ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 16678— 2017

СИСТЕМА ЗАЩИТЫ ОТ ФАЛЬСИФИКАЦИИ И КОНТРАФАКТА

Идентификация интероперабельных объектов и связанные системы проверки подлинности для противодействия фальсификациям и незаконной торговле

**(ISO 16678:2014,
Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade,
IDT)**

Издание официальное

Москва
Стандартинформ
2017

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Международной ассоциацией организаций, осуществляющих деятельность по противодействию незаконному обороту контрафактной продукции «Антиконтрафакт», Федеральным государственным унитарным предприятием «Государственный научно-исследовательский институт авиационных систем» 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 7 ноября 2017 г. № 1668-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 16678:2014 «Руководство по идентификации интероперабельных объектов и связанных систем аутентификации для противодействия фальсификациям и незаконной торговле» (ISO 16678:2014 «Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade», IDT).

Наименование настоящего стандарта изменено относительно наименования ISO 16678:2014 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

5 ВВЕДЕН ВПЕРВЫЕ

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

© Стандартинформ, 2017

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

Содержание

1 Область применения 1
2 Термины, определения и сокращения 2
3 Общие положения 4
4 Ключевые принципы 7
5 Методические указания 8
Приложение А (рекомендуемое) Цифровые сертификаты (для инспекторов) 14
Приложение В (справочное) Управление мастер-данными 16
Приложение С (рекомендуемое) Примеры применения системы 17
Библиография 22

Введение

Настоящий стандарт разработан с учетом трех основных положений. Первое — выявление фальсифицированных объектов является комплексной и часто сложной задачей, второе — точная идентифицирующая информация о рассматриваемом объекте упрощает процесс выявления фальсификаций, и третье — точную идентифицирующую информацию часто 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 содержит 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. Из этого могут быть сделаны следующие заключения.

Улучшение интероперабельности объектов идентификации и связанных систем аутентификации должно упростить использование инспекторами этих систем. Улучшение в части облегчения использования расширит для инспекторов доступ к множеству систем, содержащих достоверную информацию, таким образом увеличит способности к выявлению фальсификатов и снизит потери, связанные с фальсификациями.

Настоящий стандарт определяет правила направления запросов на получение связанной с объектом информации от соответствующих уполномоченных служб и направления ответов на них инспекторам.

Системы идентификации объектов, как правило, используют уникальные идентификаторы (УИД) для ссылок или получения доступа к информации об объекте. УИД может быть присвоен группе объектов или отдельному объекту. В обоих случаях применение УИД расширяет возможности выявления фальсификаций и контрафакта, хотя УИДы, присвоенные отдельным объектам, являются более эффективными. Настоящий стандарт включает шесть разделов:

- область применения: определяет ограничения в применении настоящего стандарта, как содержащего только общие правила и рекомендации. Настоящий стандарт не содержит обязательных требований;

- термины: определяет смысловое содержание значимых терминов, применяемых в настоящем стандарте, таких как «инспектор», «семантическая интероперабельность»;

- общие положения: содержит общее описание правил использования информации об объекте для выявления фальсификаций;

- ключевые принципы: содержит концепции и положения, влияющие на методические указания;

- методические указания: содержит описание методов, которые могут улучшить совместимость систем, способных предоставлять инспекторам информацию об объектах;

- информационные приложения: специальные примеры, поясняющие некоторые из концепций и положений, представленных в настоящем стандарте.

Ожидаемые результаты

Расширение области применения решений по валидации и аутентификации, повышение их эффективности в выявлении и противодействии правонарушениям, таким как фальсификации и незаконное использование объектов не по назначению. Настоящий стандарт предназначен для создания надежной и безопасной системы идентификации и аутентификации объектов для противодействия поступлению незаконных объектов на рынок.

Целью настоящего стандарта является представление схем взаимодействия, в которых обеспечивается совместимость различных решений по идентификации и аутентификации объектов и повышается уровень взаимного доверия участников оборота объектов на рынке. Представленные в стандарте схемы допускается использовать часто как типовые решения. Отдельные схемы могут также включать решения, которые позволяют выявлять фальсификации без аутентификации продукции. Помимо этого, схемы могут включать решения, которые позволяют получать оценки в отношении только отдельных элементов аутентификации.

Поскольку является вероятным, что системы идентификации и аутентификации объектов сами будут фальсифицироваться и копироваться, настоящий стандарт устанавливает метод формального подтверждения, что полученному из удаленного источника описанию объекта можно доверять. Участниками оборота объектов должны быть приняты меры к исключению несоответствий в данных, получае-

мых при различных независимых обращениях к указанным системам, обеспечению получения непротиворечивых данных об уникальной идентификации объектов при многократном обращении к системам и в различных приложениях.

В основе построения указанных систем стоит положение о том, что утрата взаимного доверия и утрата согласованности данных являются основными причинами противоречий между участниками оборота объектов. Для устранения этих противоречий необходимо обеспечить большую осведомленность участников оборота в данных об объектах и более широкую применимость систем, что позволит лучше выявлять и предотвращать правонарушения.

В настоящем стандарте внесены следующие редакционные изменения, не изменяющие техническое содержание и структуру аутентичного текста стандарта ISO 16678:2014. В таблице А.1 вместо обозначения конкретных географических информационных систем QGIS и QIIS приведена фраза о «географических информационных системах, применяемых в федеральных и муниципальных органах власти Российской Федерации», поскольку перечень применяемых в Российской Федерации таких систем включает и иные системы, в том числе и отечественной разработки. Из введения в перечислении **«термины:»** исключен термин «доверенный агент (trusted agent)», отсутствующий в разделе 2 и в тексте стандарта.

В тексте стандарта добавлены ссылки на документы, приведенные в структурном элементе «Библиография», отсутствующие в международном стандарте.

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 — 2018—07—01

1 Область применения

Настоящий стандарт устанавливает требования к построению систем идентификации и аутентификации объектов[1] (далее — системы). Он содержит рекомендации и методы, составленные на основе наилучших практик, относящиеся к:

- положениям о присвоении и верификации идентификаторов[2], физическом представлении идентификаторов, принятии мер должной осмотрительности участниками;
- проверке всех участников системы в рамках применения системы;
- взаимосвязи между уникальными идентификаторами и возможными элементами аутентификации, относящимися к ним;
- запросам инспекторов, относящимся к идентификации и авторизованному доступу к привилегированной информации об объекте;
- истории получения инспектором доступа к данным (регистрационные журналы).

Настоящий стандарт устанавливает схему построения систем и определяет состав функциональных подсистем, применяемых для достижения надежности и интероперабельности[3] работы таких систем.

Настоящий стандарт не определяет технические требования к реализации конкретной системы, но определяет общие требования к процессам, функциям и функциональным подсистемам, используя общую модель операций в рамках системы для пояснения вариантов применения системы. Системы идентификации и аутентификации объектов могут включать подсистемы, имеющие другие функции, такие как прослеживаемость цепи поставок, прослеживаемость характеристик качества, маркетинговая деятельность и др., но эти аспекты выходят за область применения настоящего стандарта.

