управления идентификационными данными может определять дополнительные функции, описанные в данном подразделе. Они включают следующее:

– профилирование идентификационной информации;

– получение согласия;

– поиск (нахождение) органа идентификационных данных;

– публикация.

В таблице 3 представлен обзор обмена информацией в системе управления идентификационными данными, который связан с описываемыми в данном подразделе процессами.

Таблица 3 – Обзор информации, которой обмениваются в дополнительных функциях системы управления идентификационными данными

Процесс	Действующие субъекты			
	Источник		Получатель	
	Элемент архитектуры	Деятельность	Элемент архитектуры	Деятельность
Профилирование идентификационной информации	Поставщик идентификационной информации	Определяет профиль для типа сущностей	Поставщик идентификационной информации	Реализует профиль идентификационных данных
Согласие для обеспечения прав субъектов персональных данных	Принципал	Делает запрос о просмотре или скрытии атрибута идентификационной информации	Поставщик идентификационной информации	Проверяет политику осуществления запроса, реализует соответствующие изменения, представляет информацию
Нахождение органа идентификационных данных	Орган регистрации идентификационных данных	Делает запрос об установлении доверия с другим органом идентификационных данных	Полагающаяся сторона	Проверяет приемлемость запроса о доверии
	Полагающаяся сторона	Представляет на рассмотрение запрос о доверии	Орган идентификационной информации	Подтверждает установление доверия
	Орган идентификационной информации	Утверждает поставку идентификационной информации	Поставщик идентификационной информации	Поставляет идентификационную информацию
Публикация	Орган управления идентификационными данными	Устанавливает политику публикации	Орган идентификационной информации	Утверждает политику публикации
	Поставщик идентификационной информации	Реализует утвержденную политику публикации	Полагающаяся сторона	Получает опубликованную информацию

5.4.2.4.2 Сервис профилирования идентификационной информации

Сервис профилирования идентификационной информации обеспечивает соответствующее представление идентификационной информации для сущностей данного типа, т.е. физические лица, устройства и организации. Это может включать определение, поддержку и использование различных идентификационных атрибутов и форматов идентификационных данных для различных типов сущностей.

5.4.2.4.3 Получение согласия

Процесс получения согласия субъектов может обеспечивать следующие функции:

– аутентификации сущности как известного и авторизованного субъекта для получения доступа к идентификационной информации;

– представление зафиксированной идентификационной информации;

– модификация, расширение или удаление идентификационной информации, предоставленной ранее субъектом;

– запрос о модификации сгенерированной идентификационной информации;

– уведомление субъекта о намеченном использовании идентификационной информации.

5.4.2.4.4 Нахождение органа идентификационной информации

Процесс поиска органа идентификационной информации обеспечивает возможность обнаружения других органов идентификационной информации и установления сотрудничества с целью доступа к идентификационной информации на требуемом уровне доверия.

Этот сервис идентифицирует кандидатуры сторонних органов идентификационной информации и определяет условия процессов подписки и уведомления для этих органов.

Сервис нахождения органа идентификационной информации может обеспечивать следующие функции:

– одобрение другого органа идентификационной информации с целью установления доверительных отношений на основе требований, установленных в компонентах обеспечения качества и соответствия;

– признание сущности как разрешенного пользователя идентификационной информации;

– определение типа необходимой идентификационной информации;

– определение требуемого уровня доверия для доступа к идентификационной информации;

– определение механизмов обеспечения безопасности для защиты предоставляемой идентификационной информации;

– определение идентификатора, для которого нужно уведомление об идентификационной информации;

– получение запрашиваемой идентификационной информации;

– получение идентификационной информации, когда такая информация изменяется.

Список функций, которые может включать сервис поиска, зависит от доверия, установленного с другим органом, и от условий этого доверия.

5.4.2.4.5 Публикация

Процесс публикации обеспечивает возможность публикации идентификационной информации для обслуживания запрашивающих сторон и установления сотрудничества с целью доступа к идентификационной информации на требуемом уровне доверия. Сервисы подписки и уведомления тоже являются частью сервиса публикации.

Сервис публикации может обеспечивать следующие функции:

– публикация и модификация публикации сервиса предоставления идентификационной информации, а также определение условий доступа и использования такой информации;

– признание запрашивающей стороны, которой будет предоставляться идентификационная информация на основе требований, установленных в компонентах обеспечения качества и соответствия;

– признание сущности как пользователя идентификационной информации;

– определение типа идентификационной информации, к которой разрешается доступ;

– определение требуемого уровня доверия для доступа к идентификационной информации;

– определение механизмов обеспечения безопасности для защиты предоставляемой идентификационной информации;

– определение идентификатора, для которого нужно уведомление об идентификационной информации;

– информирование об изменениях идентификационной информации, когда таковые происходят.

Список функций, которые может включать сервис публикации, зависит от требований доступа к этой информации.

5.4.3 Физическая модель

Это представление описывает реализацию каждого элемента систем управления идентификационными данными, которые обеспечивают функциональные возможности для реализации процессного представления. Физическое представление может представлять альтернативные физические реализации, т. е. отличающиеся по стоимости и качеству функционирования.

Настоящий стандарт рассматривает физическое представление только на уровне структурных компонентов. Аспекты реализации физического представления выходят за рамки сферы рассмотрения настоящего стандарта.

5.5 Сценарии управления идентификационными данными

5.5.1 Общие сведения

Развертывание системы управления идентификационными данными может происходить в соответствии с различными сценариями. Сценарий развертывания оказывает влияние на управление системой управления идентификационными данными. Сценарий развертывания будет определять доверительные отношения, которые должны существовать между сторонами, участвующими в эксплуатации и управлении системой управления идентификационными данными.

Сценарий развертывания может выбираться при расширении существующей системы управления идентификационными данными. Модель развертывания расширения может отличаться от исходной модели развертывания.

Различные сценарии, которые могут быть использованы для реализации системы управления идентификационными данными, включают следующее:

- сценарий организации;
- сценарий объединения;
- сценарий услуг;
- неоднородный сценарий.

5.5.2 Сценарий организации

В сценарии организации система управления идентификационными данными развертывается в контексте единой организации, где доверие к ее операциям и управлению унаследовано из структуры управления организации, и организация несет ответственность за осуществление менеджмента информации, которая собирается, хранится и обрабатывается системой.

Модель организации является централизованной моделью (см. ИСО/МЭК 24760-1, [1]).

5.5.3 Сценарий объединения

Система управления идентификационными данными объединения состоит из многих подсистем с независимым управлением ими. Доверие к операциям и управление в объединении устанавливаются посредством договорного соглашения. Управление может быть делегировано организации с официальной структурой или уставом, которые содержат операционные правила, обязанности и оговоренные обязательства участвующих сторон.

Когда домен применения должен быть расширен для взаимодействия или сотрудничества с другими доменами, подход централизованного сценария будет объединять исходные домены в единый более крупный домен, контролируемый единой системой управления идентификационными данными. Сценарий объединения предлагает альтернативный подход, дающий возможность системам управления идентификационными данными осуществлять обмен идентификационной информацией между доменами, не требуя объединения доменов.

Примечание — Полная интеграция системы предписывает объединение требований двух отдельных доменов в одном новом архитектурном подходе, поддерживающем все различные архитектурные представления двух отдельных доменов. Модель объединения вместо этого оставляет структуру неизменной, но вводит новые механизмы, предназначенные для того, чтобы дать возможность двум отдельным структурам взаимодействовать друг с другом.

Механизмы, поддерживающие объединения, должны обеспечивать требуемую конфиденциальность, целостность и уровень доверия между отдельными доменами, чтобы они могли обмениваться идентификационной информацией и использовать идентификационную информацию других доменов.

5.5.4 Сценарий услуг

Независимо от сценария развертывания, будь это сценарий предприятия или объединения, функциональные компоненты в системе управления идентификационными данными могут быть реализованы как услуги.

Документально оформленный проект системы управления идентификационными данными, развернутой как модель услуг, должен определять компоненты доверия и публикации и механизмы обеспечения уверенности в достижении требуемой конфиденциальности, целостности и уровня доверия при предоставлении услуг, связанных с идентификационной информацией.

5.5.5 Неоднородный сценарий

Неоднородный сценарий представляет собой сценарий, в котором независимые организации выпускают идентификационные мандаты для субъектов, соответствующие известной спецификации и уровню доверия. Полагающиеся стороны могут использовать мандаты для аутентификации субъектов, когда сопутствующий риск считается приемлемым в соответствии с их политикой управления рисками.

6 Требования управления идентификационной информацией

6.1 Общие сведения

В данном разделе описываются требования управления идентификационной информацией системой управления идентификационными данными на основе базовой модели, типов развертывания и вовлеченных причастных сторон. В этом разделе проводится различие между функциональными требованиями, служащими для поддержки взаимодействия действующих субъектов с системой, и нефункциональными требованиями, относящимися к другим операционным условиям, которые системе управления идентификационными данными может требоваться соблюдать.

Функциональные требования включают:

- политику доступа;
- условия управления;
- условия поддержки.

Требования этого подраздела не включают меры защиты информации, являющиеся частью практических приемов (см. ИСО/МЭК 24760-3).

6.2 Политика доступа к идентификационной информации

Документально оформленный проект системы управления идентификационными данными должен регламентировать политику доступа к информации, определяющую:

– условия и механизмы доступа к значению каждого атрибута в системе;

– критерии санкционирования доступа с соответствующими уровнями доверия;

– операции доступа к идентификационной информации, требующие регистрации, и степень ее детальности;

– каким образом реестр идентичностей обеспечивает защиту содержащейся в нем идентификационной информации;

– длительность хранения записей о доступе к идентификационной информации.

6.3 Функциональные требования управления идентификационной информацией

6.3.1 Политика, связанная с жизненным циклом идентификационной информации

Документально оформленный проект системы управления идентификационными данными должен регламентировать политику управления жизненным циклом идентификационной информации, определяющую:

– требования доверия к точности идентификационной информации, необходимой для внесения в реестр;

– условия и процедура активации идентификационных данных;

– условия и процедура поддержки идентификационных данных для типовой проверки точности и правильности идентификационной информации;

– условия и процедура осуществления корректировки идентификационной информации для субъекта;

– условия и процедура приостановления действия идентификационных данных;

– условия и процедура идентификации для повторной активации идентификационных данных;

– условия и процедура удаления или архивирования идентификационных данных;

– условия и процедура поддержки информации;

– условия и процедура восстановления идентификационных данных;

– информация, предназначенная для архивирования, период архивации и условия хранения архивированных идентификационных данных;

– условия и процедура прекращения действия или удаления идентификационных данных.

