ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 22378— 2026

Система защиты от фальсификации и контрафакта

ИДЕНТИФИКАЦИЯ ИНТЕРОПЕРАБЕЛЬНЫХ ОБЪЕКТОВ И СВЯЗАННЫЕ СИСТЕМЫ ПРОВЕРКИ ПОДЛИННОСТИ ДЛЯ ПРОТИВОДЕЙСТВИЯ ФАЛЬСИФИКАЦИЯМ И НЕЗАКОННОЙ ТОРГОВЛЕ

(ISO 22378:2022, Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade, IDT)

Издание официальное

Москва
Российский институт стандартизации
2026

Предисловие

1 ПОДГОТОВЛЕН Автономной некоммерческой организацией «Национальный научный центр компетенций в сфере противодействия незаконному обороту промышленной продукции» (АНО «ННЦК») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 124 «Средства и методы противодействия фальсификациям и контрафакту»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 10 февраля 2026 г. № 112-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 22378:2022 «Безопасность и устойчивость. Аутентичность, целостность и доверие к продукции и документам. Руководство по идентификации интероперабельных объектов и связанных систем аутентификации для противодействия фальсификациям и незаконной торговле» (ISO 22378:2022 «Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade», IDT).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2012 (пункт 3.5) и для увязки с наименованиями, принятыми в существующем комплексе национальных стандартов Российской Федерации.

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты, сведения о которых приведены в дополнительном приложении ДА.

Дополнительные сноски в тексте стандарта, выделенные курсивом, приведены для пояснения текста оригинала.

5 ВЗАМЕН ГОСТ Р ИСО 16678—2017

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

Содержание

Введение

Настоящий стандарт разработан с учетом трех основных положений:

- выявление фальсифицированных объектов является комплексной и, как правило, сложной задачей:
- точная идентифицирующая информация о рассматриваемом объекте упрощает процесс выявления фальсификаций;
- точную идентифицирующую информацию, как правило, бывает сложно получить.

Основной целью применения настоящего стандарта является упрощение и обеспечение доступа к точной идентифицирующей информации доверенным агентам (инспекторам) в процессе аутентификации объектов.

Для достижения этой цели настоящий стандарт устанавливает правила, направленные на облегчение задачи получения и использования идентифицирующей информации об объекте. Идентифицирующие данные и информация могут содержаться во многих местах хранения, в том числе в системах верификации и аутентификации.

Предоставление инспекторам доступа к идентифицирующей информации облегчает им задачу выявления фальсификатов.

В настоящем стандарте основное внимание уделяется вопросам маршрутизации запросов на получение информации об объекте, направляемых в соответствующую уполномоченную службу, и последующей маршрутизации ответов, направляемых обратно инспекторам.

Системы идентификации объектов, как правило, используют уникальные идентификаторы (УИД) в качестве ссылки или средства доступа к информации об объекте. УИД может быть присвоен группе объектов или отдельному объекту. В любом случае, УИД может упростить обнаружение фальсификаций и контрафакта, хотя УИД, присвоенные отдельным экземплярам объектов, могут быть более эффективными.

Настоящий стандарт содержит:

- термины и определения;
- обзор применения информации об объекте для обнаружения фальсификаций и контрафакта;
- принципы, концепции и приоритеты;
- рекомендации по улучшению интероперабельности[1)] систем, способных предоставлять инспекторам информацию об объекте;
- конкретные примеры, иллюстрирующие некоторые из представленных концепций.

Настоящий стандарт обеспечивает надежную и безопасную идентификацию объекта для предотвращения попадания на рынок незаконных объектов.

Стандарт включает в себя положения, целью которых является повышение доверия, сделав решения по идентификации объектов взаимодействующими. Например, стандарт описывает метод и решения для того, чтобы:

- обнаружить некоторые фальсифицированные и контрафактные объекты без аутентификации продукции;
- оценить элемент аутентификации;
- формально доказать, что удаленному описанию объекта можно доверять.

ИСО 22378 является частью семейства стандартов, включающего стандарты ИСО 22380, ИСО 22381, ИСО 22382, ИСО 22383, ИСО 22384.

Одной из целей настоящего стандарта является описание организационной структуры, в которой разрозненные решения по идентификации объектов будут иметь возможность взаимодействовать, при этом доверие к ним будет повышаться и, следовательно, они будут использоваться чаще. Структура также должна включать решения, которые позволяют достаточно просто обнаруживать некоторые фальсифицированные и контрафактные объекты без аутентификации продуктов.

Структура также должна включать решение, которое позволяет оценивать только элемент аутентификации. Предполагается, что сами системы идентификации и аутентификации объектов также могут быть подделаны и скопированы. Настоящий стандарт устанавливает метод формального доказательства того, что полученному из удаленного источника описанию объекта можно доверять.

Положения стандарта направлены на предотвращение несовместимости независимых реализа-

---

[1)] *Термин «интероперабельность» — по ГОСТ Р 55062—2021 «Информационные технологии. Интероперабельность. Основные положения».*

ций систем идентификации и аутентификации объектов и на обеспечение однозначности уникальных идентификационных ссылок при их использовании для нескольких вариантов обслуживания и различных приложений.

Базовое положение, лежащее в основе проектирования системы идентификации объектов, заключается в том, что отсутствие доверия к данным и отсутствие взаимодействия участников приводит к появлению «проблемных зон» для пользователей. Сокращение таких «проблемных зон» приведет к повышению осведомленности пользователей и, следовательно, к большей вероятности обнаружения и предотвращения фальсификаций и контрафакта.

Положения настоящего стандарта дополняют ИСО 22381:2018, который устанавливает требования к организации и поддержанию взаимодействия в системе идентификации и аутентификации объектов.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система защиты от фальсификации и контрафакта

ИДЕНТИФИКАЦИЯ ИНТЕРОПЕРАБЕЛЬНЫХ ОБЪЕКТОВ И СВЯЗАННЫЕ СИСТЕМЫ ПРОВЕРКИ ПОДЛИННОСТИ ДЛЯ ПРОТИВОДЕЙСТВИЯ ФАЛЬСИФИКАЦИЯМ И НЕЗАКОННОЙ ТОРГОВЛЕ

System of protection against fraud and counterfeiting. Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade

Дата введения — 2026—04—01

1 Область применения

Настоящий стандарт устанавливает общие положения, относящиеся к системам идентификации и аутентификации объектов[1)] (далее — системы). Стандарт содержит рекомендации и методы, составленные на основе анализа передового опыта, которые включают положения в области:

- управления использованием и проверки идентификаторов;
- физического представления идентификаторов;
- должной осмотрительности участников[2)];
- проверки всех участников системы;
- связи между уникальным идентификатором[3)] (УИД) и возможными элементами аутентификации, поставленными ему в соответствие;
- идентификации инспектора и авторизованного доступа к привилегированной информации об объекте;
- истории доступа инспектора (по журналам регистрации доступа).

Схема построения системы, приведенная в настоящем стандарте, предназначена для определения общих функций при различных реализациях системы.

---

1) Здесь под объектами понимаются товары народного потребления и товары производственного назначения, в отношении которых участники системы принимают меры по уникальной идентификации и аутентификации, выявлению и исключению из оборота фальсифицированных и контрафактных объектов.

2) Должная осмотрительность участников заключается в выполнении комплекса мер, направленных на исследование достоверности информации, полученной от других участников системы, и принятии решения на основе этой информации. В настоящем стандарте под участниками системы понимаются обладатели защищаемых законом прав на объекты (прав интеллектуальных и на средства индивидуализации), изготовители, поставщики, дистрибьюторы, потребители объектов, операторы систем идентификации и аутентификации, их подсистем, а также государственные, муниципальные и общественные организации, осуществляющие контроль подлинности объектов с применением системы в рамках предоставленных полномочий.

3) Здесь под идентификатором (уникальным идентификатором) понимается обозначение продукции, присвоенное согласно следующим стандартам: ГОСТ ISO/IEC 15459-1—2016 «Информационные технологии. Технологии автоматической идентификации и сбора данных. Идентификация уникальная. Часть 1. Индивидуальные транспортируемые единицы», ГОСТ ISO/IEC 15459-3—2016 «Информационные технологии. Технологии автоматической идентификации и сбора данных. Идентификация уникальная. Часть 3. Общие правила», ГОСТ ISO/IEC 15459-4—2016 «Информационные технологии. Технологии автоматической идентификации и сбора данных. Идентификация уникальная. Часть 4. Штучные изделия и упакованные единицы продукции», ГОСТ ISO/IEC 15459-5—2016 «Информационные технологии. Технологии автоматической идентификации и сбора данных. Идентификация уникальная. Часть 5. Индивидуальные возвратные транспортные упаковочные средства», ГОСТ ISO/IEC 15459-6—2016 «Информационные технологии. Технологии автоматической идентификации и сбора данных. Идентификация уникальная. Часть 6. Группы».