Примечание — Настоящий стандарт не регламентирует специальные требования к идентификации промышленной продукции, такие как присвоение Глобального номера предмета торговли (Global Trade Item Number).

---

[1] Здесь под объектами понимаются товары народного потребления и товары производственного назначения по ГОСТ Р 51303—2013, в отношении которых участники системы принимают меры по уникальной идентификации и аутентификации, выявлению и исключению из оборота фальсифицированных объектов.

[2] Здесь под идентификатором (уникальным идентификатором) понимается обозначение товара, присвоенное по ГОСТ Р ИСО/МЭК 15459-3—2007, ГОСТ Р ИСО/МЭК 15459-4—2007, ГОСТ Р ИСО/МЭК 15459-6—2009.

[3] Термин «интероперабельность» по ГОСТ Р 55062—2012 «Информационные технологии. Системы промышленной автоматизации и их интеграция. Интероперабельность. Основные положения».

Издание официальное

2 Термины, определения и сокращения

2.1 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями.

2.1.1 **система управления данными атрибутов** (СУДА) (attribute data management system (ADMS)): Система, которая хранит данные, управляет данными и контролирует доступ к данным, относящимся к объектам.

2.1.2 **аутентификация** (authentication): Процесс подтверждения подлинности сущностей или атрибутов с установленным или известным уровнем гарантии.

[ISO/IEC 29115]

2.1.3 **функция аутентификации** (authentication function): Функция, выполняющая проверку подлинности (аутентификацию).

2.1.4 **достоверный источник данных** (authoritative source): Официально установленный источник данных атрибута, ответственный за поддержание достоверности данных атрибута.

2.1.5 **копия хранителя** (custodian copy): Дубликат данных, находящихся в распоряжении достоверного источника.

2.1.6 **сущность** (entity): Нечто, существующее отдельно и независимо и которое может быть охарактеризовано набором данных, связанных с контекстом (средой, в которой находится сущность).

Примечание — Сущность может быть человеком, организацией, физическим объектом, классом объектов, нематериальным объектом.

[ISO/IEC 29115]

2.1.7 **идентификация** (identification): Процесс распознавания признаков, идентифицирующих объект.

[ISO/IEC 29115]

2.1.8 **идентификатор** (identifier): Установленный набор признаков, присвоенный сущности с целью идентификации.

2.1.9 **идентичность** (identity): Набор атрибутов, относящихся к сущности.

Примечания

1 Идентичность может иметь уникальные атрибуты, позволяющие отличить объект от всех других.

2 Идентичность может рассматриваться в отношении человека, организации, объекта (физического или нематериального).

2.1.10 **инспектор** (inspector): Лицо или устройство, использующее функции проверки объекта для получения оценки объекта.

Примечания

1 Любой участник системы может действовать в роли инспектора.

2 Инспекторы могут иметь различный уровень квалификации и подготовки.

3 Инспектором может быть автоматизированная система.

2.1.11 **история получения доступа инспектором** (inspector access history): Журнал регистрации доступа, содержащий данные о том, когда (дата события) были проверены данные кодов уникального идентификатора (УИД), каким (привилегированным или иным) инспектором (необязательные данные), с какого конкретного пункта (необязательные данные).

Примечание — В журнале также могут быть использованы метки времени.

2.1.12 **интероперабельность**[1)] (interoperability): Способность отдельной точки входа в систему направлять запросы в отношении объектов, имеющих УИД, в уполномоченные достоверные источники данных для выполнения функции доверенной верификации (ФДВ).

Примечание — Также означает способность множества систем аутентификации предоставлять ответы группам пользователей.

2.1.13 **объект** (object): Любая единичная и отличимая от иных сущность, которая может быть идентифицирована[2)].

[1)] В общем случае термин «интероперабельность» по ГОСТ Р 55062—2012.

[2)] Здесь под объектами понимаются товары народного потребления и товары производственного назначения по ГОСТ Р 51303—2013, в отношении которых участниками системы принимаются меры по уникальной идентификации и аутентификации, выявлению и исключению из оборота фальсифицированных объектов.

2.1.14 **функция экспертизы объекта** (ФЭО) (object examination function (OEF)) — действия по поиску или анализу УИД или иных атрибутов с намерением установления подлинности объекта (аутентификации).

Примечание — В этом процессе иные атрибуты могут содействовать оценке подлинности УИД.

2.1.15 **собственник:** Сущность[1], которая на законных основаниях обладает правами пользователя объекта, предоставляет права использования, распространения объекта, которому присвоен УИД.

2.1.16 **участник системы:** Поставщик решений в области идентификации интероперабельных объектов и связанных систем аутентификации, пользователь систем идентификации, включая, но не ограничиваясь этим перечислением, обладателей защищаемых законом прав на объекты, должностных лиц таможни, дистрибьюторов и потребителей[2].

2.1.17 **семантическая интероперабельность** (semantic interoperability): Способность двух и более систем или служб автоматически интерпретировать и использовать информацию, обмен которой произведен безошибочно.

2.1.18 **синтаксическая интероперабельность** (syntactic interoperability): Способность двух или более систем или служб обмениваться структурированной информацией.

2.1.19 **функция доверенной обработки запросов** (ФДОЗ) (trusted query processing function (TQPF)): Функция, предоставляющая вход в функцию доверенной верификации и в систему управления данными атрибутов.

Примечание — Реализуется с применением программных средств, работающих локально на портативном устройстве.

2.1.20 **функция доверенной верификации** (ФДВ) (trusted verification function (TVF)): Функция, проверяющая статус УИД — действительный или недействительный — и управляющая ответом в соответствии с правилами и привилегиями доступа.

2.1.21 **уникальный идентификатор**[3] (УИД) (unique Identifier (UID)): Код, представленный одним специальным набором знаков, которые поставлены в соответствие объекту или группе объектов на протяжении срока существования объекта в рамках специального домена и области применения системы идентификации объекта.

2.1.22 **верификация** (verification): Проверка, что УИД существует и действителен в рамках системы идентификации объектов.

Примечание — Верификация может показать наличие некоторых типов фальсификаций, но сама по себе не доказывает аутентичность сущности.

2.2 Сокращения

В настоящем стандарте применены следующие сокращения:

СУДА — система управления данными атрибутов (Attribute Data Management System (ADMS));
ИП — идентификатор применения (Application Identifier (AI)) (см. [6], [11]);
ОС — орган, уполномоченный по сертификации (Certification Authority (CA));
ИД — идентификатор данных (Data Identifier (DI)) (см. [6], [11]);
ФЭО — функция экспертизы объекта (Object Examination Function (OEF));
ФФО — Функция форматирования отчетов (Response Formatting Function (RFF));
ФДОЗ — функция доверенной обработки запросов (Trusted Query Processing Function (TQPF));
ФДВ — функция доверенной верификации (Trusted Verification Function (TVF));
УИД — уникальный идентификатор (Unique Identifier (UID)).