6.3.2 Условия и процедуры поддержки идентификационной информации

Документально оформленный проект системы управления идентификационными данными должен определять, как поддерживается точность идентификационной информации, управление которой она осуществляет.

Документально оформленный проект системы управления идентификационными данными должен включать процедуры мониторинга качества идентификационной информации в реестре идентичностей, в особенности атрибутов, которые:

– представляют аспекты сущности, которые могут меняться с течением времени;

– могут влиять на степень доверия к зафиксированной информации.

Документально оформленный проект системы управления идентификационными данными должен обеспечивать политики, касающиеся деятельности по обнаружению изменений идентификационной информации, особенно атрибутов, значения которых могут меняться с течением времени и изменение которых может влиять на уровень доверия к зарегистрированным идентификационным данным.

Документально оформленный проект управления идентификационными данными должен обеспечивать политики поддержки целостности идентификационной информации и метаданных в реестре идентификационных данных. Такие политики могут определять:

– процедуры предотвращения искажения зарегистрированной информации;

– процедуры обнаружения искажения зарегистрированной информации;

– процедуры исправления искажения зарегистрированной информации.

Документально оформленный проект системы управления идентификационными данными должен обеспечивать реализацию механизма сообщения полагающимися

сторонами о мошенническом или подозрительном поведении в отношении реестра идентичностей.

6.3.3 Интерфейс идентификационной информации

Система управления идентификационными данными может содержать компоненты с пользовательским интерфейсом для представления идентификационной информации. Доступ к идентификационной информации на пользовательском интерфейсе должен регулироваться политикой, определяющей:

– управление доступом;

– проведение аудита.

Назначение интерфейса для представления информации включает следующее:

– представление идентификационной информации;

– представление метаданных идентификационной информации;

– представление информации по текущим и прошлым операциям системы;

– предоставление мер защиты информации при обработке или модификации представленной информации;

– применение политик, касающихся использования представленной информации, уместного для действующего субъекта.

Документально оформленный проект системы управления идентификационными данными должен определять формат и условия представления идентификационной информации в удобочитаемой для человека форме (см. 6.2). Содержащиеся в документально оформленном проекте требования о представлении идентификационной информации в удобочитаемой для человека форме должны учитывать возможности и ограничения пользователя информации.

6.3.4 Ссылочный идентификатор

Система управления идентификационными данными может содержать компонент для генерации ссылочного идентификатора. Задача ссылочного идентификатора состоит в обеспечении того, чтобы определенные идентификационные данные, известные в системе управления идентификационными данными, были уникальными.

Доступ к значению ссылочного идентификатора может ограничиваться, например, исключительно в рамках системы управления идентификационными данными. Документально оформленный проект должен определять политику доступа для ссылочного идентификатора.

Примечание — Ограниченный доступ к ссылочному идентификатору предотвращает его использование в других системах управления идентификационными данными.

Документально оформленный проект системы управления идентификационными данными должен связывать ее реестр идентичностей с генератором ссылочных идентификаторов. Генератор ссылочных идентификаторов должен генерировать уникальное значение для каждого субъекта, идентификационная информация которого хранится в реестре идентификационных данных.

Примечания

1 Обычно ссылочный идентификатор генерируется, когда сущность регистрируется в домене.

2 Генерируемый ссылочный идентификатор может быть основан на полученной от сущности информации, например, выбранный псевдоним, прошедший проверку на уникальность.

3 Ссылочный идентификатор может генерироваться, исходя из идентификационной информации для того же субъекта, полученной из другого домена, где субъект зарегистрирован. Это может включать ссылочный идентификатор из другого домена.

Хотя точный механизм генерации уникальных значений атрибутов выходит за рамки сферы рассмотрения настоящего стандарта, проект генератора ссылочных идентификаторов должен определять следующее:

– алгоритм, используемый для генерации уникального значения, вместе с аргументированным описанием его пригодности;

– интерфейс для получения нового значения либо для новой сущности, либо для имеющейся сущности таким образом, чтобы поддерживалась его уникальность;

– требования к входной информации, если таковые имеются, необходимой для алгоритма;

– требования регистрации для генерации ссылочного идентификатора при поддержке регистрации;

– меры безопасности, обеспечивающие защиту операций системы, где размещается генератор ссылочных идентификаторов.

Примечания

1 В случаях отсутствия связи или надежного взаимодействия между доменами каждый домен будет генерировать собственный ссылочный идентификатор, и предполагается, что вероятность генерации одинакового ссылочного идентификатора для того же или другого субъекта, зарегистрированного во многих доменах, будет очень мала.

2 В целом значение идентификатора в исходном домене, который не связан с системой управления идентификационными данными, не может обеспечивать выполнение критериев для нового ссылоч-

ного идентификатора и непригодно для прямого использования. Однако, когда известно, как был создан ссылочный идентификатор в определенном несвязанном домене, например, в соответствии общепризнанными нормами, такое значение ссылочного идентификатора может быть использовано при условии надежного получения его значения.

Если система управления идентификационными данными поддерживает регистрацию операций, осуществляемых генератором ссылочных идентификаторов, запись журнала регистрации должна содержать следующее:

- сгенерированный ссылочный идентификатор;
- разрешение на инициирование генерации идентификатора;
- любые данные, предоставленные в качестве входной информации;
- отметка времени.

Генератор ссылочных идентификаторов может быть сконфигурирован для генерации ссылочных идентификаторов, предназначенных для использования вне домена происхождения. В этом случае:

- значение ссылочного идентификатора должно предоставляться таким образом, чтобы обеспечивалась его целостность;
- если значение ссылочного идентификатора предоставляется в электронной форме, должно осуществляться управление доступом к нему для защиты прав субъекта (прав субъектов персональных данных);
- следует обратить внимание на обеспечение уникальности данного ссылочного идентификатора для каждой иной сущности во внешних доменах, где также используется ссылочный идентификатор;
- должна предоставляться информация для оценки уровня доверия к уникальности значения;
- следует также обратить внимание на возможные ограничения (например, правовые и нормативные) и недостатки, относящиеся к применению некоторых видов ссылочных идентификаторов за пределами их домена, таких как государственные ссылочные идентификаторы или ссылочные идентификаторы, связанные с обеспечением прав субъектов персональных данных.

6.3.5 Качество и соответствие идентификационной информации

Документально оформленный проект системы управления идентификационными данными должен определять функциональные компоненты качества и соответствия,

которые подтверждают, что полученная идентификационная информация обрабатывается с адекватными мерами защиты информации и в соответствии с:

- применимыми политиками;
- процессами и структурой обновления информации с течением времени;
- процессами разрешения вопроса ошибочного допуска к системе;
- процессами разрешения вопроса ошибочного отказа в доступе;
- требованиями применения;
- локальными, региональными и федеральными предписаниями.

6.3.6 Архивирование информации

Документально оформленный проект системы управления идентификационными данными должен обеспечивать политики, определяющие условия и процедуры архивирования идентификационной информации.

Архивированная идентификационная информация должна быть анонимной, что достигается либо путем активной анонимизации, либо устранением идентифицирующей информации.

6.3.7 Прекращение действия и удаление идентификационной информации

Документально оформленный проект системы управления идентификационными данными должен обеспечивать политики, определяющие условия и процедуры для инициирования удаления идентификационной информации:

- субъектом или сущностью, уполномоченной действовать от имени принципала;
- системой после истечения периода хранения архивированных идентификационных данных;
- органом управления идентификационных данных.

Удаленная идентификационная информация должна фиксироваться для поддержки обращений и аудита. Такая запись должна определять инициатора и причины удаления, а также любые другие метаданные, определяемые политиками удаления. Запись об удаленной идентификационной информации должна удаляться в течение некоего периода после ее создания, определяемого политикой удаления.

Примечание – Типичная реализация удаления включает архивирование идентификационной информации на переходный период, чтобы дать необходимое время для завершения удаления.

Удаление всей идентификационной информации для субъекта должно уничтожать любую информацию, которая может продолжать идентифицировать субъекта, и которая находится под контролем органа управления идентификационными данными, например, содержится в файлах журнала регистрации, контрольных журналах или резервных копиях, которые могут также храниться во внешних хранилищах. Удаление не должно считаться завершенным, пока такая дополнительная информация не удалена.

В централизованной модели, если система управления идентификационными данными осуществляет автоматическое предоставление, должно производиться уведомление об удалении информации любой полагающейся стороны, хранящей ранее полученную идентификационную информацию. По получении уведомления об удалении информации полагающаяся сторона должна удалить любую информацию, связывающую субъекта с уведомляющим доменом. В этом случае переходный период жизненного цикла, связанный с удалением, не должен считаться завершенным, пока не получено подтверждение об удалении имеющихся связей.

Примечание – Полагающаяся сторона, уведомленная об удалении информации, может сохранить поддерживаемую ей идентификационную информацию субъекта, которая не зависит от его связи с уведомляющим доменом.

6.4 Нефункциональные требования

Нефункциональные требования определяют аспекты системы управления идентификационными данными, которые не вытекают напрямую из функционального, логического или физического представления. Подробности о нефункциональных требованиях выходят за рамки сферы рассмотрения настоящего стандарта.

Однако выполнение одного или нескольких приведенных ниже нефункциональных требований может быть важным для большинства развернутых систем управления идентификационными данными:

- доступность;
- меры защиты целостности;
- качество функционирования;
- доверие к обеспечению приватности;
- применимость доступа;
- обязательства и их представление на техническом уровне;
- меры защиты привязки ко времени;

– связанные с обеспечением соответствия ограничениям, которые вытекают из договорных, нормативных (локальных, региональных и федеральных) или организационных аспектов (см. приложение А).

Документально оформленный проект системы управления идентификационными данными должен определять, насколько его реализация соответствует [5], чтобы выполнять требования доступности и времени реагирования для полагающихся сторон, обеспечивать целостность данных и, при необходимости, реализовывать меры защиты информации для обеспечения уверенности в защите конфиденциальности чувствительной, с точки зрения защиты персональных данных, информации, а также выполнять требования защиты прав субъектов.