Издание официальное

В настоящем стандарте описываются процессы, функции и функциональные блоки в рамках общей модели системы. Стандарт не содержит требований к конкретным техническим решениям, реализующим модель системы.

Системы идентификации и аутентификации объектов могут включать другие функции и особенности, такие как прослеживаемость цепи поставок, прослеживаемость показателей качества, выполнение маркетинговых и других мероприятий, но эти аспекты не описаны настоящим стандартом.

Примечание — В настоящем стандарте не рассматриваются специфичные отраслевые требования, такие как глобальный номер предмета торговли GS1 (GTIN).

2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий стандарт [для датированных ссылок применяют только указанное издание ссылочного стандарта, для недатированных ссылок — последнее издание (включая все изменения)]:

ISO 22300, Security and resilience — Vocabulary (Безопасность и устойчивость. Словарь)

3 Термины и определения

В настоящем стандарте применены термины по ИСО 22300.

ИСО и МЭК поддерживают терминологические базы данных, используемые в целях стандартизации, по следующим адресам:

- платформа онлайн-просмотра ИСО: доступна по адресу https://www.iso.org/obp;
- Электропедия МЭК: доступна по адресу https://www.electropedia.org/.

4 Сокращения

В настоящем стандарте применены следующие сокращения[1)]:

IP — межсетевой протокол (Internet Protocol);
ИД — идентификатор данных (Data Identifier) (см. ANSI MH 10.8.2 [8]);
ИП — идентификатор применения (Application Identifier) (см. ANSI MH 10.8.2 [8]);
ОС — орган, уполномоченный по сертификации (Certification Authority);
СУДА — система управления данными атрибутов (Attribute Data Management System);
СУО — соглашение об уровне обслуживания (service level agreement);
УИД — уникальный идентификатор (Unique Identifier);
ФДВ — функция доверенной верификации (Trusted Verification Function);
ФДОЗ — функция доверенной обработки запросов (Trusted Query Processing Function);
ФФО — функция форматирования ответов (Response Formatting Function);
ФЭО — функция экспертизы объекта (Object Examination Function).

5 Общие положения

5.1 Общие требования

Преимущество использования интероперабельности систем идентификации и аутентификации объектов заключается в улучшении возможностей обнаружения фальсифицированных и контрафактных объектов за счет:

- расширения групп пользователей, использующих систему;
- увеличения количества проверяемых объектов;
- расширения доступа к доверенным источникам информации;
- снижения затрат:
  - на обучение;
  - оборудование;

[1)] *Порядок следования сокращений изменен по сравнению с оригиналом в связи с переводом на русский язык.*

- разработку;
- развертывание;
- проверку (инспекцию).

После достижения интероперабельности и широкого развертывания указанных систем доверенный субъект может использовать свой идентификатор для отправки запросов об объекте с целью принятия решения о его использовании. Инспектор может получить достоверные доказательства того, что информация, предоставленная в ответ на запрос, точна и заслуживает доверия.

Все участники системы должны выполнять свои функции с должной осмотрительностью, учитывая следующее:

- должны применяться аудит и проверка поставщиков товаров и услуг для обеспечения гарантии, что они действуют добросовестно и не являются источниками угроз в силу наличия недобросовестных агентов в составе источника поставки;
- должны применяться аудит и проверка производителей для обеспечения гарантии того, что они следуют документированным процессам и вводят точную информацию в системы;
- заинтересованные стороны, которым необходимо получать информацию, должны получить соответствующие полномочия для направления и обработки запросов, чтобы обладатели защищаемых законом прав на объекты могли предоставлять информацию, руководствуясь социальной ответственностью.

5.2 Операционный процесс в системе идентификации объектов

5.2.1 Общие положения

Системы идентификации объектов, как правило, состоят из функциональных блоков, показанных в модели на рисунке 1.

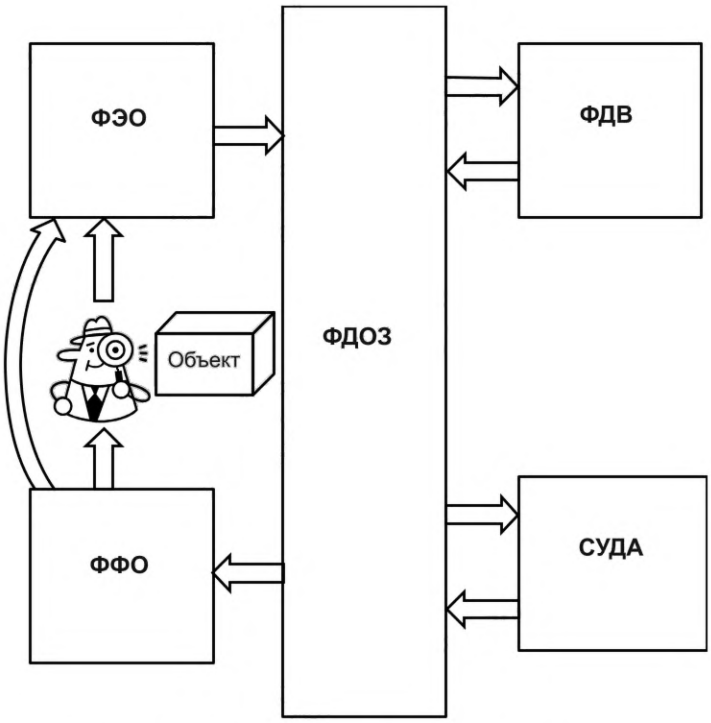


Рисунок 1 — Модель идентификации объектов

Модель не содержит никаких предположений о конкретной реализации функций.

В системе может существовать несколько экземпляров функции. Различные функции могут быть объединены в одну услугу.

Примеры реализации указанной модели приведены в приложении С.

5.2.2 Функция экспертизы объекта

Инспектор проводит экспертизу интересующего его объекта (например, товара, имеющего вещественную форму) с целью определения наличия у него УИД. Если УИД обнаружен, может потребоваться дополнительная проверка, чтобы определить, какая ФДОЗ может содержать данные об этом УИД.

Функция формирует запрос, который может состоять только из УИД, комбинации УИД с учетными данными инспектора или другими данными физических атрибутов, включая существенные присущие объекту элементы аутентификации, которые могут уникально идентифицировать объект, например такие, как цифровое изображение. ФЭО заканчивается, когда запрос отправляется одному или нескольким ФДОЗ. Когда процесс повторяется, ФЭО может оценить ответ на предыдущий запрос.

5.2.3 Функция доверенной обработки запросов

ФДОЗ маршрутизирует информацию между другими функциями в соответствии с установленными правилами. ФДОЗ может исследовать удостоверяющие данные, полученные от подающих запросы участников системы, на соответствие установленным правилам. ФДОЗ может быть распределена по нескольким услугам.

Примеры

1 ФДОЗ направляет запрос, сформированный ФЭО, к соответствующей ФДВ.

2 ФДОЗ объединяет ответ по верификации или аутентификации от ФДВ при любых учетных данных инспектора для формирования запроса в СУДА.

5.2.4 Функция доверенной верификации

ФДВ проверяет существование УИД в домене. ФДВ должна проверить удостоверяющие данные от запрашивающей ФДОЗ. ФДВ должна обеспечивать соблюдение привилегий доступа на основе установленных правил. Она может ответить источнику запроса сама или через одну или более ФДОЗ. Ответ, как правило, включает информацию по верификации УИД (является или не является УИД действующим). ФДВ может также генерировать предупреждения об опасности для заинтересованных участников системы. ФДВ должна защищать конфиденциальные данные от несанкционированного доступа.

ФДВ может также выполнять процедуры или алгоритмы аутентификации в отношении полученной информации (данных).

5.2.5 Система управления данными атрибутов

СУДА является достоверным источником мастер-данных об объекте. Для каждого атрибута объекта должна быть только одна запись мастер-данных. Если существует несколько экземпляров записей данных атрибутов, только одна запись должна считаться мастер-данными, а все остальные — вторичными данными. Различные атрибуты объектов могут находиться в различных базах данных. Множество баз данных может находиться в раздельных зонах среды.

СУДА получает ответ (через ФДОЗ) от ФДВ. СУДА проверяет удостоверяющие данные от запрашивающей ФДОЗ и удостоверяющие данные от инспектора. Привилегии доступа должны быть основаны на удостоверяющих данных и установленных правилах.

В ответ СУДА предоставляет данные, отобранные в соответствии с запросом и отфильтрованные по установленным правилам. Ответ может содержать готовые данные, отвечающие на все вопросы инспектора, или может содержать информацию, как получить эти данные. Если ответ содержит дополнительные указания, инспектор принимает решения о необходимости дополнительных действий и отправке дополнительного запроса.

Атрибуты, содержащиеся в СУДА, могут включать информацию о том, как аутентифицировать объект или как провести дальнейшие исследования.

СУДА должна обеспечивать защиту конфиденциальных данных от несанкционированного доступа.

5.2.6 Функция форматирования ответов

ФФО преобразует ответы СУДА в установленный формат и передает их инспектору.

Указанное действие является концом процесса. В некоторых случаях процесс проверки может быть повторен на основе результатов, предоставленных СУДА, или в зависимости от архитектуры системы.

5.3 Системы идентификации объектов. Настройка доверенной структуры

5.3.1 Общие положения

Система идентификации и аутентификации должна работать в соответствии с установленными определениями, правилами, видами данных и отношениями между данными.

На рисунке 2 приведен пример настройки и конфигурирования системы.

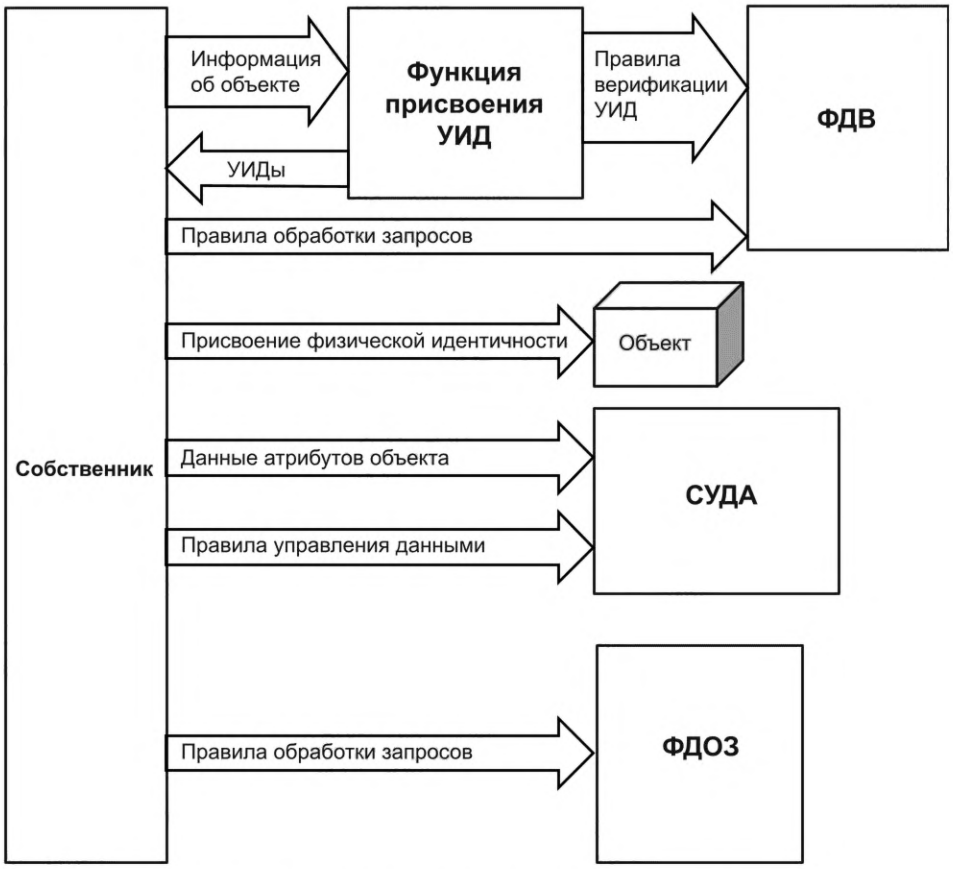


Рисунок 2 — Пример настройки и конфигурирования системы

5.3.2 Полномочия собственников

Собственники объектов определяют правила в отношении того, кто, как, где и когда получает права доступа к данным атрибутов объектов. Собственники также выбирают поставщиков услуг, которые применяют функциональные блоки системы и предоставляют доступ к данным и определяют бизнес-правила для различных поставщиков.

5.3.3 Функция присвоения уникального идентификатора

Функция присвоения УИД должна гарантировать уникальность УИД в домене применения услуг. УИД может присваиваться по установленному формату или с применением функции, в соответствии с которой в состав УИД могут быть включены определенные данные атрибутов объекта.

Функция также содержит правила верификации, которые ФДВ использует, когда производит действия в отношении конкретного УИД, содержащегося в запросе.

5.3.4 Информация об объекте

Информация об объекте содержится в виде совокупности данных атрибутов объекта или в виде указателей (ссылок) на данные атрибутов объекта.

5.3.5 Правила верификации уникального идентификатора

Алгоритмы и процедуры, которые позволяют ФДВ определять действительность УИД в рамках домена, могут включать алгоритмы и процессы, которые позволяют провести аутентификацию. Они могут включать также анализ перечня сформированных УИД.

5.3.6 Установление физической идентичности

Установление связи между УИД и объектом назначения может быть выполнено путем регистрации присвоенного УИД.

5.3.7 Данные атрибутов объекта

Данные атрибутов объекта включают атрибуты, достаточные для идентификации объекта или группы объектов. Собственник может включать дополнительные атрибуты по своему усмотрению.

5.3.8 Правила управления данными

Политика, относящаяся к защите и раскрытию данных атрибутов объектов, включает определение (перечень не является исчерпывающим):

- прав доступа, включая:
  - требования к предоставлению привилегий в уровнях доступа;
  - установление уровней доступа для видов атрибутов;
  - установление уровней защиты данных атрибутов;
- ролей пользователя (инспектора);
- правил ответов на стандартные запросы, включая:
  - бизнес-правила раскрытия данных по запросу;
  - формы ответов на запросы во всех ситуациях, например в случае недействительного УИД;
  - правила ответов на запросы в рамках привилегированного доступа и непривилегированного доступа.

5.3.9 Правила обработки запросов

Правила обработки запросов позволяют функции:

- направлять запрос или ответ в соответствующую функцию;
- проверять, авторизован ли участник осуществлять запрос;
- проверять, является ли линия коммуникаций, по которой поступил запрос, установленной для этого, и имеется ли разрешение на обмен данными.

6 Основные принципы

6.1 Общие положения

В настоящем разделе изложены основные принципы проектирования системы идентификации и аутентификации.

6.2 Доступность к использованию и своевременность ответа

Система идентификации и аутентификации должна быть спроектирована таким образом, чтобы:

- доступность системы к использованию и время отклика на запрос отвечали ожиданиям инспектора;
- время на предоставление ответа включало время, необходимое для проверки удостоверяющих данных.

Рекомендуется, чтобы доступность системы к использованию и время отклика на запрос были указаны в СУО.

6.3 Достоверный источник данных

Система идентификации и аутентификации должна быть спроектирована таким образом, чтобы только один достоверный источник данных соответствовал идентифицируемому объекту.

Применение множества источников данных может ввести в заблуждение инспектора. Злонамеренный поставщик услуг может скопировать источник, манипулировать им и заявить себя инспектору как один из достоверных источников данных.

Система идентификации и аутентификации может предоставлять поставщикам услуг привилегии хранителя данных, но всегда должно быть установлено, кто является достоверным источником данных и почему копиям хранителей данных можно доверять.

6.4 Управление данными

Система идентификации и аутентификации должна быть спроектирована таким образом, чтобы:

- мастер-данные и транзакционные данные поддерживались в актуальном состоянии;
- все данные управлялись в соответствии с ожидаемым жизненным циклом объекта;
- имелась возможность адаптироваться к будущим изменениям нормативных требований;
- имелась возможность долгосрочной идентификации объекта с гарантийными обязательствами на техническое обслуживание и контроль технического состояния, при которых следует проводить действия по аутентификации.

Примечание — Приложение В содержит дополнительную информацию об основных концептуальных положениях управления мастер-данными и транзакционными данными.

6.5 Принцип действительной необходимости ознакомления с данными

Система идентификации и аутентификации должна быть спроектирована таким образом, чтобы любые знания о перечисленных ниже аспектах были защищены и предоставлялись только по принципу необходимости ознакомления с данными:

- виды функций участников;
- содержание функций;
- процессы и архитектура системы.

6.6 Защита данных

Система идентификации и аутентификации должна быть спроектирована таким образом, чтобы она использовала передовые методы защиты критически важных для бизнеса данных. Указанное требование включает в себя проектирование и организацию безопасности как на уровне структуры системы, так и при организации ее эксплуатации, с учетом необходимости принятия соответствующих мер для защиты конфиденциальности, целостности и актуальности информации, хранящейся в системе.

6.7 Конфиденциальность

Система идентификации и аутентификации должна быть спроектирована таким образом, чтобы любая персональная идентифицирующая информация была защищена с учетом действующих законодательных норм, а также передовой отраслевой практики.

6.8 Соответствие нормативным требованиям

Система идентификации и аутентификации должна быть спроектирована таким образом, чтобы ее можно было адаптировать в соответствии с применяемыми нормативными требованиями.

Примечание — Действующие нормативные требования могут различаться в различных отраслях и странах.

6.9 Проверки

Система идентификации и аутентификации должна быть спроектирована таким образом, чтобы:

- все участвующие/вовлеченные стороны были подвергнуты проверке и аккредитованы;
- собственник мог гарантировать, что применение ФДВ и СУДА заслуживают доверия, результаты аудита и учетные данные поставщиков рассматриваются как часть процесса выбора поставщика, а удостоверяющие данные доступны и актуальны;
- лицо, выбирающее ФДОЗ, могло получить гарантию, что применение системы заслуживает доверия и удостоверяющие данные участников системы актуальны;
- поставщик услуг мог выполнять проверки идентификационных данных клиентов, запрашивающих использование их услуг по соглашению, чтобы предотвратить для злоумышленников возможность выдачи себя за собственников.

6.10 Аспекты интероперабельности

Две или более системы или услуги должны поддерживать возможность обмена структурированной информацией (синтаксическая интероперабельность), автоматически ее интерпретировать (семантическая интероперабельность), точно раскрывать смысловое значение данных. Система идентификации и аутентификации должна быть спроектирована таким образом, чтобы интероперабельность достигалась путем определения и согласования:

- целевой группы пользователей;
- минимально достаточных информационных потребностей пользователей;
- прав доступа;
- стандартов обмена данными, включая обработку данных, владение данными, защиту данных и ограничения использования, а также интерфейсы для обмена данными;
- таблиц стилей, если необходимо;
- соглашений об уровне обслуживания (СУО).

Примечание 1 — В настоящем стандарте рассматривается только семантическая интероперабельность. Для процесса маршрутизации может потребоваться введение определенной синтаксической унификации.

Примечание 2 — В ИСО 22381 приводится дополнительная информация о процессе установления интероперабельности путем организации деятельности вовлеченных участников, планирования архитектуры, а также организации и поддержания взаимодействия.

6.11 Присвоение уникального идентификатора

Система идентификации и аутентификации должна быть спроектирована таким образом, чтобы каждый УИД присваивался как уникальное обозначение в пределах домена, в котором предоставляется услуга.

7 План и реализация

7.1 Общие положения

В настоящем разделе приведены следующие положения:

- 7.2 содержит положения по определению доверенных служб с помощью ФДОЗ;
- 7.3 содержит положения по управлению данными идентификации объектов и атрибутами и характеризует, в частности, общие свойства систем;
- 7.4 содержит обзор распространенных противоправных действий и описывает преимущества и недостатки различных подходов к реализации системы с целью помочь заинтересованной стороне выбрать наиболее подходящее решение на основе конкретных обстоятельств.

7.2 Определение доверенных услуг

7.2.1 Общие положения

Система идентификации и аутентификации должна быть спроектирована таким образом, чтобы инспектор мог легко найти или определить, какая ФДОЗ связана с объектом. Инспектор должен иметь возможность оценить, какой уровень доверия связан с задействованной ФДОЗ.

Необходимо обеспечить максимально легкий поиск ФДОЗ, относящейся к объекту. Для этого должны быть приняты во внимание все обстоятельства, которые делают более легким корректное определение ФДОЗ.

7.2.2 Обеспечение доверия к функции доверенной обработки запросов

Система идентификации и аутентификации должна быть разработана таким образом, чтобы ФДОЗ, которая действует как портал для инспекторов, была указана в виде ссылки на объекте или одобрена широко известным авторитетным источником.

Должны быть приняты меры для выявления атак на порталы ФДОЗ и защиты от них. Например, злонамеренные агенты могут организовывать атаки на порталы для приведения их в состояние отказа от выполнения услуг. Атаки могут проводиться в различных формах, и принимаемые меры противодействия должны учитывать специфику атак.

Следует ограничивать количество предоставляемых услуг пользователям для более успешного выявления фальшивых услуг и несущих угрозу агентов. Объединение пользователей для работы с одной или ограниченным количеством ФДОЗ позволяет более эффективно распознавать подозрительные действия и поведение и представлять сведения о них. При появлении новой услуги следует выполнять действия по ее предварительному изучению.

7.2.3 Использование префикса или постфикса

Система идентификации и аутентификации должна быть спроектирована таким образом, чтобы можно было улучшить интероперабельность, используя стандартизированный ИД или ИП[1)] в качестве префикса или постфикса, чтобы содействовать ФДОЗ в направлении запроса к корректной ФДВ.

При отсутствии ИД, ИП или других средств для определения местоположения услуги подход заключается в проверке объекта на наличие товарных знаков или других свидетельств, идентифицирующих производителя объекта. Инспекторы могут обратиться к производителю за помощью в определении местоположения ФДОЗ.

7.2.4 Методы экспертизы объектов

Система идентификации и аутентификации должна быть спроектирована таким образом, чтобы не требовались дополнительные указания, когда все элементы данных и идентификационные данные присутствуют в системе, а все участники системы следуют соглашениям и правилам. В неидеальных

---

1) *Общие требования к ИД или ИП приведены в ГОСТ 34822—2022.*

системах следует принимать во внимание ухудшение возможностей выполнения ФЭО по мере потери или уничтожения УИД. Для расширения возможностей экспертизы объектов следует использовать элементы избыточности и корректировки ошибок для улучшения характеристик при таких обстоятельствах. Следует избегать потери взаимного доверия участников системы, в результате которого поведение пользователей будет диктоваться защитными реакциями.

7.3 Управление данными и атрибутами идентификации объектов

7.3.1 Общие положения

Система идентификации и аутентификации должна быть спроектирована таким образом, чтобы инспектор с необходимыми удостоверяющими данными мог инициировать запрос в ФДОЗ, результатом которого будет ответ от СУДА. Если правила доступа разрешают, ответ СУДА будет содержать данные идентификации объекта или другие атрибуты объекта.

Примечание — Инспекторы без удостоверяющих данных, такие как потребители товаров широкого потребления, могут получать только информацию, предоставляемую в широком доступе, или ответ с ограниченным набором данных.

7.3.2 Проверка точки входа для получения услуги (ФДОЗ)

Система идентификации и аутентификации должна быть спроектирована таким образом, чтобы заинтересованные участники системы принимали во внимание возможность получения контроля над точкой входа для предоставления фальсифицированной услуги злонамеренными агентами с целью совершения действий по фальсификации. Заинтересованные участники системы должны принимать во внимание необходимость получения ответов на ряд вопросов до того, как смогут посчитать заслуживающими доверия данные, полученные в рамках услуги. К таким вопросам относятся:

- является ли поставщик услуг надежным;
- поступают ли данные об объекте из надежного источника.

Ответы на указанные вопросы о доверии к источнику могут быть получены от независимых аудиторов. Заинтересованные участники системы могут получить данные аудита, которые свидетельствуют о доверии к удостоверяющим данным. В рамках предоставляемой услуги эти данные должны быть доступны для заинтересованных участников системы для повышения доверия к системе.

Инспекторы должны иметь возможность запросить удостоверяющие данные в рамках услуг, используемых другими участниками системы, и проверить, что все предоставляемые удостоверяющие данные действительны, для чего они должны иметь возможность обратиться с запросом к вызывающему доверие органу (организации).

7.3.3 Техническое обслуживание и управление

Система идентификации и аутентификации должна быть спроектирована таким образом, чтобы собственник мог гарантировать достоверность и актуальность данных. Например, если атрибут, описывающий объекты в классе, изменяется, может потребоваться обновление соответствующей информации в СУДА.

Собственник должен гарантировать, что функции, обеспечивающие права доступа, имеют актуальные правила и информацию об авторизованном пользователе.

7.3.4 Уровни привилегий и роли пользователей

Система идентификации и аутентификации должна быть спроектирована таким образом, чтобы доступ к конфиденциальным данным об объекте зависел от уровня привилегий доступа. Например, ответы, содержащие важные и конфиденциальные данные об объекте, могут быть направлены только инспекторам с очень высокими полномочиями, тогда как ответы, направленные инспекторам без полномочий, могут содержать только общедоступную информацию.

Уровней привилегий доступа может быть столько, сколько посчитают целесообразным сформировать собственники данных.

7.3.5 Управление доступом

Система идентификации и аутентификации должна быть спроектирована таким образом, чтобы учитывать различия отраслевых практик предоставления прав доступа по многим причинам, таким как нормативные требования, ограничения для сети связи, стоимость оборудования и т. д. Общими методами организации доступа являются следующие:

- назначение имени пользователя и пароля;
- использование цифровых сертификатов;
- контроль доступа по уникальным IP-адресам.

Должны применяться лучшие практики контроля доступа. Следует использовать средства проверки идентичности инспектора и организации перед тем, как им будет предоставлен доступ к конфиденциальной информации. Должны быть обеспечены простота применения средств единой точки входа. Контроль входа с использованием цифрового сертификата следует применять для данных с высоким уровнем конфиденциальности. Примеры цифровых сертификатов инспекторов приведены в приложении А.

7.3.6 Право собственности на транзакционные данные

Система идентификации и аутентификации должна быть спроектирована таким образом, чтобы данные о транзакционных событиях и журналы регистрации могли генерироваться по мере работы систем ФДОЗ и ФДВ. Все заинтересованные участники системы должны иметь возможность получить данные о том, кто является собственником и управляет данными транзакций и кто имеет права доступа и использования этих данных. Должны быть установлены формальные договорные отношения между заинтересованными участниками системы для предотвращения неправильного применения данных.

7.3.7 Использование транзакционных данных

Система идентификации и аутентификации должна быть спроектирована таким образом, чтобы коды УИД без соответствующей функции аутентификации не могли быть использованы для определения подлинности объекта. Записи в журнале регистрации событий могут определить некоторые систематические атаки и помочь изолировать фальсифицированные объекты. Например, запись о регистрации события, которая содержит информацию о месте нахождения объекта, может выявить ситуацию, когда объект с одним УИД заявлен как находящийся в двух разных местах одновременно. Также системы, в которых хранятся УИДы, присвоенные индивидуальным экземплярам объектов, могут выявить наличие фальсифицированных объектов в случае многократных запросов в отношении одного и того же УИД.

7.3.8 Государственные, международные организации и уполномоченные органы

Система идентификации и аутентификации должна быть разработана таким образом, чтобы государственные и международные организации могли устанавливать требования для защиты общественной безопасности. Эти требования могут быть различными в разных странах или в географических регионах. Выполнение этих требований обычно подвергается мониторингу или надзору со стороны уполномоченных органов или организаций, определенных государственными органами власти, с юрисдикцией по географическим областям. Эти органы или организации могут быть уполномочены нормативными актами государства, которые определяют предоставление доступа к конфиденциальной информации о продукции и любой информации, используемой для аутентификации продукции, необходимой для гарантии того, что она допущена для распространения на предназначенном для нее рынке и безопасна для потребителей.

Собственники должны быть уведомлены о специальных требованиях нормативных документов, которые требуют от них представлять данные о своей продукции для указанных выше органов или организаций на рынках, где распространяются или продаются их товары. Также собственники должны быть осведомлены, что в некоторых подведомственных областях могут существовать ограничения на трансграничный доступ к данным и услугам.

7.4 Основные виды фальсификаций

7.4.1 Дублирование кодов уникального идентификатора

Методы, используемые для обнаружения дублирования кодов УИД, различаются для идентификаторов групп и идентификаторов, присвоенных индивидуальным экземплярам объектов. Когда коды УИД копируются, повторно присваиваются, случайно совпадают или повторно используются, в системе появляются дубликаты или «клоны». Системы и услуги должны быть разработаны таким образом, чтобы обнаруживать и сообщать о дублирующих кодах УИД. Признаки дублирующих кодов УИД для обоих типов объектов (группа и экземпляр) могут включать (перечень не является исчерпывающим):

- запросы, поступающие из неавторизованных мест нахождения объектов или от неавторизованных инспекторов;
- объект не соответствует описанию, представленному из СУДА.

Признаки дублирующего кода УИД одного экземпляра объекта также могут включать (но не ограничиваясь):

- запросы, поступающие из разных мест одновременно;
- большее число запросов, чем можно ожидать для одного кода УИД.

Чтобы снизить риск дублирования кодов УИД, следует использовать элементы аутентификации.

Внутренний уровень физической безопасности должен быть реализован в самом представлении кода УИД на носителе. Внутренний уровень физической безопасности включает в себя (перечень не является исчерпывающим):

- чернила, краски со скрытыми свойствами, маркеры, проявляющиеся при специальном воздействии или с помощью специального оборудования, оптические объекты, меняющие свойства, и другие средства аутентификации;
- встроенные секретные ключи;
- закодированную информацию, относящуюся к элементам безопасности;
- физические неклонируемые функции или маркировки.

Варианты смежного уровня физической безопасности включают в себя (но не ограничиваются ими):

- бумагу с защитными знаками;
- чернила, краски, специальные метки, оптические объекты, меняющие свойства, другие средства аутентификации.

В дополнение к вышеизложенному могут быть использованы особые признаки торгового знака, такие как вышивки, элементы дизайна и цвет.

7.4.2 Замещение (подмена)

Фальсификация происходит, когда действительный УИД присваивается фальсифицированному объекту в целях замещения (подмены) подлинного объекта.

Злоумышленники используют несколько методов для этой фальсификации, используя:

- цепь поставок;
- списанные в утиль, восстановленные или повторно используемые изделия;
- программы замен изделий по гарантиям.

Методы снижения рисков замещения могут включать в себя (перечень не является исчерпывающим):

- использование технологий пломбирования упаковки, обеспечивающих обнаружение вскрытия;
- использование общедоступного утвержденного перечня авторизованных источников;
- прослеживание кодов УИД инспекторов и инспекций;
- деактивирование кодов УИД.

7.4.3 Недостоверные характеристики

Отсутствие кода УИД на объекте будет означать признак фальсификации, если инспектор знает, что код УИД должен присутствовать. Существует множество аутентичных изделий, для которых не применяется какой-либо УИД, поэтому отсутствие УИД на объекте не означает, что имеет место фальсификация. Фальсификация с недостоверными характеристиками имеет место, когда состав характеристик идентичности недостоверен, например:

- ожидаемый УИД отсутствует;
- УИД некорректный;
- существует большее число УИД, чем было законно присвоено;
- тип физической безопасности не соответствует установленному;
- число физических уровней защиты не соответствует установленным.

Методы снижения рисков получения объектов с фальсифицированными характеристиками включают в себя (перечень не является исчерпывающим):

- обучение инспекторов;
- обращение к собственнику или эксперту за консультацией;
- обучение широкого круга пользователей и информирование участников оборота продукции.

7.4.4 Фальсифицированные услуги

Недобросовестные участники могут направлять инспекторов к получению фальсифицированных услуг. Большинство методов, используемых для введения в заблуждение инспекторов, могут быть распознаны подготовленным инспектором, однако необученные инспекторы находятся в зоне высокого риска получения фальсифицированной услуги в виде ложной маршрутизации.

Атаки в виде фальсифицированных услуг включают:

- перемаршрутизацию, перехват и анализ трафика[1)], маскировку под другую программу или другого участника[2)], переадресацию;
- атаку посредника (перехват и подмена сообщений третьим лицом).

[1)] *Применяют также термин «сниффинг».*

[2)] *Применяют также термин «спуфинг».*

Методы снижения риска получения фальсифицированных услуг могут включать (перечень не является исчерпывающим):

- использование шифрованных каналов связи между функциональными элементами системы;
- использование цифровых сертификатов;
- проведение периодических проверок работоспособности доверенных элементов аппаратного/программного обеспечения;
- использование открытого утвержденного перечня;
- использование доверенных веб-сайтов как допустимых точек входа, например веб-сайтов:
  - собственника;
  - отрасли промышленности;
  - доверенной третьей стороны.

Собственники должны обеспечивать проведение аудитов систем и услуг, а также доступность своих удостоверяющих данных для инспекторов. Собственники должны гарантировать, что предназначенные для инспекторов обучающие материалы разработаны и обеспечено их сопровождение.

Инспекторы должны иметь возможность проверить удостоверяющие данные при первом использовании системы или получении услуги и иметь возможность периодически перепроверять, что удостоверяющие данные остаются действительными для всех используемых систем и услуг.

7.4.5 Фальшивый инспектор

Должны быть средства для обнаружения шаблонов вредоносных запросов. Примеры средств включают (но не ограничиваются ими) журналы регистрации доступа и процедуры, которые проверяют необходимость предоставления доступа на основе соответствия действительной необходимости ознакомления пользователя с запрашиваемыми данными.

7.4.6 Атаки инсайдеров

Недобросовестный сотрудник может своими действиями превратить добросовестного поставщика услуг или собственника торгового знака в недобросовестного. Недобросовестный сотрудник организации — участника системы может получить информацию о действительных значениях идентификационных номеров:

- из-за утечки конфиденциальной информации;
- ненамеренных ошибок, плохого исполнения обязанностей персоналом;
- умышленных действий;
- неадекватной информационной политики и обучения в организации;
- кражи персоналом организации действительных значений УИД.

Методы снижения риска атак инсайдеров могут включать (но не ограничиваются ими):

- адекватную политику безопасности:
- избежание существования пунктов присвоения одинаковых идентификационных номеров;
- активацию значений УИД только в случае их действительного использования.

Приложение А
(справочное)

Цифровые сертификаты (для инспекторов)

А.1 Общие положения

В данном приложении приведена одна из возможных реализаций использования сертификатов X.509 (см. ИСО/МЭК 9594-8) для передачи удостоверяющих данных инспектора до функциональных подсистем системы идентификации и аутентификации объектов. В данном примере интероперабельность улучшается за счет использования общеприменяемого и действующего стандарта (X.509) в качестве механизма для доставки информации через сеть Интернет. Это выполняется путем использования OU1 и OU2[1)].

Генерацию сертификата для инспектора может произвести собственник. Этот сертификат может использоваться всеми ФДОЗ.

Цель состоит в том, чтобы установить безопасную и надежную связь между функциями. X.509 является одним из методов достижения указанной цели при использовании общедоступных сетей.

А.2 Пример и определения цифровых сертификатов (для инспекторов)

Использование цифрового сертификата для контроля доступа к СУДА является одним из лучших методов, но при этом собственник торгового знака должен оценить достоверность как инспектора, так и самого цифрового сертификата.

А.3 Достоверность инспектора

Необходимо, чтобы владелец торгового знака оценивал достоверность инспектора, который получает цифровой сертификат для доступа к высококонфиденциальным данным в СУДА. Доверие можно повысить, используя открытый перечень доверенных инспекторов, сформированный уполномоченным источником.

А.4 Достоверность цифрового сертификата

Чтобы обеспечить достоверность цифрового сертификата, следует использовать цифровой сертификат, выпущенный в соответствии со следующими стандартами:

- ETSI/TS 102 042 [10];
- ETSI/TS 101 456 [9];
- WebTrust for CA [12].

А.5 Общее поле действия цифрового сертификата

Общие профили цифровых сертификатов могут быть необходимы для достижения интероперабельности между системами.

Пример общего профиля сертификата X.509 (см. ИСО/МЭК 9594-8) приведен в таблице А.1.

Таблица А.1 — Обязательные поля (основные поля сертификата)

Поля сертификата	Тип данных (количество символов)	Определение	Полномочия	Пример
Предмет				
Название страны	Печатная строка (2)	Двухсимвольный код страны в соответствии с ИСО3166-1 — все заглавные буквы	Администратор	JP
Название области	Печатная строка (128)	Название штата, провинции и т. д. Первый символ — заглавная буква	Администратор	Токио
Название местности	Печатная строка (128)	Название города и т. д. Первый символ — заглавная буква Разделитель - дефис	Администратор	Минато-ку

[1)] *Условные обозначения приведены в таблице А.1 для подразделений организации.*

Окончание таблицы А.1

Поля сертификата	Тип данных (количество символов)	Определение	Полномочия	Пример
Наименование организации	Печатная строка (64)	Наименование организации[a]	Администратор	JIPDEC
Наименование подразделения организации 1	Печатная строка (64)	Идентификатор, которым управляет администратор. Для отличия при автоматической проверке добавляют префикс «OU1-»[b]	Администратор	OU1-G2—1.2.392.200063.80.1.1
Наименование подразделения организации 2	Печатная строка (64)	Идентификатор, которым управляет регистрирующий орган (РО) или местный регистрирующий орган (МРО). Для отличия при автоматической проверке добавляют префикс «OU2-»[c]	РО или МРО	OU2—007
Общее наименование субъекта	Печатная строка (64)	Имя субъекта (полное имя, наименование подразделения, должность или идентификатор). Для отличия при автоматической проверке может использоваться префикс «BN-» (имя, которое используется в компании как официальное, и «BO-» (организация/роль) или «ID-»	РО или МРО	Смит Бетти (менеджер по снабжению)

[a] Следует использовать наименование, зарегистрированное в QGIS (Квалифицированный государственный источник информации), или QIIS (Квалифицированный независимый источник информации), или QTIS (Квалифицированный источник налоговой информации).

[b] Допускается использовать как указатель информации открытых атрибутов (наименование компании и т. д., которое не может быть представлено знаками алфавита), который не записан в сертификате.

[c] Допускается использовать как указатель закрытых атрибутов (наименование составной части и т. п.), который не записан в сертификате.

Приложение В
(справочное)

Управление мастер-данными

В.1 Мастер-данные и данные транзакций

Мастер-данные и данные транзакций являются двумя различными наборами данных. Они оба имеют отношение к прослеживаемости, так же как и к безопасности продукции, влияют на принятие решения об отзыве продукции и на меры против фальсификаций. Свойствами наборов данных является их принадлежность к открытым данным или конфиденциальным данным, в последнем случае требуется авторизованный доступ к информации об объекте при обнаружении проблемы фальсификации.

Доступ к мастер-данным объекта требует определенных уровней аутентификации для доступа, как правило, контролируемого собственником торгового знака или собственником прав на интеллектуальную собственность. Цепи поставки, как правило, охватывают множество участников, при этом договорные соглашения между участниками могут быть сдерживающим фактором в доведении информации о фальсификациях до компетентных органов ввиду договорных обязательств и правовых последствий.

В.2 Мастер-данные

Мастер-данные определены как статические данные о продукции, которые являются долговременными по своей природе и не подвергаются частым изменениям на протяжении жизненного цикла объекта. Они включают данные, которые можно считать открытыми, такие как идентификационное обозначение объекта на потребительской упаковке, торговое наименование, описание продукции, вес, размеры и др. Мастер-данные также могут содержать конфиденциальную бизнес-информацию, такую как технические требования разработчика, перечень материалов, источники поставки компонентов, атрибуты аутентификации и др.

Процессы, используемые для управления мастер-данными, включают создание мастер-данных, кодификацию объекта, классификацию данных, идентификацию источника, сбор данных, передачу данных, стандартизацию, выработку правил, выявление и коррекцию ошибок, консолидацию данных, хранение данных, распределение данных, синхронизацию данных, систематизацию данных, построение алгоритмов сопоставления, повышение качества данных, управление данными, мониторинг данных по жизненному циклу объектов.

В.3 Данные транзакций

Данные транзакций являются динамическими, определяемыми событиями в цепи снабжения, которые можно разделить на открытые и конфиденциальные данные. Данные транзакций создаются в информационных системах при движении объектов через цепь снабжения. Данные транзакций могут быть собраны и задокументированы, управление ими может осуществляться в рамках договорных отношений.

Приложение С
(справочное)

Примеры применения системы

С.1 Введение

Настоящее приложение содержит описание применения систем идентификации и аутентификации объекта и их соответствия общей модели, изложенной в настоящем стандарте.

Примеры функциональных блоков могут отличаться. Блоки, показанные в каждом примере, группируются для иллюстрации множественности применений.

С.2 Уникальный идентификатор группы объектов и уникальный идентификатор экземпляра объекта

Во всех примерах, представленных в настоящем приложении, УИД обеспечивает инспектору возможность поиска информации с описанием объекта.

Для УИД групп объектов информация с описанием относится к общим атрибутам всех объектов в группе, таким как содержимое и особенности продукции и упаковки. Указанные данные называют мастер-данными.

Информация для УИД групп объектов, как правило, включает несколько уровней детализации атрибутов. Информация для УИД групп объектов может быть:

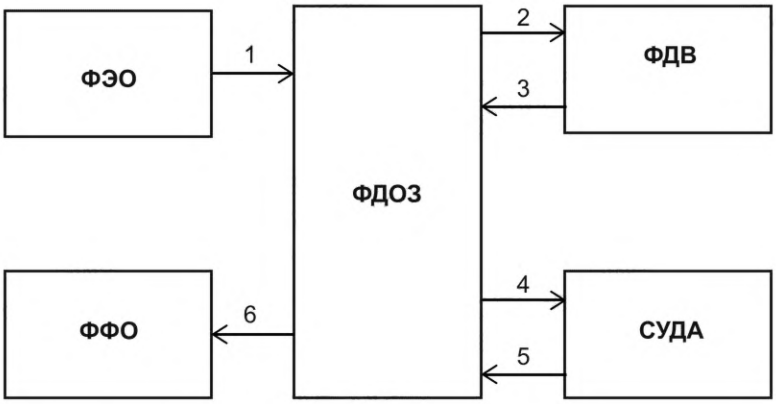
- описательной для всей группы объектов (мастер-данные содержат ту же информацию, что и для УИД всей группы), включает особенности продукции и упаковки;
- описательной для производственной партии объектов, например номер производственной партии, дата истечения годности, информация об отзыве партии;
- описательной для множества объектов партии, включает информацию об отгрузке, информацию о покупателях и продавцах партии объектов;
- описательной для отдельного экземпляра объекта, включает серийный номер отдельной единицы продукции и/или его компонентов.

При выборе способа обозначения на основе УИД группы объектов или УИД экземпляра объекта следует принимать во внимание многие факторы. Информация, ориентированная на специфические свойства объекта, может быть более эффективна, чем информация, ориентированная на специфические свойства групп объектов, при выявлении контрафактных (фальсифицированных) объектов. Например, имеется в наличии множество экземпляров объектов, каждый из которых имеет одинаковый для всей группы УИД, но для экземпляра объекта возможно наличие только индивидуального УИД экземпляра. Обнаружение двух одинаковых объектов с УИД группы не является нарушением правила, в то время как обнаружение двух объектов с одинаковым УИД экземпляра объекта является отклонением от правила. Тем не менее, применение УИД экземпляра объекта, как правило, связано с более высокими накладными расходами, чем УИД группы объектов.

С.3 Объект с уникальным идентификатором группы объектов, пример без применения функции аутентификации

Объекты в настоящем примере реализации используют только УИД группы. При настройке системы для каждого УИД собственник данных загружает в СУДА атрибуты, описывающие объекты в каждой группе. Каждый УИД указывает на один набор атрибутов объектов в СУДА.

На рисунке С.1 показан пример для применения УИД группы без функции аутентификации.



Типовой запрос требует выполнения перечисленных ниже действий:

1 ФЭО извлекает УИД с объекта и направляет в ФДОЗ.

2 ФДОЗ проверяет удостоверяющие данные инспектора на соответствие правилам и направляет соответствующие запросы в ФДВ.

3 ФДВ проверяет действительность УИД. Если УИД действителен и удостоверяющие данные инспектора приняты, ФДВ предоставляет адрес, где содержатся данные атрибутов.

4 ФДОЗ направляет принятые запросы (вместе с указателем адреса атрибутов) в СУДА. Запросы, отклоненные ФДВ, в обход СУДА направляются напрямую в ФФО для представления инспектору.

5 СУДА оценивает удостоверяющие данные инспектора на соответствие правилам доступа и представляет ответ на принятые запросы с данными атрибутов.

6 ФДОЗ направляет ответ в ФФО для представления инспектору.

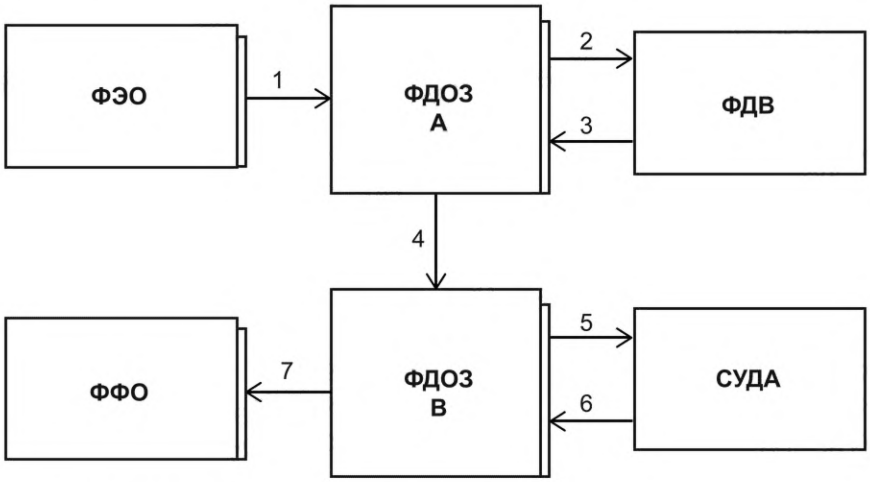
Примечание — Фальсификация выявляется по признакам несоответствия атрибутов, полученных инспектором, атрибутам, представленным на объекте.

Рисунок С.1 — Объект с УИД группы, пример без функции аутентификации

С.4 Пример с уникальным идентификатором экземпляра, без функции аутентификации

В данном примере приведен объект с УИД экземпляра, когда каждый из объектов имеет различный УИД. Каждый УИД поставлен в соответствие атрибутам одного объекта. Другие объекты не обязательно имеют идентичные атрибуты. Возможна ситуация, когда только УИДы уникальны в группе объектов, а все объекты в группе имеют идентичные атрибуты и неразличимы с помощью УИД.

На рисунке С.2 показан пример УИД экземпляра без функции аутентификации.



Типовой запрос требует выполнение перечисленных ниже действий:

1 ФЭО извлекает УИД с объекта и отправляет запрос во ФДОЗ.

2 ФДОЗ оценивает удостоверяющие данные инспектора и направляет запрос в ФДВ.

3 ФДВ проверяет действительность УИД. Если УИД действителен и удостоверяющие данные инспектора приняты, ФДВ предоставляет адрес, где содержатся данные атрибутов.

4 ФДОЗ направляет принятый запрос (вместе с указателем адреса атрибутов) ко второму и независимому ФДОЗ (данный пример показывает, что функции могут быть разделены. В этом случае ФДОЗ-А имеет сведения о месте нахождения ФДВ, в то время как ФДОЗ-В имеет сведения о месте нахождения СУДА).

5 Вторая ФДОЗ направляет запрос в СУДА. Запросы, отклоненные ФДВ, направляются в обход СУДА непосредственно в ФФО для представления инспектору.

6 СУДА оценивает удостоверяющие данные инспекторов на соответствие правилам доступа и представляет ответ на принятые запросы с данными атрибутов.

7 ФДОЗ направляет ответ в ФФО для представления инспектору.

Примечание 1 — Фальсификаты определяют по фактам выявления несовпадения атрибутов, предоставленных инспектору и размещенных на объекте.

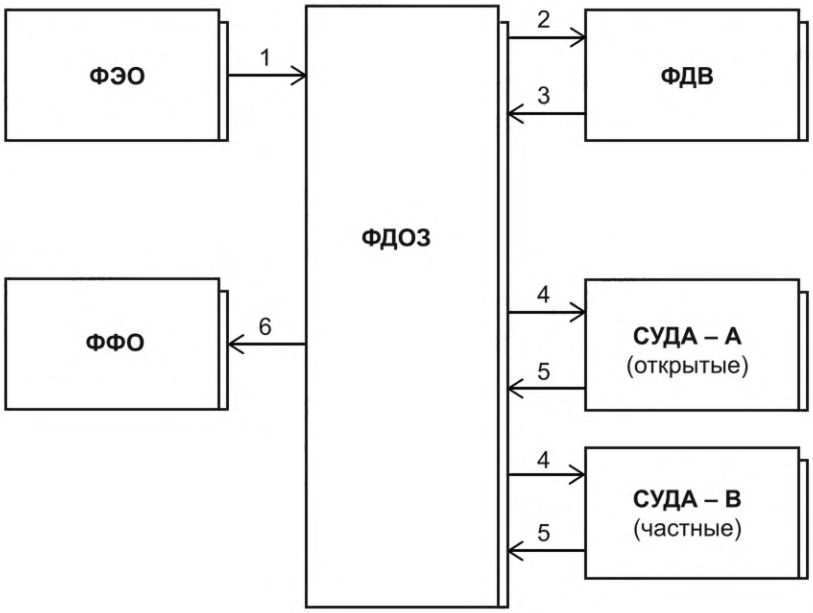
Примечание 2 — Фальсификаты определяют по фактам выявления слишком большого числа повторений конкретного УИД.

Примечание 3 — Фальсификаты определяют по фактам выявления экземпляров с конкретным УИД, одновременно находящимся в двух и более местах размещения.

Рисунок С.2 — Объект УИД экземпляра, пример без функции аутентификации

С.5 Объект с уникальным идентификатором группы, пример с функцией аутентификации

В настоящем примере используют УИД группы, при этом открытые мастер-данные хранятся в СУДА-А и конфиденциальные мастер-данные хранятся в СУДА-В. При настройке системы собственник загружает в СУДА описывающие атрибуты, относящиеся к каждому объекту в группе. Каждый УИД указывает на один набор данных атрибутов в какой-либо СУДА. Только инспекторы, представившие удостоверяющие данные, прошедшие проверку на соответствие правилам, загруженным в СУДА-В, будут получать ответы, содержащие конфиденциальные (составляющие частную собственность) мастер-данные.



Типовой запрос требует выполнение действий:

1 ФЭО извлекает УИД с объекта и направляет запрос во ФДОЗ.

2 ФДОЗ оценивает удостоверяющие данные инспекторов на соответствие правилам и направляет соответствующие запросы в ФДВ.

3 ФДВ проверяет действительность УИД. Если УИД является действительным и удостоверяющие данные инспектора приняты, ФДВ предоставляет адрес, где содержатся данные атрибутов.

4 ФДОЗ направляет принятые запросы (вместе с указателем адреса атрибутов) в СУДА-А, СУДА-В. Запросы, отклоненные ФДВ, направляются в обход СУДА напрямую в ФФО для представления инспектору.

5 Каждая из СУДА-А, СУДА-В оценивает удостоверяющие данные инспектора на соответствие правилам доступа и отвечает на соответствующие запросы данными атрибутов.

6 ФДОЗ направляет ответ ФФО для представления инспектору.

Примечание 1 — Фальсификаты определяют по фактам выявления несовпадения атрибутов, представленных инспектору и находящихся на объекте.

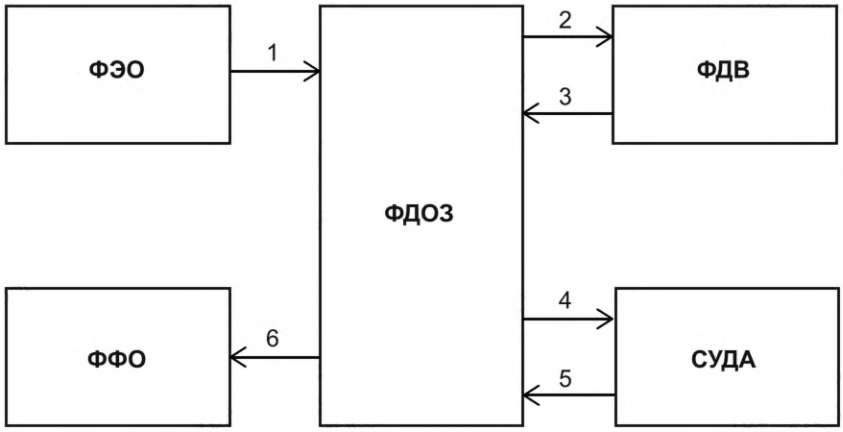
Примечание 2 — Фальсификаты определяют при выполнении ФДВ верификации по элементу аутентификации.

Рисунок С.3 — Объект с УИД группы, пример с функцией аутентификации[1)]

С.6 Объект с уникальным идентификатором экземпляра, пример с функцией аутентификации

В настоящем примере используются УИД экземпляров, каждый экземпляр объекта имеет отличный от других УИД. Каждый УИД поставлен в соответствие атрибутам одного экземпляра объекта. Другие объекты могут иметь идентичные или иные атрибуты. Возможна ситуация, когда только УИДы уникальны в группе объектов, а все объекты в классе имеют идентичные атрибуты и неразличимы без помощи УИД.

[1)] *Исправлена ошибка рисунка С.3 оригинального стандарта, на котором для ADMS-B указано «public».*



Типовой запрос требует выполнение действий:

1 ФЭО извлекает УИД с объекта и направляет запрос во ФДОЗ.

2 ФДОЗ оценивает удостоверяющие данные инспекторов на соответствие правилам и направляет соответствующие запросы в ФДВ.

3 ФДВ проверяет действительность УИД. Если УИД является действительным и удостоверяющие данные инспектора приняты, ФДВ предоставляет адрес, где содержатся данные атрибутов.

4 ФДОЗ направляет принятые запросы (вместе с указателем адреса атрибутов) в СУДА. Запросы, отклоненные ФДВ, направляются в обход СУДА напрямую в ФФО для представления инспектору.

5 СУДА оценивает удостоверяющие данные инспектора на соответствие правилам доступа и отвечает на соответствующие запросы данными атрибутов.

6 ФДОЗ направляет ответ в ФФО для представления инспектору.

Примечание 1 — Фальсификаты определяют по несоответствиям присланных инспектору атрибутов атрибутам объекта.

Примечание 2 — Фальсификаты могут быть определены в случае, когда конкретный УИД экземпляра запрашивается слишком большое количество раз.

Примечание 3 — Фальсификаты могут быть определены по фактам выявления экземпляра с конкретным УИД, который заявлен как находящийся в более чем одном месте нахождения в одно время.

Примечание 4 — Фальсификаты определяют при выполнении ФДВ верификации элемента аутентификации.

Рисунок С.4 — Объект с УИД экземпляра, пример с функцией аутентификации

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO 22300	IDT	ГОСТ Р 22.0.12—2015/ИСО 22300:2012 «Безопасность в чрезвычайных ситуациях. Международные термины и определения»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта: - IDT — идентичный стандарт.		

Библиография

[1] ISO 3166-1 Codes for the representation of names of countries and their subdivisions — Part 1: Country code (Коды для представления названий стран и их составных частей. Часть 1. Код страны)

[2] ISO 22380 Security and resilience — Authenticity, integrity and trust for products and documents — General principles for product fraud risk and countermeasures (Безопасность и устойчивость. Подлинность, целостность и доверие к продукции и документам. Общие принципы противодействия риску незаконных действий с продукцией)

[3] ISO 22381:2018 Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines for establishing interoperability among object identification systems to deter counterfeiting and illicit trade (Безопасность и устойчивость. Подлинность, целостность и доверие к продукции и документам. Руководство по установлению межоперабельности между системами идентификации объектов для предотвращения подделок и незаконной торговли)

[4] ISO 22382 Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines for the content, security, issuance and examination of excise tax stamps (Безопасность и устойчивость. Подлинность, целостность и доверие к продуктам и документам. Руководство по содержанию, безопасности, выпуску и проверке акцизных марок)

[5] ISO 22383 Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines for the selection and performance evaluation of authentication solutions for material goods (Безопасность и устойчивость. Подлинность, целостность и доверие к продукции и документы. Руководство по выбору и оценке эффективности решений по аутентификации для материальных товаров)

[6] ISO 22384 Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines to establish and monitor a protection plan and its implementation (Безопасность и устойчивость. Подлинность, целостность и доверие к продукции и документам. Руководство по разработке и мониторингу выполнения плана защиты)

[7] ISO/IEC 9594-8 Information technology — Open systems interconnection — Part 8: The Directory: Public-key and attribute certificate frameworks (Информационные технологии. Взаимосвязь открытых систем. Часть 8. Справочник. Структуры сертификатов открытого ключа и атрибутов)

[8] ANSI MH 10.8.2 Data Identifier and Application Identifier Standard (Стандарт идентификаторов данных и идентификаторов применения)[1)]

[9] ETSI/TS 101 456 Electronic Signatures and Infrastructures (ESI); Policy requirement for certification authorities issuing qualified certificates (Электронные подписи и инфраструктура. Требования политики для сертификационных органов, выдающих квалифицированные сертификаты)[2)]

[10] ETSI/TS 102 042 Electronic Signatures and Infrastructures (ESI); Policy requirement for certification authorities issuing public key certificates (Электронные подписи и инфраструктура. Требования политики для сертификационных органов, выдающих сертификаты открытых ключей)

[11] ITU-T Recommendation X.509 (03/00) Information Technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks (Информационные технологии. Взаимосвязь открытых систем. Справочник. Структуры сертификатов открытых ключей и атрибутов)

[12] WebTrust for CA CA criteria designated from many browsers (Критерии органа по сертификации, установленные с учетом использования множества браузеров)

[1)] *Общие требования к использованию ИП приведены в ГОСТ 34822—2022.*

[2)] *В Российской Федерации применение электронной подписи на основе Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».*

УДК 347.822.4:006.354 ОКС 13.310

Ключевые слова: идентификация, интероперабельность, проверка подлинности, фальсификации, незаконная торговля, прослеживаемость в цепи поставок, риск, фальсифицированная и контрафактная продукция

Редактор *Е.В. Якубова*
Технический редактор *И.Е. Черепкова*
Корректор *О.В. Лазарева*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 15.01.2026. Подписано в печать 06.03.2026. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 3,26. Уч.-изд. л. 2,77.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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