---

[1] Обладатели защищаемых законом прав на объекты (прав интеллектуальных и на средства индивидуализации), изготовители.

[2] 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] В общем случае «уникальный идентификатор» по ГОСТ Р ИСО/МЭК 15459-3—2007, ГОСТ Р ИСО/МЭК 15459-4—2007, ГОСТ Р ИСО/МЭК 15459-6—2009.

3 Общие положения

3.1 Общие требования

Преимуществом применения интероперабельных систем идентификации и аутентификации является улучшение условий для выявления фальсифицированных и контрафактных объектов за счет:

- расширения возможностей применения систем специальными группами пользователей;
- увеличения количества инспектируемых объектов;
- расширения доступа к ресурсам достоверных данных, а также
- снижения затрат на содержание систем, связанных:
  - с обучением персонала;
  - с оснащением;
  - с разработкой;
  - с развертыванием;
  - с проверками.

Как только интероперабельность достигнута и системы доступны для потребителей, инспектор может применить идентификатор для производства запроса в отношении объекта, ответ на который им будет использован при принятии решения о действиях в отношении объекта. Инспектор должен иметь подтверждения, что представленная в ответе информация является точной и заслуживающей доверия.

Действия участников системы должны выполняться в рамках своих ролей с соблюдением следующих общих требований.

Проведение инспекций и проверок поставщиков услуг следует рассматривать как изначально основанное на предположении о добросовестности их действий, а не как изначально направленное на выявление их недобросовестности и причинение им ущерба.

Проведение инспекций и проверок изготовителей следует рассматривать как изначально основанное на предположении следования ими документированным процессам и предоставления ими точной информации в системы.

Заинтересованные стороны, имеющие потребность в получении данных, должны получать соответствующие полномочия на подачу и обработку запросов, так чтобы обладатели защищаемых законом прав на объекты могли предоставлять информацию, руководствуясь социальной ответственностью.

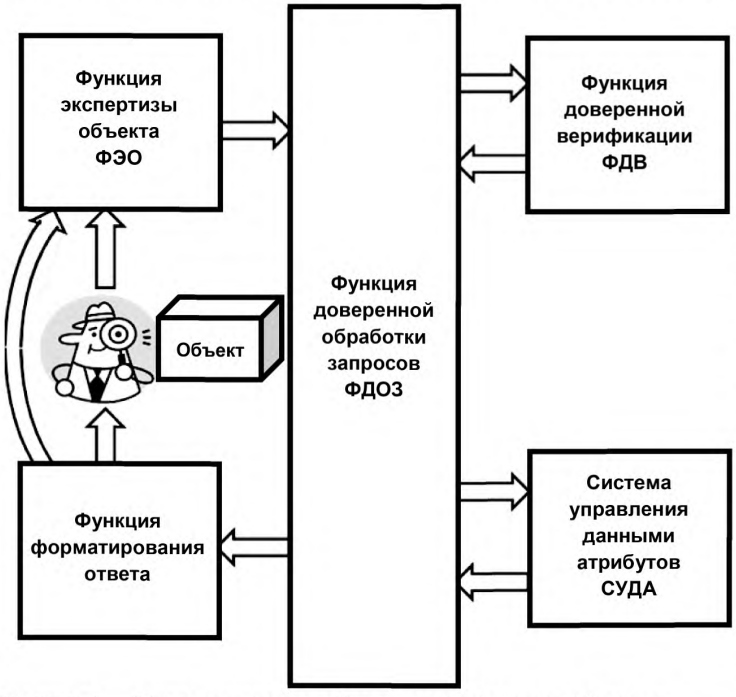


Рисунок 1 — Модель инспекции объекта в системе идентификации и аутентификации

3.2 Системы идентификации и аутентификации объектов (находящиеся в процессе применения)

3.2.1 Общие сведения

Системы идентификации и аутентификации объектов, как правило, состоят из функциональных единиц, указанных ниже на модели (рисунок 1).

Модель не содержит описания способов реализации функций. В системе может быть реализовано множество видов функций. Различные функции могут быть объединены в одну услугу.

Пример, раскрывающий применение данной модели, приведен в приложении С.

3.2.2 Функция экспертизы объекта (ФЭО)

Инспектор проводит экспертизу интересующего его объекта (например, товара, имеющего вещественную форму) с целью определения наличия у него УИД. Если УИД обнаружен, дальнейшая

экспертиза может потребовать определения, какая функция (функции) доверенной обработки запросов может содержать данные об этом УИД. Функции формируют запросы, которые могут состоять только из УИД, из комбинации УИД и удостоверяющих данных инспектора или содержать другие данные физических атрибутов, включая существенные присущие объекту элементы аутентификации, которые могут уникально идентифицировать объект, например такие, как цифровое изображение. Функция экспертизы объекта включает принятие решения о направлении запроса в одну или более ФДОЗ. Когда процесс повторяется, ФЭО может оценить ответ и на предыдущий запрос.

3.2.3 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.

Например, ФДОЗ может маршрутизировать запрос, сформированный ФЭО к соответствующей ФДВ. ФДОЗ может комбинировать ответ по верификации или аутентификации от ФДВ при любых удостоверяющих данных инспектора для формирования запроса в СУДА.

3.2.4 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 обычно 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).

3.2.5 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 множество 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.

СУДА получает ответ (через ФДОЗ) из ФДВ. СУДА проверяет как удостоверяющие данные запрашивающей ФДОЗ, так и удостоверяющие данные инспектора. Привилегии допуска должны быть основаны на удостоверяющих данных и установленных правилах. СУДА отвечает, используя выбранные данные, связанные с запросом и отфильтрованные в соответствии с установленными правилами. 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 исследование.

СУДА должна обеспечивать защиту конфиденциальных данных от несанкционированного доступа.

3.2.6 Функция форматирования ответов

Функция преобразует ответы СУДА в установленный формат.

В некоторых случаях процесс экспертизы может быть повторен исходя из результатов, представленных СУДА, или основываясь на архитектуре системы.

3.3 Системы идентификации и аутентификации объекта (находящиеся в процессе формирования)

Перед началом применения системы должны быть установлены правила функционирования системы, определены содержащиеся в системе данные и отношения между данными.

На рисунке 2 показан вариант конфигурации формируемой системы.