Приложение А

(справочное)

Правовые и нормативные аспекты

Система управления идентификационными данными должна соблюдать правовые требования. В целом такие требования предписывают, чтобы система использовалась для заявленных и санкционированных целей. Например, предписания и законы, касающиеся корпоративного управления, телекоммуникаций, здравоохранения и борьбы с отмыванием денег, могут содержать требования, влияющие на управление идентификационными данными.

Орган управления идентификационными данными должен быть в курсе предписаний и законов, которые могут оказывать влияние на требования его системы управления идентификационными данными.

Правовые и нормативные требования, которые нужно учитывать, включают следующее:

– идентификация сущности, отвечающей за определение требований управления идентификационными данными;

– определение идентификационной информации и политик обращения с информацией (см. 6.2);

– определение цели, для которой разрешено использовать идентификационную информацию;

– домен(-ы) применения вне исходного домена, где может использоваться конкретная идентификационная информация;

– управление жизненным циклом идентичностей (см. 6.3);

– идентификация органа управления идентификационными данными исходного домена, где создавалась идентификационная информация (см. 5.3.2.7);

– требования подтверждения идентификационных данных (включая защиту информации, собранной в процессе подтверждения идентификационных данных) и требования сообщения в случаях, когда подтверждение идентификационных данных обнаруживает недействительную идентификационную информацию;

– идентификация сущности, отвечающей за поддержку содержания любого реестра идентификационных данных;

– аспекты безопасности физических мандатов, в частности мандатов, предназначенных для использования при аутентификации.

Приложение В

(справочное)

Модель варианта использования

В данном приложении представлена более подробная модель с примерной декомпозицией элементов базовой архитектуры. Эта декомпозиция включает действующих субъектов, описанных в таблице В.1.

Таблица В.1 – Действующие субъекты, представленные на диаграмме варианта использования.

Действующий субъект	Подробности
Оператор системы управления идентификационными данными	Сущность, отвечающая за обеспечение соблюдения политик управления идентификационными данными, осуществление управления конфигурационными данными в масштабе системы, обеспечение повседневной операционной поддержки. Примечание – В объединении идентичностей эта роль может называться «оператором объединения»
Поставщик утверждений по идентификационным данным	Обязанностью поставщика утверждений по идентификационным данным является подтверждение аутентификации и/или атрибутов. Он выполняет работу проверяющей стороны и может иметь доступ к реестру идентификационных данных. Полагающаяся сторона может делегировать задачи аутентификации и/или предоставления атрибутов поставщику утверждений по идентификационным данным. Поставщик утверждений по идентификационным данным аутентифицирует заявителя и/или получает данные из реестра идентификационных данных для предъявления идентификационной информации. Таким образом, система управления идентификационными данными может предоставлять полагающейся стороне услуги аутентификации, услуги, связанные с атрибутами, или те и другие
Орган идентификационных данных	Действующий субъект, который может делать доказуемые заявления о действительности и/или правильности одного или нескольких значений атрибутов в идентификационных данных. Орган идентификационной информации обычно связан с доменом, например, с исходным доменом, где атрибуты, по которым орган идентификационных данных может делать заявления, имеют особую значимость. Действующий субъект объединяет орган идентификационной информации и поставщика связанных с мандатами услуг
Поставщик связанных	Доверенный действующий субъект, который выпускает мандаты и/или

Окончание таблицы В.1

Действующий субъект	Подробности
с мандатами услуг	управляет ими. В этом контексте роль поставщика связанных с мандатами услуг ограничена выпуском мандатов для использования при аутентификации сущности

Цель описания вариантов использования состоит в том, чтобы представить договор между действующим субъектом и системой, идентифицируя доступные действующему субъекту взаимодействия. Действующий субъект инициирует взаимодействие с системой для достижения четко определенной цели, и каждый вариант использования описывает ответное поведение системы.

Вариант использования может также описываться с помощью текстовых блоков, циклограмм и иной формализованной системы обозначений, которая сделает возможным определение дальнейших подробностей взаимодействия с системой. Представленная в данном приложении модель варианта использования является высокоуровневым представлением, которое включает только диаграммы, дополненные в качестве примера коротким формализованным описанием варианта использования «аутентификации сущности».

Описание вариантов использования может детализироваться для показа дальнейших подробностей, обычно представленных на многих уровнях абстракции. Описание варианта использования на более низком уровне абстракции может вводить дополнительных действующих субъектов для подсистем, и такие действующие субъекты находятся в рамках системы.

Вариант использования, показанный на рисунке В.1, описывает два основных варианта использования в системе управления идентификационными данными:

– доступ к защищенному ресурсу;
– доставка сообщения, подлежащего аутентификации.

Модель варианта использования в таблице В.2 описывает внутренних действующих субъектов системы управления идентификационными данными из таблицы В.1, чтобы показать варианты использования с большей степенью детализации.

Таблица В.2 – Краткое определение вариантов использования для системы управления идентификационными данными

Вариант использования	Описание
доступ к услуге	Субъект хочет получить доступ к ресурсу, доступному после аутентификации сущности
аутентификация сущности	Деятельность, связанная с аутентификацией субъекта в онлайновой транзакции

Окончание таблицы В.2

Вариант использования	Описание
аутентификация сообщения	Деятельность, связанная с аутентификацией отправителя сообщения
использование сообщения	Получение сообщения и аутентификация отправителя
управление согласием	Предоставление, пересмотр и аннулирования согласия на использование идентификационной информации с целью аутентификации для доступа к ресурсу
управление мандатами	Деятельность, связанная с созданием, аннулированием и восстановлением мандатов, часто включает управление аппаратными мандатами
управление метаданными	Управление конфигурационными данными поставщиков утверждений по идентификационным данным и полагающихся сторон машиночитаемым, надежным и функционально совместимым образом. Включает технические параметры, такие как адресация и криптографические ключи
управление жизненным циклом идентификационной информации субъекта	Внесение в реестр, обновление, архивирование и удаление идентификационной информации
управление политиками	Определение политики и процедур для управления системой управления идентификационными данными и ее поддержки
получение запрашиваемых атрибутов	Получение атрибутов для аутентифицированного принципала, необходимых для санкционирования его запрашиваемого доступа к услуге
предоставление услуги	Полагающаяся сторона предоставляет ресурсы, требующие санкционированного доступа
услуга предоставления	Предоставление полагающейся стороне идентификационной информации о субъектах
отправка аутентифицированного сообщения	Отправка документа, запроса веб-сервиса и чего-то подобного. Здесь нет прямого ответа в процессе или транзакции. ***Примеры:*** ***a) Компания представляет на рассмотрение подписанный документ с балансовым отчетом, который она обязана предоставлять банку для поддержки кредитного лимита. Технически метод использует пересылку файла из клиентского компьютера в удаленный компьютер как анонимный пользователь. Аналогичными деловыми вариантами использования являются граждане, обращающиеся с заявлением о какой-то государственной деятельности, используя форму с электронной подписью.*** ***b) Отправитель доставляет асинхронное подписанное сообщение, например, как определено в SOAP, сервису***

UML обозначения варианта использования могут рассматриваться как графическое со-

держание совокупности вариантов использования. Его элементы включают следующее:

– эллипс: конкретный вариант использования;

– фигурка: действующий субъект (в смысле роли, а не конкретного лица);

– линия между действующим субъектом и вариантом использования: взаимосвязь «использования»;

– прямоугольник (пунктирный): границы системы;

– стрелка «включение»: вариант использования включает поведение варианта использования, на который указывает стрелка, подобно тому как программа вызывает подпрограмму;

– стрелка «расширение»: вариант использования, на который указывает стрелка, определяет, как и когда будет включено поведение другого варианта использования;

– стрелка с треугольником: указатель от более конкретного элемента (действующий субъект, вариант использования) на более обобщенный;

– пунктирная линия с одной стрелкой: общая зависимость вариантов использования.

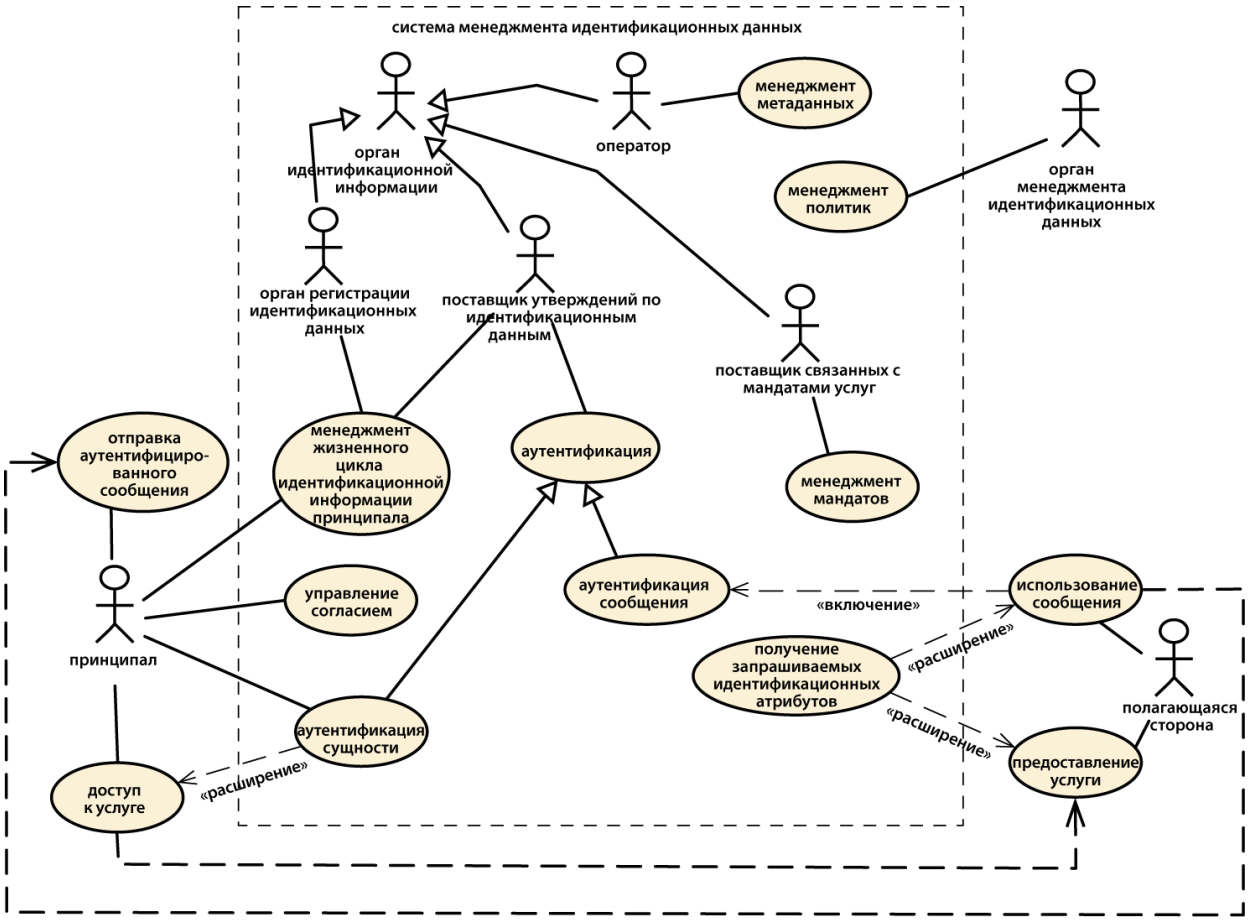

Рисунок В.1 – Примерная диаграмма варианта использования для системы управления идентификационными данными