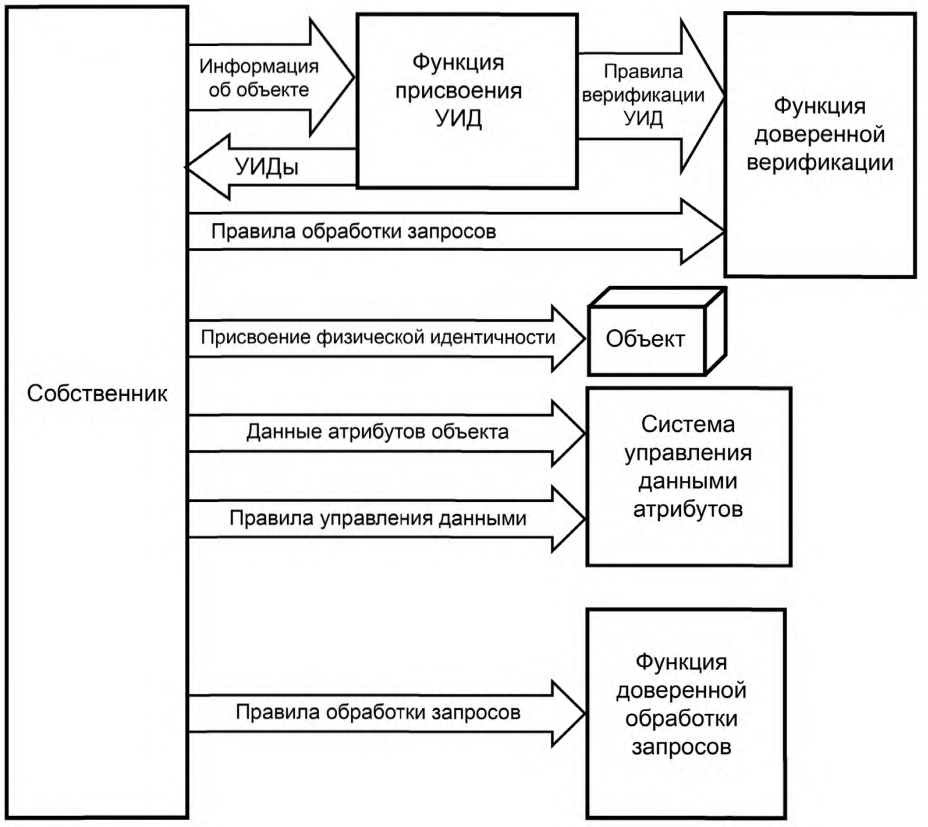


Рисунок 2 — Конфигурирование системы при ее формировании

3.3.1 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.

3.3.2 Функция присвоения УИД

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.

3.3.3 Информация об объекте

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

3.3.4 Правила верификации УИД

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.

3.3.5 Установление физической идентичности

Установление связи между УИД и объектом может быть осуществлено путем регистрации в системе присвоенного УИД.

3.3.6 Данные атрибутов объекта

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

3.3.7 Правила управления данными

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

- прав доступа, включая в себя:
  - 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 в себя:
  - бизнес-правила раскрытия данных по запросу;
  - формы ответов на запросы (например, форма ответа, когда УИД является недействительным);
  - правила ответов на запросы в рамках привилегированного доступа и непривилегированного доступа.

3.3.8 Правила обработки запросов

К правилам обработки запросов относятся правила, которые позволяют функциям:

- маршрутизировать запрос или ответ для соответствующей функции,
- верифицировать, поступил ли запрос от участника, имеющего установленные полномочия запрашивать, или требуется разрешение на запрос;
- верифицировать, является ли линия коммуникаций, по которой поступил запрос, установленной для этого или одной из разрешенных к применению.

4 Ключевые принципы

4.1 Доступность к использованию и своевременность ответа

Доступность системы к использованию и время отклика на запрос должны отвечать ожиданиям инспектора.

Время на предоставление ответа должно включать время, необходимое для проверки удостоверяющих данных. Рекомендуется, чтобы доступность системы к использованию и время отклика на запрос были указаны в соглашении об уровне обслуживания.

4.2 Достоверный источник данных

Только один достоверный источник данных должен быть связан с идентифицируемым объектом. Множество источников может ввести в заблуждение инспектора, злонамеренный поставщик услуг может скопировать источник, манипулировать им и заявить себя инспектору как один из достоверных источников данных. Должны быть поставщики услуг в рамках системы, которые имеют привилегии хранителей копий данных, но пользователям должно быть всегда известно, кто является достоверным источником данных в отношении объекта и почему копиям хранителей данных можно доверять.

4.3 Управление данными

Мастер-данные и данные транзакций следует поддерживать в актуальном состоянии. Управление данными следует осуществлять в сроки, согласованные с ожидаемым сроком жизненного цикла объекта. Должно быть принято во внимание, что нормативные требования в будущем могут быть изменены, а также учтены требования по проведению идентификации объектов с длительным сроком существования, в отношении которых при обслуживаниях, выполнении гарантийных обязательств и при испытаниях следует проводить действия по аутентификации. См. приложение В в части основных концептуальных положений об управлении мастер-данными и управлении данными транзакций.

4.4 Принцип действительной необходимости ознакомления с данными

Для создания эффективной системы любые сведения относительно состава характеристик, значений характеристик, процессов и архитектуры системы должны быть защищены и предоставлены пользователям только на основе принципа действительной необходимости ознакомления.

4.5 Защита данных

Система содержит критичные для деловых интересов участников системы данные и должна использовать лучшие практики защиты данных. В рамках проектирования и организации технической

эксплуатации системы должны быть реализованы меры, которые обеспечат необходимый уровень защиты конфиденциальности, целостности, актуальности информации, содержащейся в системе.

4.6 Конфиденциальность

Любые персональные идентификационные данные должны быть защищены на основе законодательных норм и иных установленных требований, в отсутствие правового регулирования в отношении каких-либо иных видов данных следует использовать лучшие практики защиты данных.

4.7 Соблюдение установленных норм

Различные отрасли промышленности и различные страны регулируются своими нормативными документами, которые не могут быть учтены в настоящем стандарте. Любые интероперабельные системы должны быть приспособлены к тому, чтобы обеспечить соответствие особым нормативным требованиям.

4.8 Проверки

Собственники должны гарантировать, что применение ФДВ и СУДА заслуживает доверия. Они должны принимать во внимание результаты аудитов и удостоверяющие данные поставщиков и рассматривать их анализ как часть процесса выбора поставщиков. Собственники должны гарантировать, что удостоверяющие данные доступны и актуальны.

При обращении к ФДОЗ любого участника системы должно быть гарантировано, что применение системы заслуживает доверия и удостоверяющие данные участников системы актуальны.

Поставщики услуг должны проводить проверки данных потребителей, запрашивающих их услуги по контракту, для противодействия злонамеренным участникам, которые пытаются представить себя собственниками.

Проверки должны быть двунаправленными, и для достижения высокого уровня доверия участники системы должны характеризоваться удостоверяющими данными.

4.9 Интероперабельность

Интероперабельность — способность двух и более систем или служб обмениваться структурированной информацией (синтаксическая интероперабельность), автоматически ее интерпретировать (семантическая интероперабельность) и затем использовать информацию, обмен которой был произведен точно, без искажения смысла, для получения приемлемых для них результатов.

Принципы интероперабельности включают в себя:

- определение целевых групп пользователей, в том числе:
  - определение минимальных информационных потребностей пользователей;
  - определение таблицы форматов сообщений (при необходимости);
  - заключение соглашения по управлению правами доступа;
- определение правил действий с данными, в том числе:
  - заключение соглашения о собственности на данные;
  - заключение соглашения о защите данных и ограничениях по их пользованию;
- определение интерфейса для обмена данными, в том числе:
  - определение применяемых стандартов обмена данными;
  - определение уровня предоставляемых услуг для гарантированного получения ответа.

4.10 Присвоение УИД

УИД должны присваиваться таким образом[1)], чтобы они были уникальны в домене, в котором предоставляется услуга.

5 Методические указания

5.1 Введение

Условия применения отдельных систем могут существенно отличаться, однако должны быть реализованы общие функции таких систем, которые обеспечивают интероперабельность. Это позволяет давать описание систем с точки зрения функциональности для представления общих операций. В 5.2 и 5.3 приведены общие характеристики этих систем.

[1)] Присвоение УИД по ГОСТ Р ИСО/МЭК 15459-3—2007, ГОСТ Р ИСО/МЭК 15459-4—2007, ГОСТ Р ИСО/МЭК 15459-6—2009.

Представленные здесь указания в основном ориентированы на общие характеристики фальсификаций, перечисленные в 5.4. Особенности применения систем влияют на эффективность, с которой в рамках услуги может быть выявлен каждый конкретный вид фальсификаций из перечисленных. Методические указания направлены на демонстрацию наиболее эффективных подходов для каждого вида фальсификаций. Положения, согласованные с 5.4, раскрывают преимущества и недостатки наиболее общих подходов к применению систем для содействия заинтересованным сторонам в выборе наиболее подходящего подхода исходя из конкретной ситуации.

5.2 Определение доверенных услуг

5.2.1 Общие сведения

Инспектор должен определить, какая ФДОЗ связана с объектом. Инспектор должен также оценить уровень доверия, связанный с привлекаемой ФДОЗ. При разработке функции экспертизы объекта должны быть приняты во внимание проблемы, с которыми сталкивается новый или с недостатком опыта инспектор при определении ФДОЗ.

Необходимо обеспечить максимально легкий поиск ФДОЗ, относящейся к объекту. Для этого должно быть принято во внимание все, что делает более легким корректное определение ФДОЗ.

5.2.2 Обеспечение доверия к ФДОЗ

ФДОЗ, которая работает как портал для инспекторов, должна быть 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.

5.2.3 Использование префикса или постфикса

В целях улучшения интероперабельности могут быть использованы стандартные идентификаторы данных (ИД) и идентификаторы применения (ИП)[1)] в качестве префиксов или постфиксов данных для облегчения задачи для ФДОЗ маршрутизировать запрос в корректную ФДВ. В библиографии представлены несколько существующих стандартов, определяющих ИД и ИП, [1], [2], [6], [7], [11].

При отсутствии ИП, ИД или иных вспомогательных средств для локализации услуги принятым подходом является осмотр объекта для выявления логотипов товарных знаков или других признаков, которые идентифицируют изготовителя объекта. Инспекторы могут обратиться к изготовителю для содействия в поиске ФДОЗ.

5.2.4 Методы экспертизы объектов

При наличии всех данных и идентифицирующих признаков объекта в системе, при выполнении участниками всех соглашений и правил экспертиза объекта выполняется без дополнительных методических указаний по [3], [4], [12], [13], [14], [15], [16], [17], [18], [19], [20], [22]. В неидеальных случаях следует принимать во внимание ухудшение возможностей проведения экспертизы объектов при утрате УИД или внесении искажений в УИД. Для расширения возможностей экспертизы объектов следует использовать элементы избыточности и корректировки ошибок для улучшения характеристик при таких обстоятельствах.

Следует принимать во внимание необходимость обеспечения возможностей выполнения функций экспертизы объектов в условиях частичного нарушения правил и соглашений участниками системы. Следует избегать потери взаимного доверия участников системы, в результате которого поведение пользователей будет диктоваться защитными реакциями.

5.3 Управление данными и атрибутами идентификации объектов

5.3.1 Общие сведения

Инспектор с необходимыми удостоверяющими данными может направить запрос в ФДОЗ, результатом которого будет ответ от СУДА. Если правила доступа разрешают, ответ СУДА будет содержать данные идентификации объекта или другие атрибуты объекта.

[1)] По ГОСТ ISO/IEC 15418—2014 «Информационные технологии. Технологии автоматической идентификации и сбора данных. Идентификаторы применения GS1 и идентификаторы данных ASC MH 10 и их ведение».

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.

5.3.2 Проверка точки входа для получения услуги (ФДОЗ)

Заинтересованные участники системы должны принимать 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. Примерами таких вопросов являются:

- является ли поставщик услуги заслуживающим доверия?
- является ли надежным источник, предоставивший данные об объекте?

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 используемых услуг у других участников системы и проверить, что все предоставляемые удостоверяющие данные действительны, для чего они должны иметь возможность обратиться с запросом к вызывающему доверие органу (организации).

5.3.3 Ведение данных и управление доступом

Собственники должны гарантировать, что данные в системе являются достоверными и актуальными. Например, если атрибут, описывающий объект в составе класса объектов, изменен, соответствующая информация в СУДА должна быть обновлена.

Собственник должен гарантировать, что функции, обеспечивающие предоставление прав доступа к данным, реализуются по актуализированным правилам и для авторизованных пользователей.

5.3.4 Уровни привилегий и роли пользователей

Доступ к конфиденциальным данным идентификации объекта может зависеть от привилегий доступа. Например, ответы, содержащие важные и конфиденциальные данные об объекте, могут направляться только инспекторам с очень высоким уровнем удостоверяющих данных, в то время как ответы, направляемые инспекторам без удостоверяющих данных, могут содержать только данные, находящиеся в публичном доступе.

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

5.3.5 Контроль доступа

Применяемые в отраслях промышленности практики предоставления прав доступа к данным отличаются по многим причинам, таким как различные нормативные требования, ограничения в линиях коммуникаций, стоимость оборудования и другие. 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.

5.3.6 Собственность на данные транзакций

События транзакции и учетные записи генерируются при функционировании 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 контрактные отношения между заинтересованными участниками системы для предотвращения неправильного применения данных.

5.3.7 Использование данных транзакций

Коды УИД без соответствующей функции аутентификации не могут быть использованы для определения подлинности объекта, однако записи в журнале регистрации событий могут определить некоторые систематические атаки и помочь изолировать фальсифицированные объекты.

Например, запись 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.

5.3.8 Государственные, международные организации и уполномоченные органы

Государственные и международные организации могут устанавливать требования для обеспечения 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.