Название варианта использования: Аутентификация сущности

Основной действующий субъект: Принципал

Сфера рассмотрения: Краткая сводка

Причастные стороны, имеющие свои интересы:

- **Принципал** – Предоставление идентификационных данных услуге, только если услуга обеспечивает защиту его прав как субъекта персональных данных – Возможность использовать услугу без регистрации и обременительной аутентификации

- **Полагающаяся сторона** – Обеспечение низкого порога для первого использования принципалами услуги и для последующих посещений – Обретение достаточной уверенности в праве принципала на использование услуги – Соблюдение законов и предписаний

- **Орган управления идентификационными данными** – Надзор за соответствием системы правилам и процедурам.

Предпосылка: Действующий субъект зарегистрирован в системе и действительно является принципалом.

Гарантии успеха: Принципал аутентифицирован, и утверждение по идентификационным данным использовано полагающейся стороной.

Инициирующее событие: Принципал пытается получить доступ к услуге полагающейся стороны и еще не аутентифицирован.

Основной сценарий успеха:

1. Доступ к услуге инициирует запрос об аутентификации.

2. Принципал осуществляет аутентификационное взаимодействие.

Рисунок В.2 – Примерное формализованное описание варианта использования

Приложение С

(справочное)

Компонентная модель

С.1 Модель

Это приложение далее расширяет пример, приведенный в приложении В, и представляет на рисунке С.1 функциональные компоненты системы управления идентификационными данными. Представленных компонентов достаточно для реализации расширенных вариантов использования, представленных в приложении D. Рисунок использует UML [1]. В подразделе С.2 представлены условные обозначения используемых на диаграмме символов.

Эта компонентная диаграмма показывает структурированные по времени рабочего цикла элементы системы. Она включает зависимости и интерфейсы. В таблице С.1 представлена краткая сводка показанных элементов.

Таблица С.1 – Функциональные компоненты системы управления идентификационными данными

Название	Описание
Управление мандатами субъектов	Подсистема для управления жизненным циклом мандатов субъектов
Управление метаданными	Этот компонент хранит метаданные и предоставляет средства для их поддержки и публикации. Уровень его безопасности должен быть равным или превышающим уровень безопасности системы, использующей метаданные
Агент предоставления услуги	Этот компонент продвигает идентификационную информацию к услуге, например, полагающейся стороне
Услуга полагающейся стороны	Услуга, действующая/предоставляемая под контролем полагающейся стороны. Предоставление доступа к услугам часто является основной целью системы управления идентификационными данными. Соответственно, важно осуществить определение интерфейсов и информирование о них на начальных этапах мероприятий приобретения или разработки для услуг полагающейся стороны
Импорт/Экспорт	Это компонент, который может быть реализован с характерными для источника сценариями, программным обеспечением метакаталогов или другими интерфейсами
Аудиторский репозиторий	Этот компонент хранит журнал операционных событий для целей аудита. Он обеспечивает контролируемый доступ к контрольному журналу

Окончание таблицы С.1

Название	Описание
Система управления идентификационными данными	Этот компонент представляет техническую инфраструктуру системы управления идентификационными данными в целом
Реестр идентификационных данных	Репозиторий сгруппированной идентификационной информации для домена. Это может быть физическое хранилище, такое как каталог, база данных или смарт-карта, или виртуальное хранилище, такое как виртуальный каталог
Доверенная основа	Обычно криптографическая защита информации, обрабатываемой в системе управления идентификационными данными, использует протоколы с открытым ключом на основе сертификатов открытых ключей, используемых системой. Сертификат открытого ключа предоставляется внеполосным способом

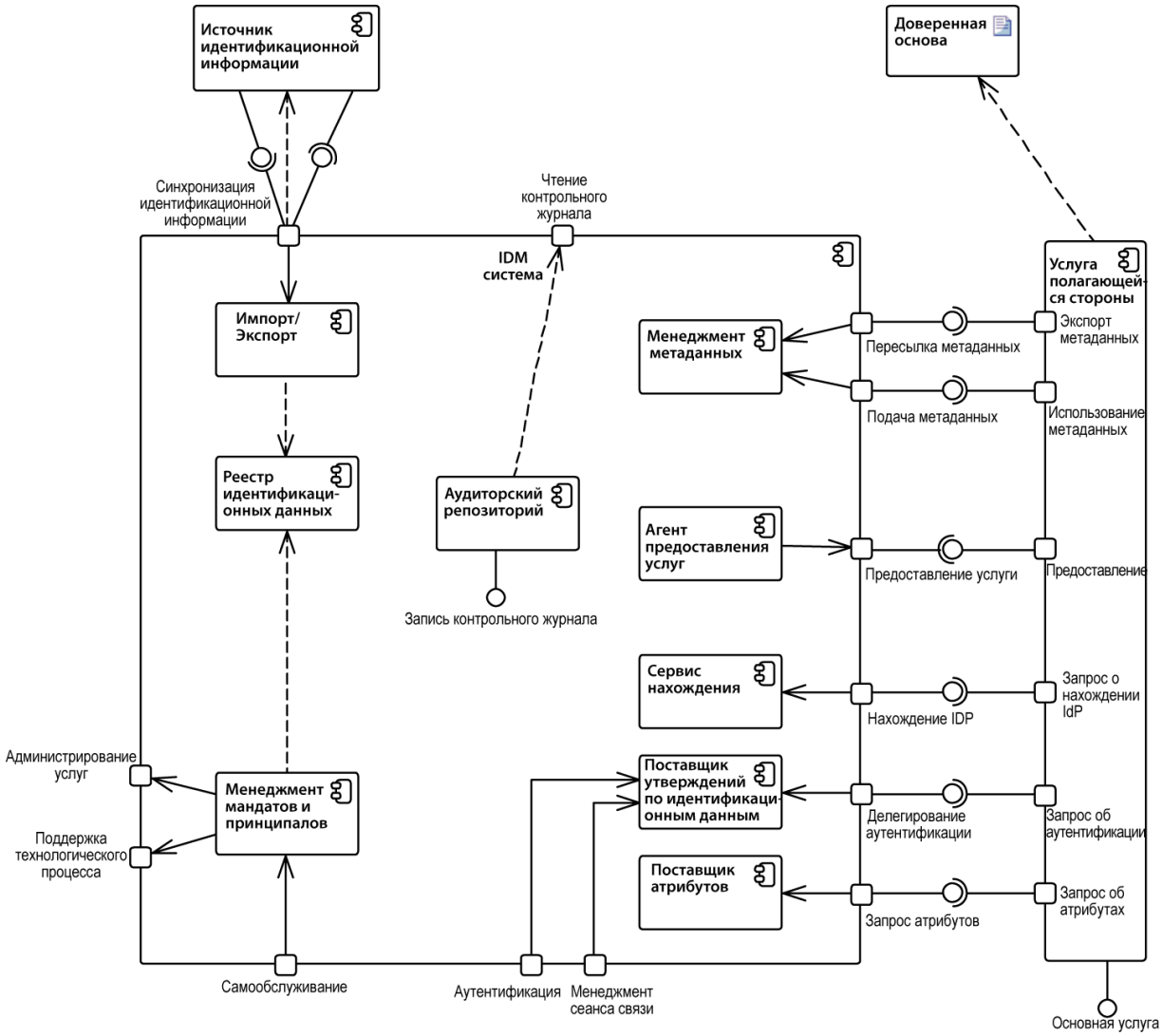

Рисунок С.1 – Функциональные компоненты системы управления идентификационными данными

С.2 Условные обозначения языка UML

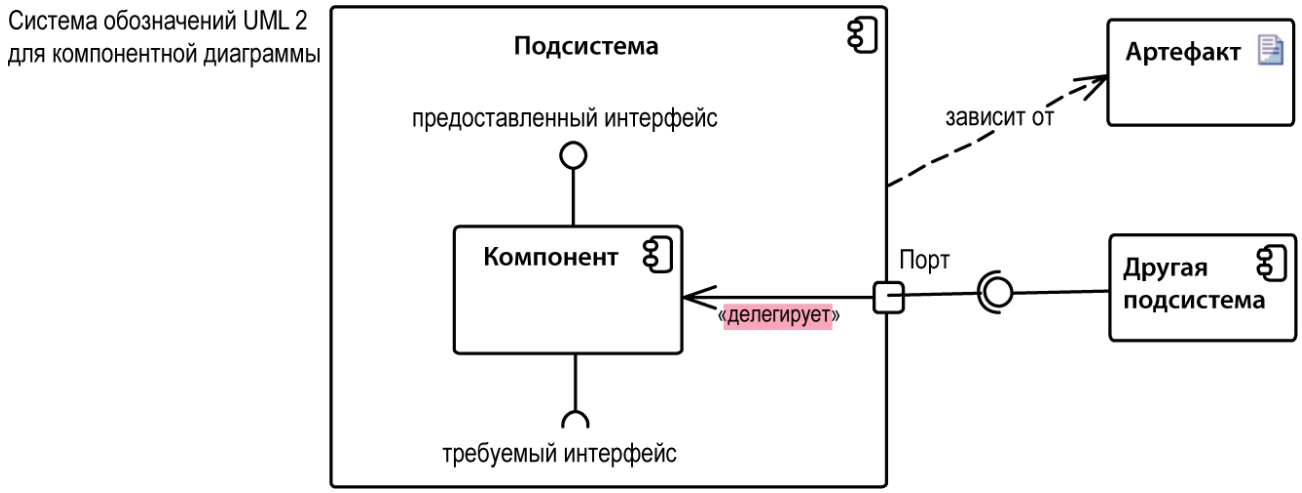

Рисунок С.2 – Графические элементы компонентной UML диаграммы

Таблица С.2 – Терминология компонентной UML диаграммы

Обозначение	Подробности
Артефакт	Артефакт – это любая физическая информация, используемая или создаваемая системой
Компонент	Компонент представляет модульную часть системы, которая инкапсулирует ее содержание и проявление которой заменяемо в рамках ее среды. Компонент определяет поведение с точки зрения предоставленного и требуемого интерфейса
Порт	Порты определяют взаимодействие между компонентом и его средой. Может быть много интерфейсов, контролирующих это взаимодействие. Порты появляются на границе компонента
Предоставленный интерфейс	Интерфейс – это спецификация поведения (или договора), которой реализующие стороны договорились соответствовать. Компонент реализует поведение, используя предоставленный интерфейс
Требуемый интерфейс	Интерфейс – это спецификация поведения (или договора), которой реализующие стороны договорились соответствовать. Компонент полагается на такое поведение, используя требуемый интерфейс
Подсистема	Подсистема изображена как компонент более крупной совокупности систем