5.4 Основные виды фальсификаций

5.4.1 Дублирование кодов УИД

Методы, используемые для дублирования кодов УИД, различаются для идентификаторов, присвоенных группам, и идентификаторов, присвоенных индивидуальным экземплярам объектов. При дублировании УИД за счет повторного присвоения, случайного совпадения, повторного использования дубликаты или «клоны» существуют в одной системе. Системы или услуги должны быть спроектированы так, чтобы выявлять и сигнализировать о наличии дублирующих кодов УИД. Выявление дублирующих кодов УИД обоих типов (для групп и для экземпляров объектов) может проводиться на основе следующих данных (перечень не является исчерпывающим):

- запросов, поступающих из неавторизованных мест нахождения или от неавторизованных инспекторов, и
- описаний объектов, которые не соответствуют описаниям, представленным из СУДА.

Признаком дублирования кода УИД для отдельного экземпляра объекта могут быть данные (перечень не является исчерпывающим):

- запросов, поступающих с разных мест нахождения в одно и то же время, и
- большего количества запросов, чем может ожидаться для одного кода УИД.

С целью снижения рисков 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 (личные) ключи;
- закодированная информация, относящаяся к элементам безопасности, и
- различные физические свойства и маркировки.

Смежный уровень физической безопасности включает в себя (перечень не является исчерпывающим):

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

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

5.4.2 Замещение

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

Недобросовестные участники системы могут использовать множество методов совершения 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 упаковки, обеспечивающих обнаружение вскрытия;
- использование общедоступного утвержденного перечня авторизованных источников;
- прослеживание кодов УИД, инспекторов и инспекций;
- деактивирование кодов УИД.

5.4.3 Недостоверные характеристики

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

- УИД утрачен;
- 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.

5.4.4 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, попытки доступа с имитацией IP адреса запрашивающего, переадресацию;
- атаку посредника (перехват и подмена сообщений третьим лицом).

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

- использование шифрованных каналов связи между функциональными элементами системы;
- использование цифровых сертификатов по [8], [9], [10], [21];
- проведение периодических проверок работоспособности доверенных элементов аппаратного/программного обеспечения;
- использование открытого утвержденного перечня и
- использование доверенных вебсайтов как допустимых точек входа, например веб-сайтов:
  - собственника;
  - отрасли промышленности;
  - доверенной третьей стороны.

Собственники должны обеспечивать проведение аудитов систем и услуг, а также доступность их 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.

5.4.5 Фальшивый инспектор

В системе должны быть реализованы средства распознавания фальшивых запросов. Например, должны быть реализованы записи регистрации доступа и процедуры, которые проверяют необходимость предоставления доступа на основе соответствия принципу действительной необходимости ознакомления пользователя с запрашиваемыми данными.

5.4.6 Атаки инсайдеров

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

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

В системе должны быть реализованы методы снижения рисков от атак инсайдеров (перечень не является исчерпывающим), включающие:

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

Приложение А
(рекомендуемое)

Цифровые сертификаты (для инспекторов)

А.1 Введение

В настоящем приложении представлено возможное применение сертификатов по [5], [8] для доведения удостоверяющих данных инспекторов до функциональных подсистем системы идентификации и аутентификации объектов. В данном примере интероперабельность улучшается за счет использования правил [5], [8] в целях доставки информации по Интернету. Это достигается путем использования OU1 или OU2 (пример в таблице А.1).

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

Должны быть установлены безопасные и доверенные коммуникации между функциями. Правила [5], [8] являются методом реализации этого требования при использовании находящихся в общественном доступе сетей.

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

Использование цифровых сертификатов для обеспечения контроля доступа к СУДА является одной из лучших практик, но при этом собственник торговой марки должен рассмотреть достоверность как инспектора, так и самого цифрового сертификата.

А.3 Достоверность инспектора

Собственник торговой марки должен рассмотреть достоверность инспектора, получившего цифровой сертификат с целью получения доступа к высоко конфиденциальным данным в системе управления данными атрибутов. Более высокая достоверность может быть получена использованием открытого перечня обладателей сертификатов. Открытый перечень включает доверенных инспекторов, включаемых в перечень уполномоченным источником.

А.4 Достоверность цифрового сертификата[1)]

С целью гарантировать достоверность электронной подписи пользователя следует использовать цифровой сертификат пользователя, выпущенный аккредитованным/уполномоченным органом по выдаче сертификатов в соответствии со следующими документами:

- [10];
- [9];
- [21] для органов сертификации.

А.5 Общее поле действия цифрового сертификата

Могут быть необходимыми общие профили цифровых сертификатов с целью достижения интероперабельности между системами.

Пример общего профиля представлен в таблице А.1.

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

Поля сертификата	Тип данных (число знаков)	Определение	Полномочия	Пример
Субъект				
Наименование страны	Печатная строка (2)	Два знака кода страны по ИСО 3166-1 (2 знака) - все буквы прописные	Администратор	JP
- Наименование области государства	Печатная строка (128)	-Наименование области, региона, т. д. - первая буква прописная	Администратор	Токио

[1)] В Российской Федерации электронная подпись, ключ проверки электронной подписи, сертификат ключа проверки электронной подписи в соответствии с Федеральным законом от 06.04.2011 «Об электронной подписи» № 63-ФЗ. Процессы формирования и проверки электронной цифровой подписи — по ГОСТ Р 34.10—2001.

Окончание таблицы А.1

Поля сертификата	Тип данных (число знаков)	Определение	Полномочия	Пример
Наименование района	Печатная строка (128)	- наименование города, др. - первая буква прописная - разделителем является дефис	Администратор	Минато-ку Minato-ku
Наименование организации	Печатная строка (64)	- наименование организации[a]	Администратор	JIPDEC
Наименование подразделения 1-й организации	Печатная строка (64)	- идентификатор управляющего администратора - для распознавания при автоматической идентификации, должен добавляться префикс «OU1-»[b]	Администратор	OU1-G2—1.2.392.200063.80.1.1
Наименование подразделения 2-й организации	Печатная строка (64)	- Идентификатор управляющего ОР или ЛОР - для распознавания при автоматической верификации, должен добавляться префикс «OU2-»[c]	Орган регистрации или локальный орган регистрации (ОР или ЛОР)	OU2—007
Полное имя	Печатная строка (64)	- Имя субъекта (полное имя, сокращенное имя, роль или ID) - для распознавания при автоматической верификации может добавляться префикс «BN-» (бизнес-имя, используемое как официальное полное имя в организации, такое как подлинное имя и девичья фамилия), «BO-» (организация/роль), или «ID-»	Орган регистрации или локальный орган регистрации (ОР или ЛОР)	Smith Betty (менеджер по снабжению)

[a] Следует использовать наименование, зарегистрированное в географических информационных системах, применяемых в федеральных и муниципальных органах власти Российской Федерации.

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

[c] Допускается использовать как указатель закрытых атрибутов (наименование составной части и т. п.), которое не записано 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, также как и к безопасности продукции, влияют на принятие решения об отзыве продукции и на меры против фальсификаций. Свойствами наборов данных являются их отнесение к открытым данным или конфиденциальным данным, в последнем случае требуется авторизованный доступ к информации об объекте, когда обнаруживается проблема фальсификации.

Доступ к мастер-данным объекта требует определенных уровней аутентификации для доступа, обычно контролируемого собственником торговой марки или собственником на права интеллектуальной собственности. Цепи поставки, как правило, охватывают множество участников, при этом контрактные соглашения между участниками могут быть сдерживающими факторами в доведении информации о фальсификациях до компетентных органов ввиду контрактных 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, управление данными 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 контрактных соглашений.

Приложение С
(рекомендуемое)

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 УИД группы объектов и УИД 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. Эти данные называют «мастер-данными».

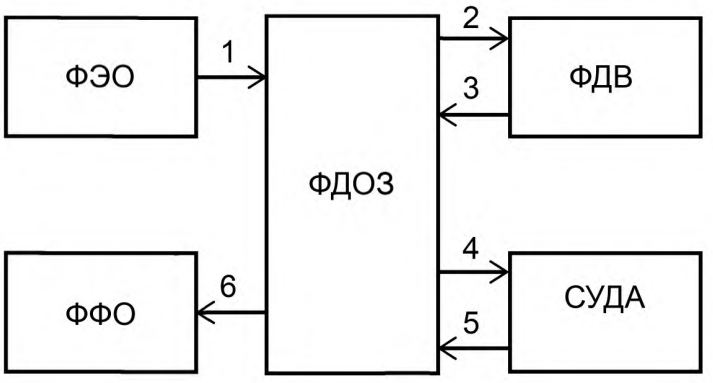
Информация для «УИД групп объектов», как правило, включает несколько уровней детализации атрибутов. Информация для УИД групп объектов может быть:

- описательной для всей группы объектов (мастер-данные — та же информация, что и для УИД всей группы), включает особенности продукции и упаковки;
- описательной для объектов части группы (серии) — т. е. обозначение части группы (серии), дата истечения годности, информация об отзыве части группы (серии);
- описательной для объектов партии, включает информацию об отгрузке, информацию о покупателях и продавцах партии объектов;
- описательной для отдельного предмета, включает серийный номер отдельной единицы продукции и/или его компонентов.

Многие факторы следует принимать во внимание при выборе способа обозначения на основе «УИД группы объектов» или «УИД экземпляра объекта». 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 для каждого из группы с УИД группы, но для УИД экземпляра объекта возможно наличие только одного объекта. 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 УИД группы объектов, пример без применения функции аутентификации

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



Пояснение

Типовой запрос требует выполнение 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 прямо в ФФО для представления инспектору.

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

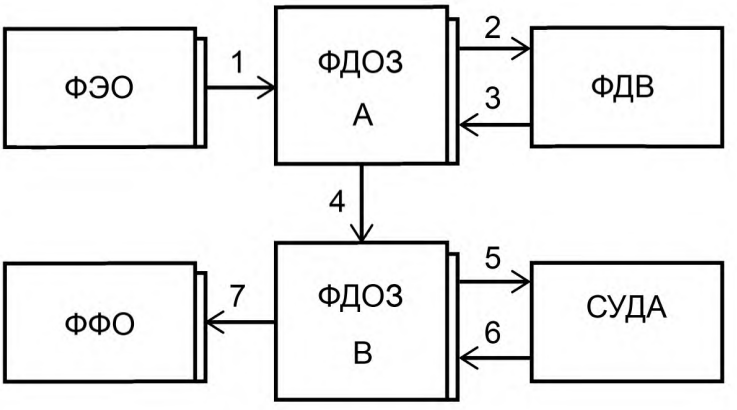
6 ФДОЗ направляет ответ в ФФО для представления инспектору.

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 Объект с УИД экземпляра, пример 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 могут иметь такие же или другие атрибуты. Возможна ситуация, когда только УИДы уникальны в группе объектов, а все объекты в классе имеют идентичные атрибуты и неразличимы с помощью УИД.



Пояснение

Типовой запрос требует выполнение 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.

Примечания

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

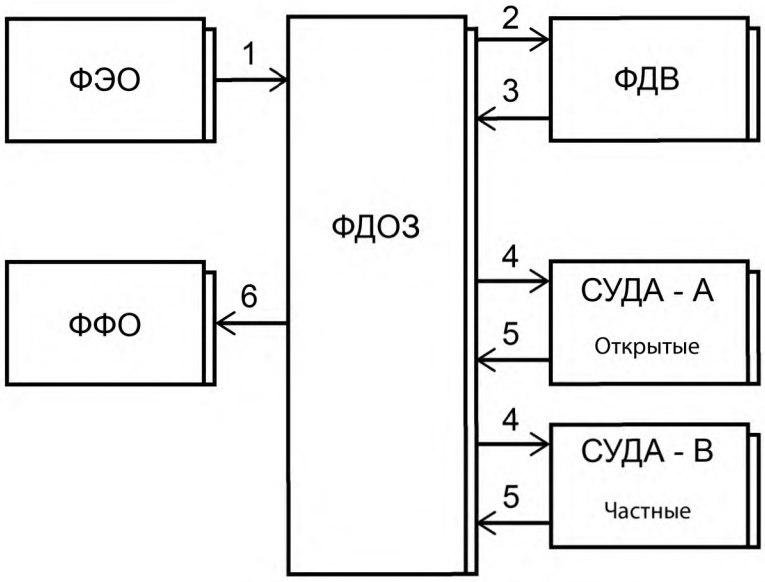
2 Фальсификаты определяют по фактам выявления слишком большого числа повторений конкретного УИД.

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 УИД 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.



Пояснение

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, -В; запросы, отклоненные ФДВ, направляются в обход СУДА напрямую в ФФО для представления инспектору.

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

6 ФДОЗ направляет ответ ФФО для представления инспектору.

Примечания

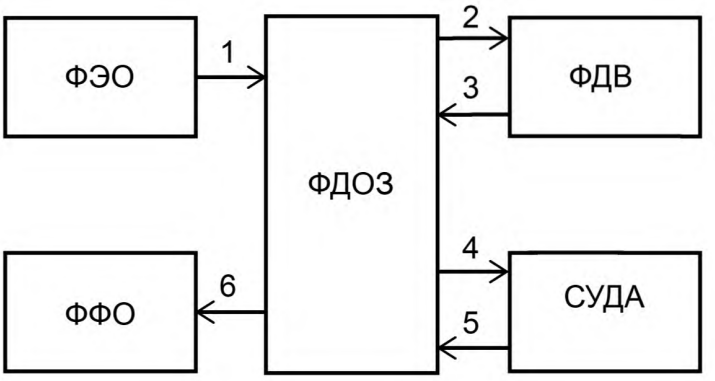
1 Фальсификаты определяют по фактам выявления несовпадения атрибутов, представленных инспектору, и находящихся на объекте.