Приложение D
(справочное)
Модель процесса функционирования

D.1 Общие сведения

Это приложение далее расширяет пример, приведенный в приложении B, используя примерное описание процесса функционирования. Процесс функционирования представляет собой совокупность взаимосвязанных структурированных видов деятельности или задач, создающих определенную услугу или продукт (служащих конкретной цели) для конкретного пользователя или группы пользователей.

В документально оформленном проекте модель процесса функционирования предоставляет описание потоков информации и управления, событий, целей и выходов для поддержки детального описания вариантов использования.

В данном приложении представлены диаграммы модели процесса функционирования с использованием расширенного языка UML [2].

D.2 Управление согласием

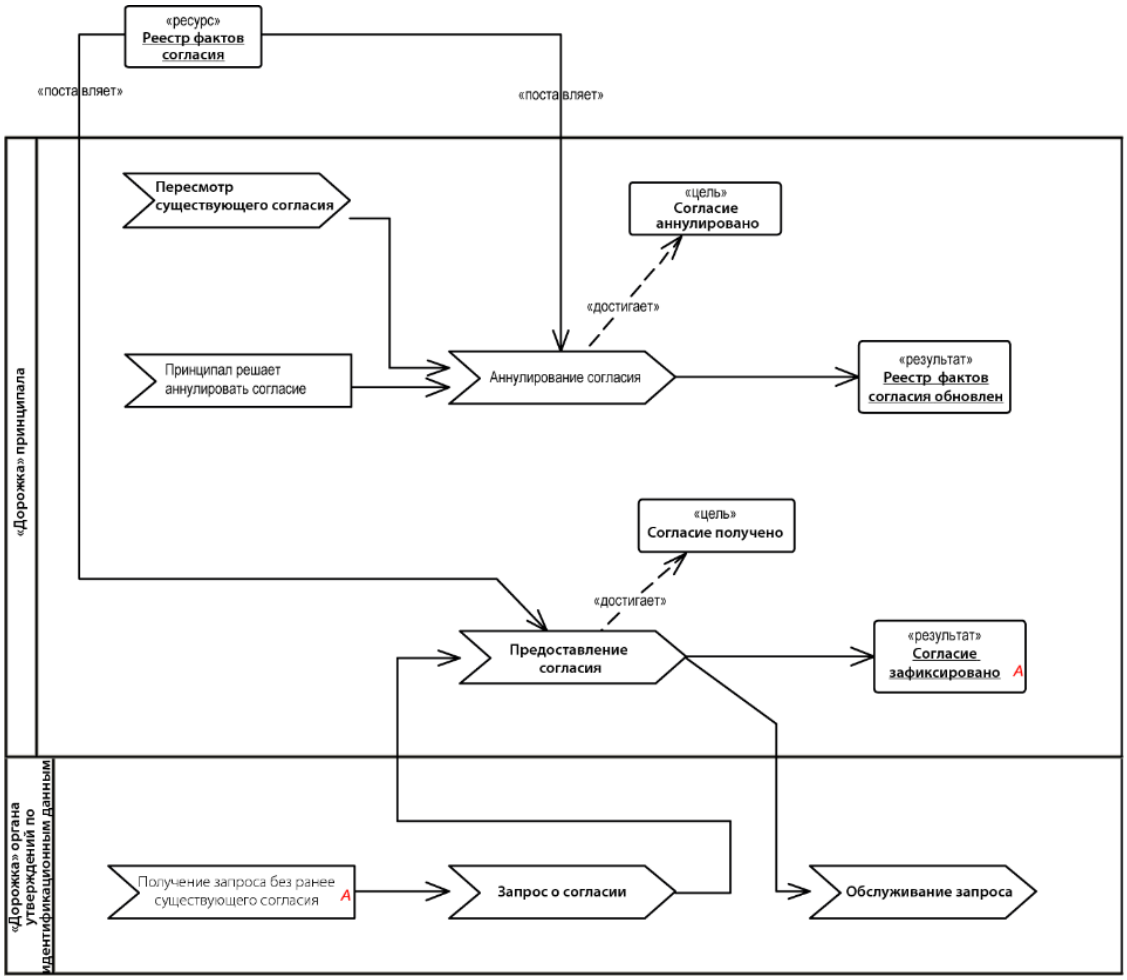

Рисунок D.1 – Диаграмма процесса управления согласием

Таблица D.1 – Описание элементов процесса управления согласием

Процесс	Подробности
Аннулирование согласия	В случаях, когда согласие не является подразумеваемым, принципалу должен предоставляться вариант аннулирования ранее предоставленного согласия.
Пересмотр существующего согласия	Пользователям нужно иметь возможность отзывать ранее предоставленное согласие.
Предоставление согласия	Согласие должно предоставляться в соответствии с политикой защиты прав субъектов персональных данных, например: – явное для деловой транзакции, связанной с медицинскими данными; – явное для полагающейся стороны для всех будущих транзакций, связанных с доступом в библиотеке сервисов для учащегося; – неявное для доступа к сервисам веб-приложения, чтобы

Окончание таблицы D.1

Процесс	Подробности
	выполнять официальные обязанности государственного служащего
	Подробности
Событие	Подробности
Субъект решает аннулировать согласие	Это событие предполагает, что субъекту предоставляются средства, чтобы аннулировать согласие – онлайновым образом, через центр обработки вызовов или по другому каналу связи
Получение запроса без ранее существующего согласия	Запрос об аутентификации или запрос атрибутов без ранее существующего согласия. Предыдущее согласие не существует, срок его действия истек или оно неприменимо для транзакции
Цель	Подробности
Согласие аннулировано	Согласие аннулировано. Политике нужно принять решение, следует ли это интерпретировать как отказ или как удаление. В последнем случае принципала попросят снова предоставить согласие
Согласие получено	Для совместного использования идентификационной информации с полагающейся стороной инспектор получает и документально оформляет согласие надлежащим образом (для транзакции, для взаимоотношений и т. д.)
Ресурс	Подробности
Реестр фактов согласия	Реестр фактов согласия хранит сведения о согласии пользователей в машиночитаемом формате. Неструктурированные документы могут быть включены для аудиторских целей Примечание – Реестр фактов согласия может группироваться поставщиком идентификационной информации или другими действующими субъектами
Результат	Подробности
Реестр фактов согласия обновлен	
Согласие зафиксировано	Решение о согласие зафиксировано. Если оно было положительным, разрешается запрос об аутентификации и/или атрибутах.

D.3 Управление жизненным циклом мандатов

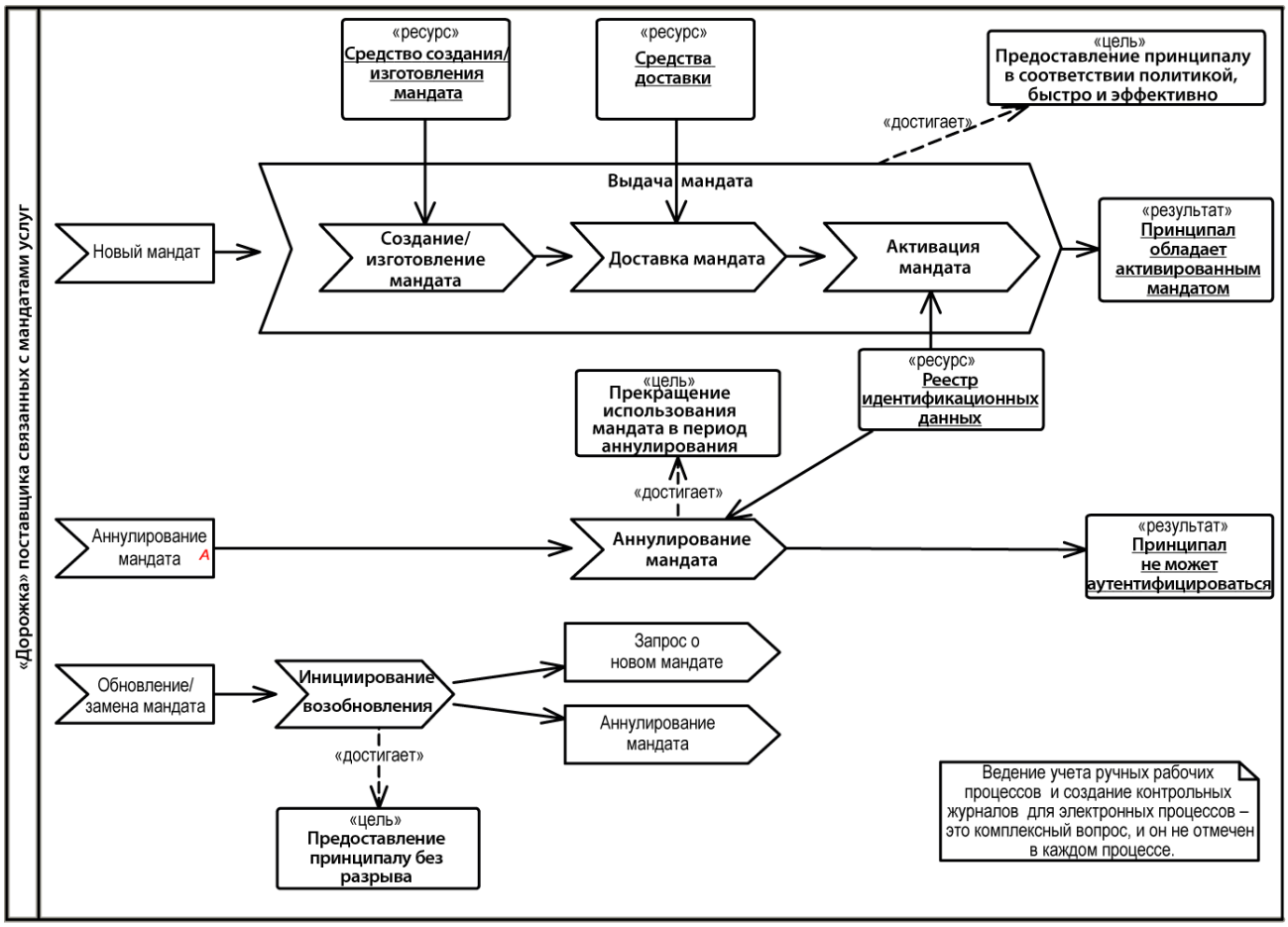

Рисунок D.2 – Диаграмма процесса управления жизненным циклом мандатов

Примечание – Приостановление действия мандата не поддерживается на этой диаграмме. Оно не включено для уменьшения сложности и может быть добавлено в случаях, когда необходима определенная архитектура.

Таблица D.2 – Описание элементов процесса управления жизненным циклом мандатов

Процесс	Подробности
Замена мандата	Выпуск нового мандата вместо существующего
Аннулирование мандата	Обновление реестра идентификационных данных, чтобы отразить статус аннулирования. Процесс может также инициировать сбор физических мандатов, таких как токен с динамически изменяющимся паролем
Инициирование возобновления	Выпуск нового мандата и обеспечение отсутствия разрыва в переходной период
Выдача мандата	Предоставление мандата субъекту
Создание/изготовление мандата	Это общий указатель для простого (например, пароль) или сложного (например, смарт-карта, биометрия) процесса выпуска мандата. Примечание – Несмотря на то, что мандат, как правило, это только данные, в процесс его создания может потребоваться также включить изготовление физического токена, содержащего мандат
Доставка мандата	Доставка мандата (и физического токена в качестве контейнера) может устанавливать или обеспечивать осуществление привязки мандата к субъекту
Активация мандата	Активация представляет собой процесс, дающий возможность сущности получать доступ к ресурсам, используя свой мандат
Событие	Подробности
Обновление/замена мандата	Замена может осуществляться по разным причинам, например: – мандат потерян или неправильно функционирует; – подозревается или известно, что предпринята атака на мандат; – срок действия мандата истек (например, смарт-карта перед концом срока службы)
Аннулирование мандата	Аннулирование старого мандата с учетом периода возобновления
Новый мандат	Другой процесс инициирует процесс выдачи мандата
Запрос о новом мандате	Инициирование процесса выдачи нового мандата
Аннулирование мандата	Процесс инициирует аннулирование мандата

Окончание таблицы D.2

Процесс	Подробности
Ресурс	Подробности
Средство создания/изготовления мандата	В зависимости от типа мандата это может быть генератор паролей или, например, производство смарт-карты
Средства доставки	Мандаты могут доставляться электронным образом, физически из рук в руки или через службу доставки
Реестр идентификационных данных	Содержит подмножество идентификационной информации, которая требуется для услуг регистрации, аутентификации и аннулирования

D.4 Управление данными конфигурации

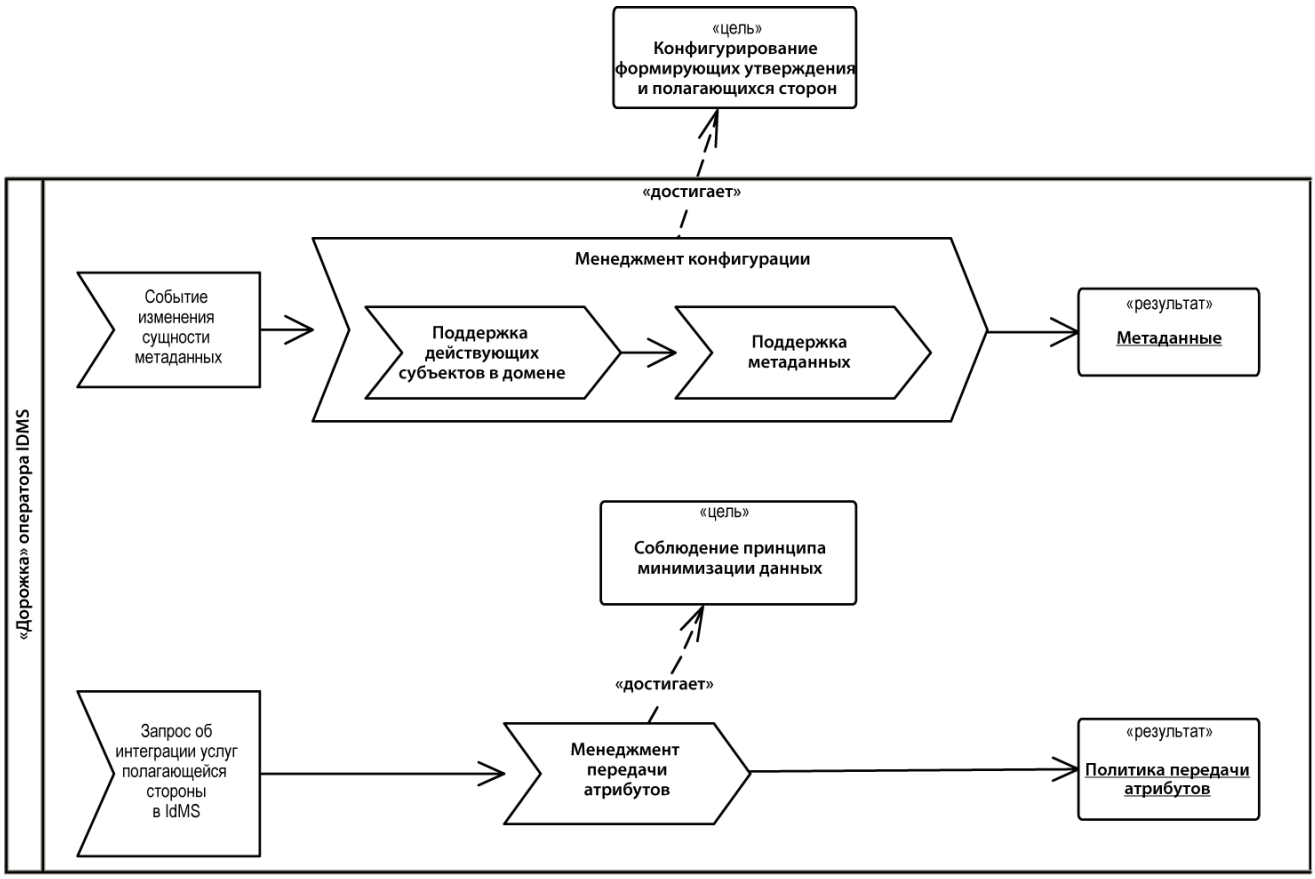

Рисунок D.3 – Диаграмма процесса управления данными конфигурации

Таблица D.3 – Описание элементов процесса управления конфигурацией

Процесс	**Подробности**
Поддержка данных конфигурации	Создание машиночитаемой конфигурации или метаданных
Поддержка действующих субъектов в домене	Администрирование участников системы управления идентификационными данными данных на деловом и техническом уровне. Это включает надзор и проверку достоверности данных, администрирование которых осуществляют сами участники системы управления идентификационными данными
Менеджмент передачи атрибутов	При предоставлении услуг могут быть переданы только те атрибуты, которые требуются и на которые получено согласие пользователя. Для достижения этого необходимо определить политику передачи атрибутов при включении услуг полагающейся стороны в систему управления идентификационными данными
Событие	Подробности
Запрос об интеграции услуг полагающейся стороны в IMS	Полагающаяся сторона обращается с просьбой об интеграции ее услуг с системой менеджмента идентификационных данных
Цель	Подробности
Соблюдение принципа минимизации данных	Орган идентификационных данных должен ограничивать свои услуги доверенными полагающимися сторонами и ограничивать передачу атрибутов теми из них, которые уместны для услуги и/или на которые получено согласие пользователя
Конфигурирование формирующих утверждения и полагающихся сторон	Администрирование технических данных о формирующих утверждения и полагающихся сторонах, чтобы способствовать их взаимодействию и доверительным отношениям
Результат	Подробности
Политика передачи атрибутов	

D.5 Управление политикой

Управление политикой связано с созданием и поддержкой политики системы управления идентификационными данными и взаимосвязанным управлением соответствием (GRC).

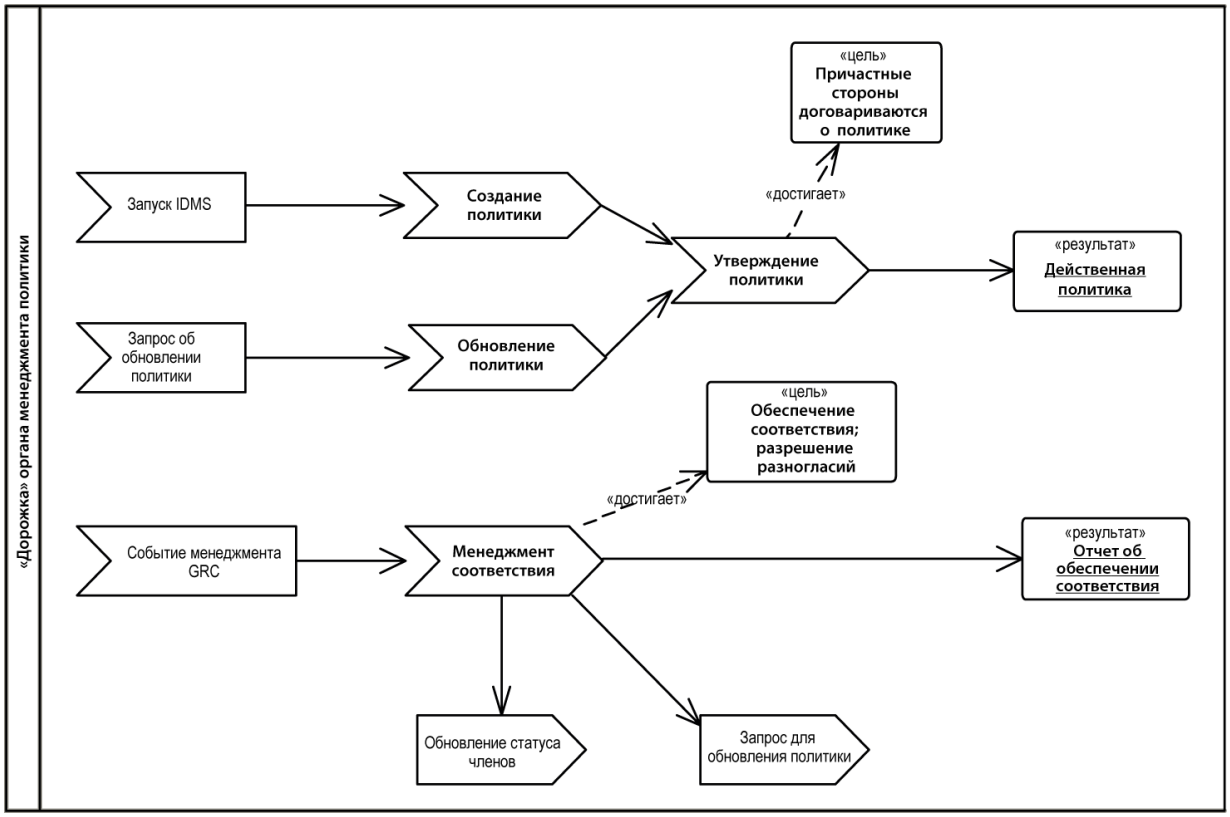

Рисунок D.4 – Диаграмма процесса управления политикой и соответствием

Таблица D.4 – Описание элементов процесса управления политикой и соответствием

Процесс	Подробности
Обновление политики	Эта деятельность обычно осуществляется специальной группой или рабочей группой
Создание политики	Эта деятельность обычно осуществляется специальной группой или рабочей группой
Утверждение политики	Эта деятельность обычно осуществляется правлением или общим собранием
Управление соответствием	Управление соответствием включает реализацию системы управления, определенной в политике системы управления идентификационными данными
Событие	Подробности
Запрос для обновления политики	Отправка запроса для обновления политики
Запуск системы управления идентификационными данными	Руководители организации, организаторы проекта или члены-учредители объединений решают начать разработку и развертывание системы управления идентификационными данными
Событие управления соответствием (GRC)	Политика определяет мероприятия обеспечения соответствия, осуществляемые запланированным образом или для конкретного случая
Запрос об обновлении политики	Осуществление обновлений может запрашиваться членами системы управления идентификационными данными, аудиторами или через регулярные интервалы времени для запланированного пересмотра
Обновление статуса членов	Сбои в обеспечении соответствия обычно регулируются руководителем проекта. Он может принимать решение о предупреждении, временном отстранении или исключении членов системы управления идентификационными данными из-за сбоев в обеспечении соответствия
Цель	Подробности
Обеспечение соответствия; разрешение разногласий	Доверие к обеспечению соответствия должно основываться на установлении и поддержке системы управления. Вопросы, которые не могут быть урегулированы системой управления, требуют передачи на более высокий уровень и разрешения силами руководителя проекта
Причастные стороны договариваются о политике	Причастные стороны (например, представители действующих субъектов или спонсоры) договариваются о правилах и процедурах управления системой управления идентификационными данными

D.6 Управление жизненным циклом субъекта

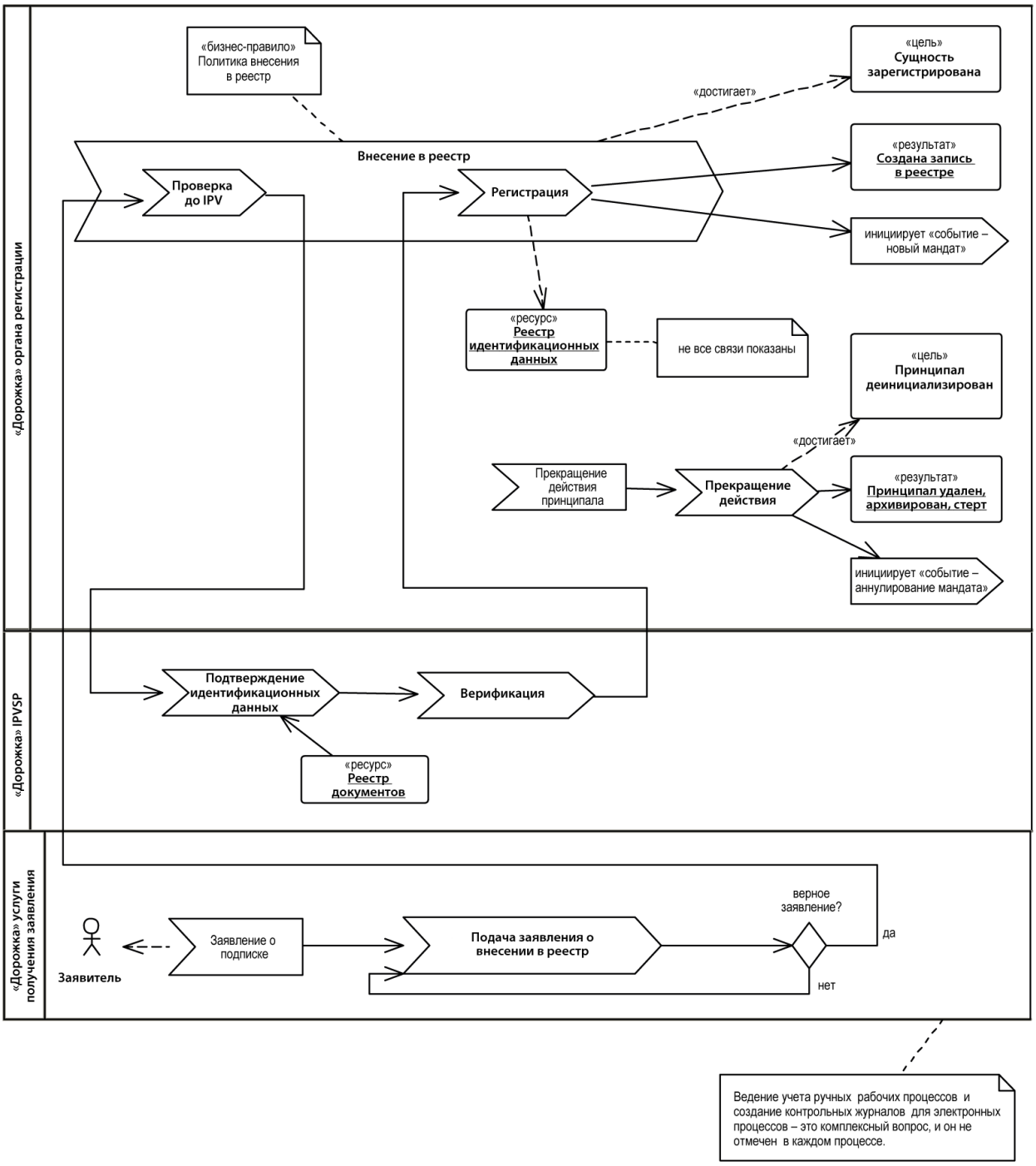

Рисунок D.5 – Диаграмма процесса управления жизненным циклом субъекта

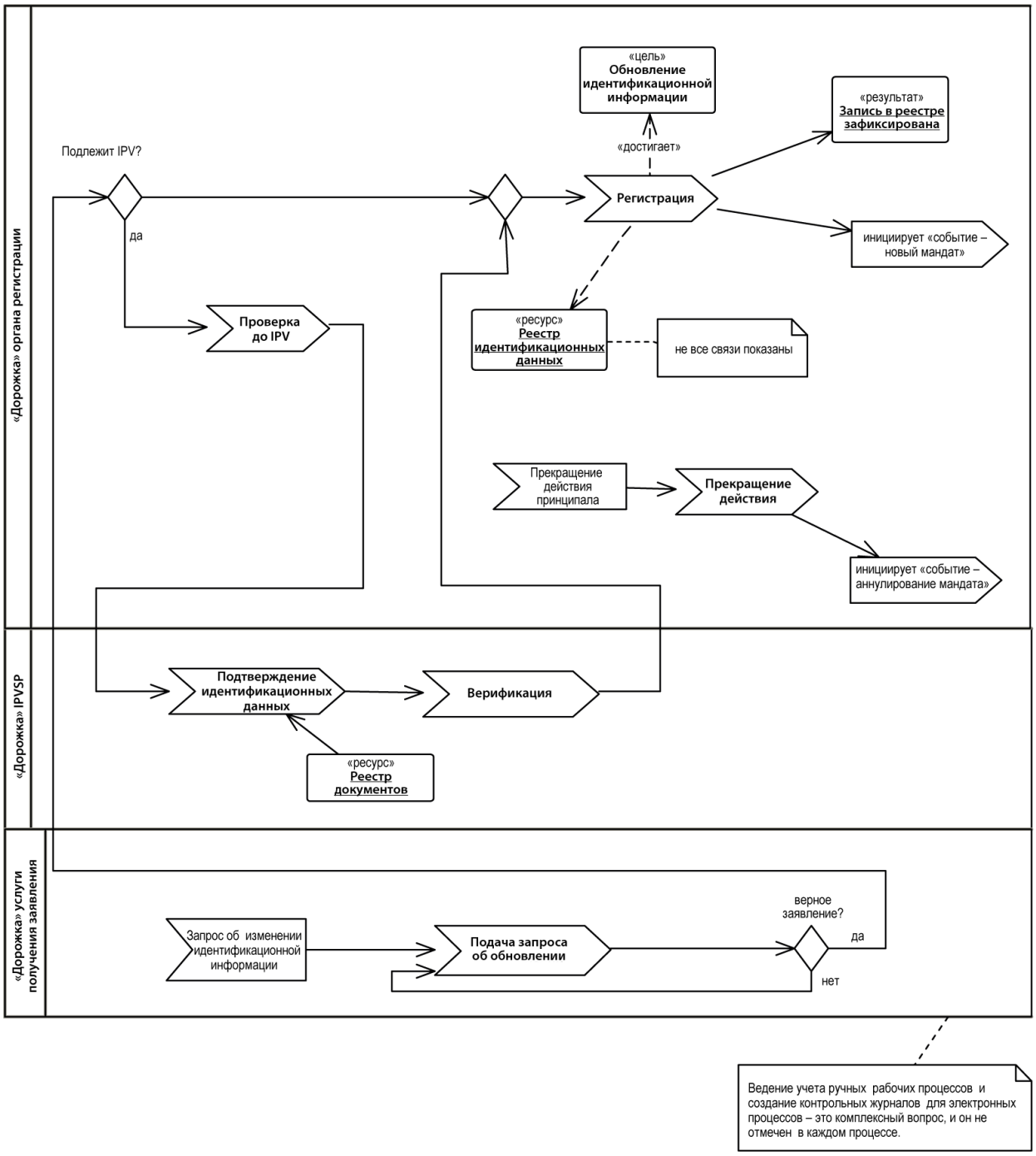

Рисунок D.6 – Диаграмма процесса корректировки идентификационной информации

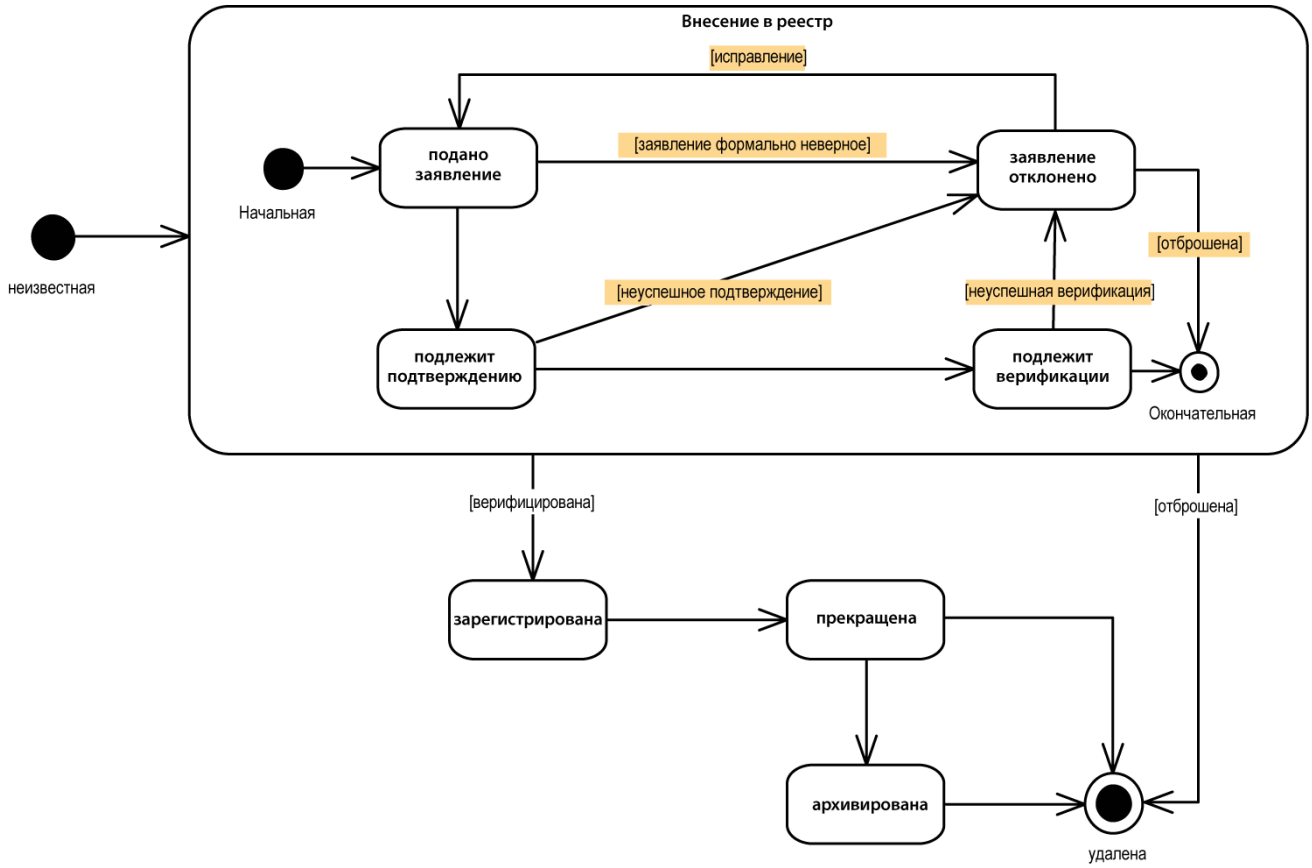

Рисунок D.7 – Диаграмма жизненного цикла для управления жизненным циклом идентификационной информации

Таблица D.5 – Описание элементов процесса управления жизненным циклом принципала

Процесс	Подробности
Внесение в реестр	Процесс, включающий следующее: – подтверждение идентификационных данных (мандатов в отношении фальсификации); – проверка достоверности (мандатов относительно источников выпускающей стороны); – проверка фактов сущности, имевших дело в прошлом (кредитная история, надежность); – оценка уровня доверия; – регистрация сущности как субъекта в реестре идентификационных данных. В зависимости от требуемого уровня доверия некоторые из этих шагов могут быть пропущены
Проверка до	Проверка заявления по формальным критериям, таким как полнота,

Продолжение таблицы D.5

Процесс	Подробности
подтверждения подлинности и верификации (IPV)	синтаксическая правильность и не запрошенные сообщения (SPAM). Логическое обоснование: экономия расходов процесса подтверждения подлинности и верификации, которые могут быть понесены, даже если результат отрицательный
Подтверждение идентификационных данных	Процесс сбора и проверки достаточного количества информации, чтобы идентифицировать субъекта на определенном или понятном уровне доверия
Верификация	Верификация идентификационной информации. Процесс проверки идентификационной информации и мандатов у выпускающих лиц, в источниках данных или других внутренних или внешних источниках на предмет их подлинности, достоверности, правильности и привязки к сущности [3] Примечание – Это определение относится к процессу внесения в реестр. С ним связан термин проверяющая сторона, который относится к процессу аутентификации. Данная архитектура не использует верификацию в контексте аутентификации
Подача заявления о внесении в реестр	Заявление о внесении в реестр может быть представлено удаленно сущностью или передано внеполосным способом, например, в бумажной форме или через систему, находящуюся вне системы управления идентификационными данными
Подача запроса об обновлении	Заявление об изменении идентификационной информации может быть представлено удаленно сущностью или передано внеполосным способом, например, в бумажной форме или через систему, находящуюся вне системы управления идентификационными данными
Регистрация	В процессе регистрации берется подтвержденная и верифицированная идентификационная информация и записывается в реестр идентификационных данных. Примечание – Технически эта информация может уже храниться там в результате предшествующих шагов процесса. В этом случае процесс обновляет статус на «зарегистрированный». Сравните с диаграммой состояния для управления жизненным циклом субъекта
Прекращение деятельности	Прекращение деятельности – это процесс, состоящий из нескольких шагов: а) архивирование идентификационной информации субъекта; б) замена «заглушкой» идентификационной информации после ее удаления из реестра идентичностей; в) по истечении срока периода архивирования удаление

Продолжение таблицы D.5

Процесс	**Подробности**
	архивированной информации, включая резервные копии
Событие	Подробности
Заявление о подписке	Сущность подает заявление (самостоятельно или через посредника), чтобы стать подписчиком органа управления идентификационными данными
Прекращение деятельности субъекта	«событие представлено для завершенности»
Инициируется «событие – аннулирование мандата»	«событие представлено для завершенности»
Запрос об изменении идентификационной информации	Запрос может исходить от базовой пользовательской организации, сущности, источника идентификационной информации или других действующих субъектов
Инициируется «событие – новый мандат»	«событие представлено для завершенности»
Цель	Подробности
Обновление идентификационной информации	«цель представлена для завершенности»
Сущность зарегистрирована	Цель процесса внесения в реестр состоит в том, чтобы зарегистрировать сущность и сделать так, чтобы ее мандаты были подтверждены, проверены на достоверность, а идентификационная информация зарегистрирована
Субъект деинициализирован	Цель процесса прекращения деятельности состоит в том, чтобы деактивировать мандаты субъекта во временные сроки, определенные политикой, архивировать идентификационную информацию на определенный срок и удалить всю идентификационную информацию по истечении срока периода архивирования
Ресурс	Подробности
Реестр документов	Реестр или сервис, который может быть использован для проверки того, что: – мандат, представленный для установления идентификационных данных, действительно существует у выпускающего органа; – мандат не был аннулирован

Окончание таблицы D.5

Процесс	**Подробности**
Ресурс	Подробности
Субъект удален, архивирован, стерт	Это результаты действий, связанных с прекращением деятельности
Создана запись в реестре	Сущность зарегистрирован как субъект в реестре идентичностей
Запись в реестре зафиксирована	Сущность зарегистрирован как субъект в реестре идентичностей; в случае корректировки идентификационная информация обновляется

Приложение ДА

(справочное)

Сведения о соответствии межгосударственных стандартов ссылочным международным стандартам (международным документам)

Т а б л и ц а ДА. 1

Обозначение и наименование международного стандарта (международного документа)	Степень соответствия	Обозначение и наименование межгосударственного стандарта
ISO/IEC 24760-1	-	*
ISO/IEC 29115	-	*
* - Соответствующий межгосударственный стандарт отсутствует		

Библиография

[1] Fowler, Martin UML distilled: a brief guide to the standard object modeling language. Addison-Wesley Professional, 2004

[2] Eriksson H.-E. UML 2 toolkit. John Wiley & Sons, 2003

[3] ISO/IEC 29115:2013, Information technology – Security techniques – Entity authentication assurance framework

[4] ISO/IEC 18014-1, Information technology — Security techniques — Time-stamping services — Part 1: Framework

[5] ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security controls

[6] Rozanski, N., and Woods, E. Software Systems Architecture: Working With Stakeholders Using Viewpoints and Perspectives, 2011

УДК 004 МКС: 01.040.35; 35.020 Э46 ОКС 35.030

Ключевые слова: атрибут, идентификатор, идентификационная информация, идентификационные атрибуты, идентификационные данные, идентификация, система управления идентификационными данными, идентичность

Заместитель директора ФИЦ ИУ РАН А.А. Зацаринный