2 Фальсификаты определяют при выполнении ФДВ верификации по элементу аутентификации.

Рисунок С.3 — Объект с УИД группы, пример с функцией аутентификации

С.6 Объект с УИД экземпляра, пример с функцией аутентификации

В настоящем примере используются УИД экземпляров, каждый объект имеет отличный от других УИД. Каждый УИД поставлен в соответствие атрибутам одного 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 с помощью УИД.



Пояснение

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.

Примечания

1 Фальсификаты определяют по несоответствиям присланных инспектору атрибутов атрибутам на объекте.

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

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.

4 Фальсификаты определяют при выполнении ФДВ верификации элемента аутентификации.

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

Библиография

[1] ISO 3166-1 — Codes for the representation of names of countries and their subdivisions — Part 1: Country codes (Коды для представления наименований стран и их регионов. Часть 1. Коды стран)[1)]

[2] ISO 3166-2 — Codes for the representation of names of countries and their subdivisions — Part 2: Country subdivision code (Коды для представления наименований стран и их регионов. Часть 1. Коды регионов стран)[2)]

[3] ISO 12931 — Performance criteria for authentication solutions used to combat counterfeiting of material goods (Критерии эффективности решений по аутентификации, применяемых для противодействия фальсификациям материальных товаров)

[4] ISO 16022 — Information technology — Automatic identification and data capture techniques — Data Matrix bar code symbology specification (Информационные технологии. Технологии автоматической идентификации и сбора данных. Спецификация символики штрихового кода Data Matrix)

[5] ISO/IEC 9594-8 — Information technology — Open Systems Interconnection — The Directory — Part 8: Public-key and attribute certificate frameworks (Информационные технологии. Взаимодействие открытых систем. Справочник. Структура сертификата на ключ общего пользования и атрибуты)[3)]

[6] ISO/IEC 15418 — Information technology — Automatic identification and data capture techniques — GS1 Application Identifiers and ASC MH10 Data Identifiers and maintenance (Информационные технологии. Технологии автоматической идентификации и сбора данных. Идентификаторы применения GS1 и идентификаторы данных ASC MH10 и их ведение)[4)]

[7] ISO/IEC 15459 (all parts) — Information technology — Unique identifiers (Информационные технологии. Уникальные идентификаторы. Все части)[5)]

[8] ITU-T Recommendation X. 509(03/00) — Information Technology — Open Systems Interconnection. The Directory: Public-key and attribute certificate frameworks (Информационные технологии. Взаимодействие открытых систем. Руководство. Структура сертификата на ключ общего пользования и атрибуты)

[9] ETSI/TS 101456 — Electronic Signatures and Infrastructures (ESI); Policy requirement for certification authorities issuing qualified certificates (Электронные подписи и инфраструктура. Требования политики к организациям по сертификации, выпускающим квалифицированные сертификаты)

[10] ETSI/TS 102042 — Electronic Signatures and Infrastructures (ESI); Policy requirement for certification authorities issuing public key certificates (Электронные подписи и инфраструктура. Требования политики к органам по сертификации, выпускающим сертификаты ключей общего пользования)

[11] ANSI MH 10.8.2 — Data Identifier and Application Identifier Standard (Стандарт на идентификаторы данных и идентификаторы применения)

[12] SEMI G83-0301 — Specification for Bar Code Marking of Product Packages (Спецификация на маркировку штриховыми кодами упаковки продукции)

[13] SEMI T15-0705 — General Specification of Jig ID: Concept (Общая спецификация идентификаторов сборочных приспособлений: Концепция)

[14] SEMI T19-0311 — Specification for Device Marking (Спецификация на маркирование изделий)

[15] SEMI T20-0710 — Specification for Authentication of Semiconductors and Related Products (Спецификация на аутентификацию полупроводниковых устройств и относящихся к ним изделий)

[1)] В Российской Федерации действует ГОСТ 7.67—2003 (ИСО 3166-1:1997).

[2)] В Российской Федерации действует ОК 019—95 «Общероссийский классификатор объектов административно-территориального деления (ОКАТО)».

[3)] В Российской Федерации действует ГОСТ Р ИСО/МЭК 9594-8—98.

[4)] В Российской Федерации действует ГОСТ ISO/IEC 15418—2014.

[5)] В Российской Федерации действуют ГОСТ ИСО/МЭК 15459-1—2008, ГОСТ ИСО/МЭК 15459-2—2008, ГОСТ Р ИСО/МЭК 15459-3—2007, ГОСТ Р ИСО/МЭК 15459-4—2007, ГОСТ Р ИСО/МЭК 15459-5—2008, ГОСТ Р ИСО/МЭК 15459-6—2009.

[16] SEMI T20.1-1109 — Specification for Object Labelling to Authenticate Semiconductors and Related Products in an Open Market (Спецификация на маркировку объектов для аутентификации полупроводниковых устройств и относящихся к ним изделий на открытом рынке)

[17] SEMI T20.2-1109 — Guide for Qualifications of Authentication Service Bodies for Detecting and Preventing Counterfeiting of Semiconductors and Related Products (Руководство по подготовке органов, оказывающих услуги по аутентификации, для выявления и предотвращения оборота фальсифицированных полупроводниковых устройств и относящихся к ним изделий)

[18] SEMI T20.3-0710 — Specification for Service Communication for Authentication of Semiconductors and Related Products (Спецификация на служебную связь при аутентификации полупроводниковых устройств и относящихся к ним изделий)

[19] SEMI T21-0212 — Specification for Organization Identification by Digital Certificate Issued from Certificate Service Body (CSB) for Anti-Counterfeiting Traceability in Components Supply Chain (Спецификация на идентификацию организаций с использованием цифрового сертификата, выпущенного органом по оказанию услуг сертификации для противофальсификатной прослеживаемости в цепях снабжения компонентов)

[20] SEMI T22-0212 — Specification for Traceability by Self Authentication Service Body and Authentication Service Body (Спецификация на обеспечение прослеживаемости органом по оказанию услуг самоаутентификации и органом по оказанию услуг аутентификации)

[21] Web Trust for CA — CA criteria designated from many browsers (Критерии органа по сертификации, установленные с учетом использования множества браузеров)

[22] NIST Special Publication 800-63-1 — Electronic Authentication Guideline (Руководство по электронной аутентификации)

УДК 347.822.4:006.354 ОКС 01.040.01, 13.310

Ключевые слова: аутентификация, идентификация, инспектор, контрафакт, оценка риска, прослеживаемость в цепи поставок, риск, фальсифицированные изделия

БЗ 6—2017/54

Редактор *Л.В. Коретникова*
Технический редактор *И.Е. Черепкова*
Корректор *М.И. Першина*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 10.11.2017. Подписано в печать 22.11.2017. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 3,72. Уч.-изд. л. 3,34. Тираж 22 экз. Зак. 2375.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123001 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru