ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 58637— 2019 (ИСО 12931:2012)

Система защиты от фальсификаций и контрафакта

КРИТЕРИИ ЭФФЕКТИВНОСТИ РЕШЕНИЙ ПО АУТЕНТИФИКАЦИИ, ПРИМЕНЯЕМЫХ ДЛЯ БОРЬБЫ С КОНТРАФАКТНОЙ ПРОДУКЦИЕЙ

**(ISO 12931:2012,
Performance criteria for authentication
solutions used to combat counterfeiting of material goods,
MOD)**

Издание официальное

**Москва
Стандартинформ
2020**

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Международной ассоциацией организаций, осуществляющих деятельность по противодействию незаконному обороту контрафактной продукции, «Антиконтрафакт» и Федеральным государственным унитарным предприятием «Государственный научно-исследовательский институт авиационных систем»

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 29 ноября 2019 г. № 1286-ст

4 Настоящий стандарт является модифицированным по отношению к международному стандарту ИСО 12931:2012 «Критерии эффективности средств аутентификации материальных товаров для борьбы с подделками» («ISO 12931:2012 Performance criteria for authentication solutions used to combat counterfeiting of material goods», MOD). При этом дополнительные слова, фразы, включенные в стандарт для учета потребностей национальной экономики Российской Федерации и особенностей российской национальной стандартизации, выделены полужирным курсивом или рамкой из тонких линий. Ссылочные стандарты ISO 31000, ISO/IEC 15408-1, ISO/IEC 27002 заменены на идентичные национальные стандарты Российской Федерации.

Наименование настоящего стандарта изменено относительно наименования ISO 12931:2012 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.

Сведения о соответствии ссылочных национальных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте, приведены в дополнительном приложении ДА

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, уведомления 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

ISO, 2012 — Все права сохраняются
© Стандартинформ, оформление, 2020

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

Содержание

1 Область применения 1
2 Нормативные ссылки 2
3 Термины и определения 2
4 Общие положения 4
5 Установление критериев эффективности на основе анализа риска 8
6 Оценка эффективности средства аутентификации 16
Приложение А (рекомендуемое) Таблица данных для оценки средств аутентификации 19
Приложение В (рекомендуемое) Таблица средств контроля доступа 27
Приложение ДА (справочное) Сведения о соответствии ссылочных национальных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте 28
Библиография 29

Введение

За последние десять лет в мировой торговле существенно выросли объемы и ассортимент фальсифицированной и контрафактной продукции, и в настоящее время такая продукция не ограничивается предметами роскоши. Продажа фальсифицированной и контрафактной продукции преобладает в большинстве развивающихся стран и становится массовой в развитых странах. Многие изготовители и правообладатели сталкиваются с ростом числа подделок и других противоправных действий в отношении своей продукции. Эту проблему усугубляет использование сети Интернет для продвижения товаров. Фальсифицированная и контрафактная продукция, как правило, предлагается без надлежащих гарантий в отношении безопасности, соответствия требованиям по охране окружающей среды и требованиям нормативных документов, что создает риски для потребителей и дистрибьюторских сетей. Оборот данной продукции приводит к потере прибыли изготовителей и правообладателей законной продукции, потерям у них рабочих мест, наносит ущерб стоимости торговой марки (бренда) изготовителей и правообладателей, в отношении продукции которых осуществлены противоправные действия, а также приводит к потерям налоговых поступлений для государства. Оборот фальсифицированной и контрафактной продукции сопровождается претензиями и судебными исками потребителей к изготовителям законной продукции и дистрибьюторской сети. Изготовление и сбыт фальсифицированной и контрафактной продукции стали одним из основных видов деятельности организованной преступности на внутренних рынках, в международной торговле и контрабандных перевозках.

Чтобы защитить свой бизнес, компании все шире используют средства аутентификации, приспособленные к их собственным потребностям. Важно установить требования к эффективности средств аутентификации, предназначенных для противодействия обороту фальсифицированной и контрафактной продукции на национальном и международном уровнях. Это приведет к повышению доверия со стороны потребителей, поддержит безопасность цепи поставок и поможет уполномоченным органам в разработке и проведении превентивных, сдерживающих и карательных мер.

Противоправные действия, связанные с оборотом фальсифицированной и контрафактной промышленной продукции, могут включать следующие действия (но не ограничиваются указанным перечнем):

- обман (намеренное введение в заблуждение) конечного потребителя продукции;
- обман (намеренное введение в заблуждение) изготовителей конечной продукции, которые являются покупателями составных частей, материалов или запасных частей;
- нарушение прав интеллектуальной собственности законных правообладателей;
- нарушение национальных, региональных или международных законов.

Изготовление контрафактной продукции может включать неправомерное использование:

- прав интеллектуальной собственности (см. [1]);
- секретов производства;
- решений внешнего вида продукции законных изготовителей.

Примечания

1 К неправомерному использованию прав интеллектуальной собственности при изготовлении продукции отнесены: изготовление продукции с нарушением законодательства об авторском праве либо с нарушением существенных условий договора о передаче исключительных прав, либо применение наряду с правомерно используемыми объектами авторского права неправомерно используемых, содержащих изобретения, полезные модели, промышленные образцы, топологии интегральных микросхем, находящихся в обороте с нарушением прав и законных интересов правообладателя, требований патентного законодательства, либо существенных условий лицензионного договора.

2 К неправомерному использованию секретов производства отнесены: получение в результате неправомерного завладения, разглашения секретов производства (ноу-хау), и использование их с нарушением прав и законных интересов правообладателя, требований законодательства о коммерческой тайне.

3 К неправомерному использованию решения внешнего вида продукции отнесены: использование решения (существенных признаков) внешнего вида изделия промышленного или кустарно-ремесленного производства, зарегистрированного в качестве промышленного образца. К существенным признакам промышленного образца относятся признаки, определяющие эстетические особенности внешнего вида изделия, в частности форма, конфигурация, орнамент, сочетание цветов, линий, контуры изделия, текстура или фактура материала изделия. Признаки, обусловленные исключительно технической функцией изделия, не являются охраняемыми.

К фальсифицированной продукции не следует относить продукцию, изготовление и введение в оборот которой осуществлено с нарушениями требований к качеству продукции, однако эти действия не связаны с намерением ввести в заблуждение потребителя.

К контрафактной продукции не следует относить продукцию, существенные признаки которой схожи с существенными признаками продукции иных изготовителей, однако при этом данные признаки не зарегистрированы в установленном порядке как охраняемые результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации.

Проблема противодействия обороту фальсифицированной и контрафактной продукции усугубляется следующими факторами:

- рынки становятся все более глобальными, а промышленная продукция все более сложной;
- объемы и интенсивность перемещения продукции в мире увеличиваются, и могут возникать и использоваться нетрадиционные каналы продвижения товаров.

Ввиду этого для инспектора задача распознавания признаков подлинности промышленной продукции становится в общем случае все более сложной.

Следует учитывать, что изготовители фальсифицированной и контрафактной продукции стремятся обойти нормы законодательства, включая требования о предоставлении гарантий соответствия и качества, предназначенные для обеспечения выпуска безопасных промышленных товаров на рынок и защиты конкуренции[1)]. Покупатели продукции не всегда имеют возможность и желание должным образом изучить предлагаемые товары, в частности из-за отсутствия необходимых знаний, времени, привлекательной низкой стоимости товара. Наличие методов аутентификации обеспечивает конкретный и более надежный метод определения подлинности товара или выявления фальсификации.

Установление подлинности промышленной продукции, то есть признание ее подлинной или фальсифицированной, заключается в сверке существенных характеристик заведомо подлинного и исследуемого товара. Первым шагом такой проверки должно быть установление инспектором характеристик происхождения товара, а затем получение подтверждения соответствия исследуемого товара данным характеристикам.

При наличии каких-либо сомнений в отношении подлинности товара задача инспектора должна заключаться в получении дополнительных данных о совпадении или расхождении характеристик заведомо подлинного и исследуемого товара на основе данных о прослеживаемости в цепи поставок, применения элементов и методов аутентификации, проведения разрушающих и неразрушающих испытаний, технического анализа или сочетания этих средств.

Настоящий стандарт разработан для определения цели и области применения средств аутентификации продукции в промышленности, торговле и в сфере услуг. Стандарт устанавливает также критерии эффективности специально разработанных средств аутентификации (подтверждения подлинности). Данные средства предназначены для обеспечения надежного доказательства подлинности или фальсифицированности, или контрафактности промышленной продукции, которая обращается как товар в цепи поставок.

Цель настоящего стандарта заключается в интеграции требований к эффективности средств аутентификации в жизненный цикл материальных товаров в любой ситуации, когда это требуется. Аутентификация, таким образом, позиционируется как особая характеристика жизненного цикла материального товара или услуги, не допускающая фальсификации.

Настоящий стандарт предложен как часть более широкой концепции, изложенной в соответствующих стандартах в области борьбы с подделками, где доказательство того, что товар является подлинным или фальсифицированным, может быть получено любым способом; в то же время стандарт не предназначался и не разрабатывался для определения единственного средства аутентификации.

[1)] Защита конкуренции в соответствии с Федеральным законом от 26 июля 2006 г. № 135-ФЗ «О защите конкуренции».

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система защиты от фальсификаций и контрафакта

КРИТЕРИИ ЭФФЕКТИВНОСТИ РЕШЕНИЙ ПО АУТЕНТИФИКАЦИИ, ПРИМЕНЯЕМЫХ ДЛЯ БОРЬБЫ С КОНТРАФАКТНОЙ ПРОДУКЦИЕЙ

The system of protection against fraud and counterfeiting.
Performance criteria for authentication solutions used to combat counterfeiting of material goods

Дата введения — 2020—03—01

1 Область применения

Настоящий стандарт устанавливает критерии эффективности и методологию оценивания средств, используемых для установления подлинности продукции[1)] в процессе ее жизненного цикла. При этом способы достижения критериев эффективности этими техническими средствами не устанавливаются.

Стандарт предназначен для использования всеми типами организаций, которым требуется подтверждение подлинности продукции (товара), и содержит требования и рекомендации по выбору элементов аутентификации, необходимых для борьбы с рисками появления фальсифицированной и контрафактной продукции, а также для анализа и определения критериев выбора элементов аутентификации по результатам анализа рисков появления фальсификаций и контрафакта. Элементы аутентификации могут быть частью самого товара и/или его упаковки. Критерии применяются к товару и/или его упаковке.

Критерии эффективности должны рассматриваться организациями с учетом особенностей конкретных ситуаций. Положения данного стандарта направлены в том числе на установление подлинности товаров, на которые распространяются права интеллектуальной собственности, подпадающих под действие национальных или региональных правовых актов, имеющих значение для безопасности и охраны здоровья, обладающих тем или иным четким отличием от иных товаров.

Настоящий стандарт не применим к товарам, используемым, например, в финансовом секторе, к официальным административным документам, документам, удостоверяющим личность, или к программной продукции для вычислительной техники.

Настоящий стандарт не применяется к технологиям или системам, предназначенным для прослеживания и локализации продукции. Прослеживание и локализация сами по себе не являются средством аутентификации и поэтому не входят в область применения данного стандарта[2)].

[1)] ***В настоящем стандарте под термином «продукция» понимается промышленная продукция, к которой относятся материальные объекты промышленного производства, предназначенные для применения в сферах производства, эксплуатации или потребления. Объекты промышленного производства могут являться изделиями, материалами, веществами и другими материальными объектами, которые до производства подлежат разработке в соответствии с требованиями к ним. Также к объектам промышленного производства принадлежат природные ресурсы и сельскохозяйственная продукция, которые не являются объектами разработки до производства, однако при введении в оборот в качестве товара подлежат контролю на соответствие установленным требованиям к продукции и идентификации как товарные и логистические единицы.***

[2)] ***Требования к прослеживаемости продукции — в соответствии с ГОСТ Р 58636—2019 «Система защиты от фальсификаций и контрафакта. Прослеживаемость оборота продукции. Общие требования»***.

Издание официальное

Настоящий стандарт не определяет экономические критерии, целью которых является установление соотношения между эффективностью и стоимостью средств аутентификации.

Некоторые отрасли промышленности и сферы услуг могут иметь специальные требования, дополнительные к требованиям данного стандарта.

Организация должна определить уровень обеспечения безопасности от фальсификаций и контрафакта, необходимый для выбранного средства аутентификации. Поставщик средства аутентификации должен действовать в соответствии с рисками и требованиями безопасности организации.

Стандарт не содержит положений, ограничивающих для организаций выбор технологий аутентификации.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 57881 Система защиты от фальсификаций и контрафакта. Термины и определения

ГОСТ Р ИСО 9000 Системы менеджмента качества. Основные положения и словарь

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с указанием всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины ***по ГОСТ Р ИСО 9000, ГОСТ Р 57881***, а также следующие термины с соответствующими определениями:

3.1 **агрессивное воздействие** (attack)**:** Успешная или безуспешная попытка(и) обойти средство аутентификации, включая попытки имитации, создания или воссоздания элементов аутентификации.

3.1.1 **внутреннее агрессивное воздействие** (internal attack)**:** Воздействие, совершаемое физическими или юридическими лицами, прямо или косвенно связанными с законным изготовителем, разработчиком продукции или правообладателем (персонал правообладателя, подрядчика, поставщика и т. д.).

3.1.2 **внешнее агрессивное воздействие** (external attack)**:** Воздействие, совершаемое физическими или юридическими лицами, прямо или косвенно не связанными с законным изготовителем, разработчиком продукции или правообладателем.

3.2 **подлинная материальная продукция** (authentic material good[1])**:** Материальная продукция, произведенная под контролем законного изготовителя, разработчика продукции или правообладателя интеллектуальной собственности на продукцию.

3.3 **установление подлинности, аутентификация** (authentication)**:** Действие по установлению подлинности или поддельности материальной продукции.

3.3.1 **элемент аутентификации** (authentication element)**:** Осязаемый объект, визуальный признак или информация, связанные с материальной продукцией или ее упаковкой, которые используются как часть средства аутентификации.

3.3.1.1 **открытый элемент аутентификации** (overt authentication element)**:** Элемент аутентификации, который можно обнаружить и проверить с помощью одного из органов чувств человека без привлечения вспомогательных средств (исключая обычные средства коррекции несовершенного восприятия, такие как очки или слуховые аппараты).

---

[1] ***Соответствует оригиналу стандарта ИСО, относится к единице продукции.***

3.3.1.2 **скрытый элемент аутентификации** (covert authentication element): Элемент аутентификации, который скрыт от органов чувств человека до тех пор, пока использование инструмента подготовленным человеком не откроет его этим органам чувств или иным образом не позволит автоматически интерпретировать этот элемент.

3.3.2 **инструмент аутентификации** (authentication tool): Комплект системы аппаратного и/или программного обеспечения, который является частью средства борьбы с подделками и используется для восприятия и обработки элемента аутентификации.

3.3.2.1 **автономный инструмент аутентификации** (stand-alone authentication tool): Инструмент аутентификации, который используется для обнаружения органами чувств человека скрытого элемента аутентификации с целью его проверки человеком либо включает функции, необходимые для независимой проверки элемента аутентификации.

3.3.2.2 **интерактивный инструмент аутентификации** (on-line authentication tool): Инструмент аутентификации, который для обеспечения локальной интерпретации элемента аутентификации требует подсоединения к компьютерной сети в режиме реального времени.

3.3.2.3 **серийный инструмент аутентификации** (off-the-shelf authentication tool): Инструмент аутентификации, который можно приобрести в открытой продаже.

3.3.2.4 **специализированный инструмент аутентификации** (purpose-built authentication tool): Инструмент аутентификации, сделанный специально для конкретного средства аутентификации.

3.3.3 средство аутентификации (authentication solution): Полный набор средств, способов и процедур, который позволяет установить подлинность материального товара.

3.4 **автоматическая интерпретация** (automated interpretation): Подлинность, оцениваемая автоматически с помощью одного или нескольких компонентов средства аутентификации.

3.5 **фальсифицировать** (counterfeit): Несанкционированно имитировать, воспроизводить или модифицировать материальную продукцию или ее упаковку.

3.6 **фальсифицированная продукция** (counterfeit good[1)]): Материальная продукция, имитирующая или копирующая подлинную материальную продукцию.

3.7 **доля ошибочной приемки** (false accept an cerate): Доля аутентификаций, при которых поддельная материальная продукция ошибочно объявлена подлинной.

3.8 **доля ошибочной браковки** (false rejection rate): Доля аутентификаций, при которых подлинный материальный товар ошибочно объявлен поддельным.

3.9 **специальный лабораторный анализ, в том числе судебный криминалистический анализ** (forensic analysis): Научная методология установления подлинности материальной продукции посредством подтверждения элемента аутентификации или присущего признака с помощью специализированного оборудования опытным специалистом, обладающим специальными знаниями.

Примечание — Объектами судебного криминалистического анализа могут быть поддельные документы, связанные с продукцией, а также уничтоженные полностью или частично, измененные маркировочные обозначения продукции, другие объекты.

3.10 **интерпретация, выполненная человеком** (human interpretation): Подлинность, оцененная человеком.

3.11 **инспектор** (inspector): Любой специалист, использующий средство аутентификации с целью аутентификации материального товара.

3.12 **интегрированный элемент аутентификации** (integrated authentication element): Элемент аутентификации, добавленный к материальной продукции.

3.13 **целостность** (integrity): Свойство ненарушенного состояния элемента аутентификации, связанных с ним данных, элементов и методов их обработки.

3.14 **операционная совместимость** (интероперабельность) (interoperability): Степень, в которой средство аутентификации способно работать вместе с другими различными средствами.

3.15 **присущий элемент аутентификации** (intrinsic authentication element): Элемент аутентификации, свойственный (приданный разработчиком и/или изготовителем) данному материальному товару.

3.16 **вероятность** (likelihood): Шанс на то, что какое-либо событие произойдет.

Примечания

1 В терминологии менеджмента риска слово «вероятность» используется для обозначения шанса на то, что произойдет некое событие, установленное, измеренное или определенное объективно или субъективно, ка-

[1)] ***Соответствует оригиналу стандарта ИСО, относится к единице продукции.***

чественно или количественно, и описанное с использованием общих терминов или математически (например, как вероятность или частота появления за данный период времени).

2 Английский термин «likelihood» не имеет прямого соответствия в некоторых языках; вместо него часто используется эквивалент термина «probability» (вероятность). Однако «probability» часто переводится с английского языка только как математический термин. Поэтому в терминологии менеджмента риска,«likelihood» используется в смысле, имеющем более широкую интерпретацию, как термин «probability» во многих других языках, кроме английского.

[ISO Guide 73:2009, пункт 3.6.1.1]

3.17 **материальная продукция** (material good[1]): Произведенная, выращенная продукция или продукция, обеспечиваемая природой.

3.18 **жизненный цикл материальной продукции** (material good lifecycle): Совокупность этапов существования продукции, включая разработку концепции, проектирование, производство, хранение, обслуживание, продажу, применение и утилизацию.

3.19 **правообладатель** (rights holder): Физическое или юридическое лицо, обладающее одним или несколькими правами на интеллектуальную собственность, либо имеющее разрешение на использование одного или нескольких таких прав.

3.20 **анализ риска** (risk analysis): Процесс осмысления природы риска и определения степени риска.

Примечания

1 Анализ риска обеспечивает основу для оценивания риска и принятия решений в отношении риска.

2 Анализ риска включает его оценку.

[ISO Guide 73:2009, пункт 3.6.1]

3.21 **устойчивость** (robustness): Способность системы противостоять виртуальным или физическим, внутренним или внешним агрессивным воздействиям.

Примечание — В данном стандарте это способность противостоять попыткам имитации, копирования, вмешательства или обхода.

3.22 **безопасность** (security): Состояние свободы от опасности или угроз там, где соблюдаются процедуры или приняты соответствующие меры.

3.23 **секрет** (secret): Данные и/или знания, которые защищены от несанкционированного раскрытия.

3.24 **разработчик требований** (specifier): Физическое или юридическое лицо, определяющее требования к средству аутентификации, которое должно применяться к конкретной материальной продукции.

3.25 **очевидность подделки** (фальсификации) (tamper evidence): Способность элемента аутентификации показывать, что данный материальный товар вызывает подозрение в его подделке (фальсификации).

3.26 **прослеживание и локализация** (track and trace): Возможность для участников оборота продукции устанавливать, где продукция находилась ранее и в каком состоянии (прослеживание) и где она находится в данный момент (локализация) в цепочке поставок, реализуемая с применением средств идентификации каждой отдельной единицы материальной продукции, серии или партии продукции.

4 Общие положения

4.1 Выбор средств аутентификации

4.1.1 Средства аутентификации могут применяться в различных формах, от простых, в виде знаков и графических изображений, до сложных, включающих в себя элементы информационных технологий. Простое средство может являться более эффективным и предпочтительным в конкретных

---

[1] ***Соответствует оригиналу стандарта ИСО, относится к единице продукции.***

условиях применения, и выбор подходящего средства аутентификации продукции должен зависеть от обстоятельств его внедрения и использования.

4.1.2 Технические, логистические и финансовые критерии, применяемые при выборе средства аутентификации, должны определяться с учетом следующих факторов:

- характеристик элемента(ов) аутентификации;
- уровней, целей и методов проверок;
- требуемых информационных систем;
- требований к безопасности;
- стойкости к фальсификации;
- ценности продукции, подлежащей защите;
- рисков появления фальсификации и контрафакта на протяжении жизненного цикла продукции;
- требований к интегрированию и реализации средств аутентификации;
- роли упаковки в обороте продукции.

4.1.3 Средства аутентификации не должны влиять на функциональность и целостность продукции.

Надлежащее применение данного стандарта опирается на соблюдение национальных, региональных и международных законов и регламентов, особенно касающихся конфиденциальности и безопасности.

4.1.4 Применение процессов проверки элементов аутентификации требует способности к считыванию данных, восприятию специальных признаков и, в некоторых случаях, восприятию с помощью органов чувств человека или с помощью инструментов. Такие инструменты контроля либо сразу должны обеспечивать получение заключения на месте, либо должны иметь возможность обращаться в реальном времени в защищенную информационную систему, или должны перенаправлять данные, образец или собственно материальный товар в структуру, проводящую анализ силами специалистов в автономном режиме.

4.1.5 Средство аутентификации должно формироваться в процессе создания как элемент продукции с последующим проведением проверки аутентификации. Процесс создания средства должен состоять из определения, формирования и производства элементов аутентификации и их интеграции с продукцией (товаром) или его упаковкой. Процесс проверки должен заключаться в контроле работоспособности и эффективности элементов аутентификации в цепочке поставок подготовленными специалистами с помощью органов чувств, инструментов или справочных данных. Эти два процесса связаны в последовательности действий цикла «Планирование — Исполнение — Проверка — Действие» [Plan-Do-Check-Act (PDCA)], а привлеченные исполнители составляют существенную часть средства аутентификации.

Уровень пригодности средства аутентификации должен оцениваться в целом, включая все применимые компоненты и интерфейсы.

4.1.6 При анализе стратегии защиты правообладатели должны рассматривать следующие основные вопросы:

- какими могут быть фальсификации, последствия и вероятность угрозы фальсификации;
- какой из видов продукции подделывают или могут подделать;
- где может проводиться выпуск фальсификаций и контрафакта и как они могут распространяться;
- в каком окружении и каких условиях находятся законное производство и законные цепи поставок;
- как и кем должен выполняться процесс аутентификации;
- каково влияние ошибки человека на средство аутентификации.

4.2 Процесс аутентификации

4.2.1 На рисунке 1 приведена схема применения типового средства аутентификации, которая раскрывает взаимосвязь между продукцией (товаром), подлежащим аутентификации, и типовыми компонентами средства аутентификации.

4.2.2 Совместное применение элементов и методов аутентификации должно позволять получить заключение об аутентичности (правдивое или ложное) либо предоставить информацию, которая при дальнейшей обработке и с привлечением новых данных позволит выявить подлинность товара.

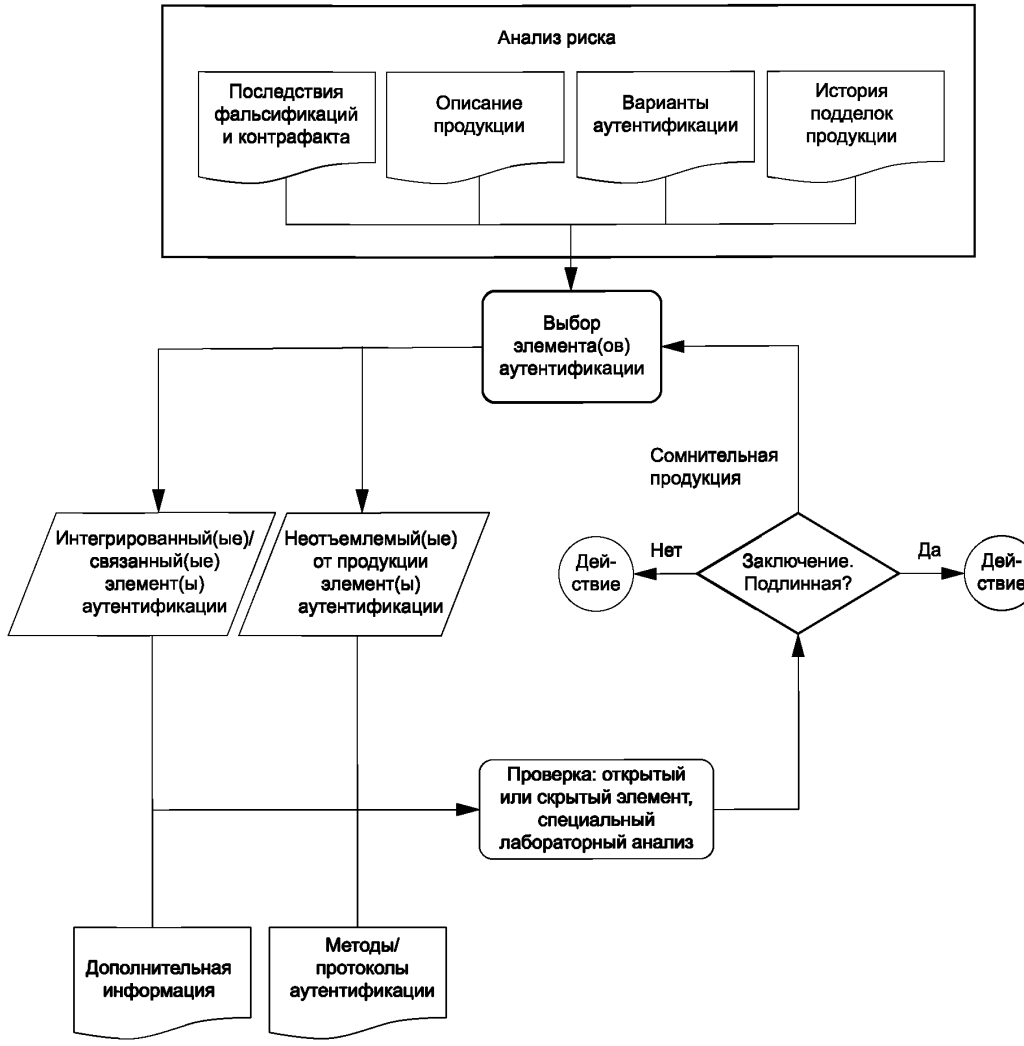

Рисунок 1 — Функциональная схема типового средства аутентификации

4.3 Категории средств аутентификации

4.3.1 Различают категории средств аутентификации по следующим признакам: по объему знаний, по аудитории, по методам контроля, по режиму работы инструментов контроля, по доступности приобретения, по принадлежности к открытым и закрытым элементам.

4.3.2 Категория по объему знаний, которыми должен располагать инспектор. Следует учитывать, что применение средства аутентификации требует от инспектора некоторого объема знаний. Без информации о том, что данное средство аутентификации применено к рассматриваемому товару, инспектор не может контролировать связанный с этим средством элемент аутентификации. Без знания соответствующей процедуры контроля он не может надлежащим образом установить подлинность товара. Требуемый объем знаний может быть подразделен на общие знания (например, как знания о классе элементов аутентификации) и знание, касающееся конкретного товара (например, какой конкретный элемент аутентификации, примененный к данному товару, подлежит контролю). В то же

время правообладатель может держать под контролем предполагаемую целевую аудиторию, обладающую такими знаниями, в частности знаниями о конкретном товаре.

4.3.3 Категория по аудитории, в которой распространяются знания. Знания о применяемом средстве аутентификации могут принадлежать общей аудитории, в этом случае они свободно распространяются в обществе, например через рекламу, сайты или маркетинговые материалы.

Доступ к знаниям о применяемом средстве аутентификации может быть организован только для некоторой группы людей, которым они необходимы и которые в силу своей профессии должны осуществлять контроль товара. Таким образом, они исключаются из общей аудитории. Такой подход ограничен потенциальным риском, что знания через целевую аудиторию могут в конечном итоге стать достоянием широкой аудитории; с другой стороны, безопасность средства аутентификации может заметно увеличиться посредством ограничения доступности знаний о нем.

4.3.4 Категория по методам контроля. Процесс контроля элемента аутентификации должен включать некоторую форму физического наблюдения или измерения. В этом отношении для разделения на категории используется следующее различие — применение органов чувств человека или инструментов идентификации. Инструмент аутентификации применяется для выполнения требуемого контроля и отображения результата некоторым надлежащим образом для представления инспектору. Используемый инструмент может быть инструментом, либо имеющимся на месте нахождения товара, либо требующим применения лабораторного оборудования или аналогичного окружения и передачи товара на исследование.

Основные категории средств аутентификации представлены в таблице 1.

Таблица 1 — Виды категорий средств аутентификации по признакам — аудитория, методы контроля

Признаки отнесения к категориям	Органы чувств человека	Инструмент аутентификации		Специальный лабораторный анализ
		Имеется в открытой продаже	Сделанный специально	
Общая аудитория	открытый	скрытый	—	—
Ограниченная аудитория	открытый	скрытый	скрытый	скрытый

Таблица видов средств аутентификации приведена в приложении В.

4.3.5 В случае, когда средство аутентификации предполагает использование инструмента аутентификации для контроля элемента аутентификации, применяемый технический инструмент может быть охарактеризован с помощью следующих категорий режима работы — автономный и онлайн. Инструмент аутентификации может работать и выполнять контроль элемента аутентификации полностью автономно (за исключением источника электропитания, если требуется). Для режима онлайн работа инструмента аутентификации требует подсоединения к компьютерной сети. Соединение может потребоваться, например, для отсылки или получения данных, необходимых для выполнения контроля, или для запроса авторизации на выполнение контроля элемента аутентификации.

4.3.6 В зависимости от того, каким образом можно приобрести инструмент аутентификации, можно различать две категории его доступности. Инструмент аутентификации может быть приобретен как обычный коммерческий продукт, поставляемый из одного и более источников как готовый инструмент, имеющийся в продаже. К другой категории относится специально спроектированный и изготовленный инструмент.

4.3.7 Элементы аутентификации могут делиться на категории по принадлежности к открытым элементам или закрытым элементам. Открытая аутентификация может выполняться напрямую информированным инспектором и не требует дополнительного оборудования, позволяющего подтвердить подлинность характеристики элемента аутентии-

фикации. Открытые элементы аутентификации выявляются с помощью органов чувств человека, наиболее часто используется зрение, но иногда также и осязание. Поэтому открытые элементы аутентификации, как правило, должны применяться там, где визуальная проверка является единственным методом, которым можно воспользоваться незамедлительно и который может быть выполнен информированными инспекторами, например, потребителями, работниками складов и проверяющими сотрудниками. Предпочтительно, чтобы у инспектора был подлинный элемент аутентификации для контрольного сравнения.

4.3.8 Открытые элементы аутентификации должны быть достаточно сложными для точного копирования. Отсутствие элемента аутентификации или наличие признаков фальсификации элементов являются основанием для заключения, что рассматриваемый товар не является подлинным.

4.3.9 Скрытые элементы аутентификации не предназначены для немедленного распознавания и интерпретации с помощью органов чувств человека. Они требуют инструментов аутентификации и/или специальных знаний для подтверждения их наличия и подлинности либо посредством преобразования их в вид, пригодный для восприятия органами чувств человека (обычно зрения), либо для непосредственного считывания (восприятия) инструментом аутентификации. Такие инструменты могут быть автономными или могут требовать присоединения к компьютерной сети, также они могут быть серийными или созданными единично специально для данной цели. Результат проверки, представленный инструментом аутентификации, может сразу непосредственно свидетельствовать о подлинности элемента аутентификации, или окончательное решение должно быть принято инспектором с привлечением его знаний или дополнительных данных. Инспекторам, анализирующим такие элементы аутентификации, требуется специальная подготовка.

4.3.10 Скрытые технологии могут использовать различные виды физических, химических или биологических явлений, а также логические взаимосвязи между явлениями, данными и продукцией. Элементы аутентификации, использующие данные в электронном виде, должны использовать установленные виды программного и/или аппаратного обеспечения и протоколы обмена данными с внешними ресурсами, однозначно связанными с подлинным товаром, для доказательства подлинности или поддельности исследуемого товара.

4.3.11 Скрытые средства аутентификации следует проектировать таким образом, чтобы аутентификацию можно было осуществлять в производственных и послепроизводственных условиях.

В случае, когда при скрытой аутентификации используются данные, которые связаны или могут быть связаны с изготовителем или правообладателем, должны соблюдаться принципы и законы, относящиеся к защите информации, частной собственности и исключительных прав. Следует учитывать, что по мере развития техники аудитория, которая имеет возможность установить наличие и подлинность скрытого элемента аутентификации, будет расширяться.

4.3.12 В сложных случаях и в случае нарушения законодательства для проведения аутентификации может быть использован специальный лабораторный анализ, в том числе судебный криминалистический анализ, который включает использование специальных знаний и специализированных научных методов для проверки элементов аутентификации или присущих признаков рассматриваемого материального товара. Специальный лабораторный анализ может быть выполнен в производственных условиях, в других условиях, где осуществляется оборот продукции (вне экспертной организации), или в условиях экспертной организации с применением обычных и специализированных средств обследования.

В процессе валидации средства аутентификации, если это возможно, следует использовать оригинальные экземпляры элементов аутентификации для сравнительного анализа.

5 Установление критериев эффективности на основе анализа риска

5.1 Критерии эффективности средства аутентификации должны использоваться разработчиком требований к средствам аутентификации для определения применяемых к продукции категорий средств аутентификации или их сочетания, которые будут удовлетво-

рять целям применения средств аутентификации и требованиям потребителей продукции, участников оборота продукции.

Также необходимо учесть, что общая эффективность средств аутентификации зависит от эффективности каждого элемента аутентификации, инструментов аутентификации и от эффективности связей между ними. Эффективность средств аутентификации (как совокупности средств, способов и процедур), в частности их стойкость к агрессивному воздействию, должна приниматься в расчет в той же степени, что и эффективность элементов аутентификации.

Следует обратить внимание на то, что риск определяется сочетанием вероятности наступления события и последствий неблагоприятного события. Оценка риска должна являться общим процессом идентификации риска, анализа риска и сравнительной оценки (оценивания) риска[1].

Следует также учитывать, что на эффективность любого элемента аутентификации могут влиять изменения в технологии. Со временем эти изменения могут сделать средство неэффективным, в том числе сделать легкодоступным воспроизведение технологии аутентификации для фальсификатора. В рамках оценки значений критериев эффективности средств аутентификации следует периодически проводить анализ уязвимости методов и технологии аутентификации, чтобы обеспечить их актуальность и защищенность в условиях технического прогресса.

5.2 Критерии эффективности средств аутентификации определяют в следующих областях:

- физические характеристики;
- сопротивление воздействиям;
- интеграция с продукцией, упаковкой, условиями оборота продукции;
- взаимодействие с инфраструктурой участников оборота продукции и окружающей средой;
- процессы внедрения и ***применения***.

Разработчик требований к средствам аутентификации может выбрать для использования средство аутентификации, которое объединяет несколько элементов аутентификации, работающих вместе для создания защиты. Такие элементы могут принадлежать к различным категориям (открытые, скрытые, с различными уровнями доступности аудитории к знаниям о них и пр.). При выборе критериев следует учитывать, что чем надежнее средство аутентификации и выше компетентность инспектора, тем достовернее результат процесса аутентификации.

Хотя категории критериев могут быть одинаковы для разных средств аутентификации, для самого процесса аутентификации следует применять различные методы. В подразделе ***5.3*** описаны критерии для элементов аутентификации; в ***5.4*** — критерии для инструментов аутентификации; в ***5.5*** — критерии для средств аутентификации.

В приложении А для разработчика требований представлена матрица для выбора критериев.

5.3 Критерии для выбора элементов аутентификации

5.3.1 Критерии эффективности, связанные с физическими характеристиками элементов аутентификации. Ключевым критерием является возможность считывания элементов аутентификации человеком или машиной. Необходимо учесть также дополнительные критерии, связанные с многочисленными факторами, включая физические характеристики товара, пользователя/инспектора, окружающие условия аутентификации и ее продолжительность. Все эти факторы могут влиять на физические характеристики элементов аутентификации и надежность их восприятия. В составе физических характеристик товаров и средств аутентификации различают статические и динамические характеристики.

5.3.1.1 К статическим характеристикам относят значения:

- геометрических размеров;
- массы.

Данные характеристики средств аутентификации должны учитываться с учетом свойств товара: доступное пространство, операционная совместимость, потенциальные помехи со стороны характерных особенностей товара или процесса его обработки (см. характеристики процесса интеграции, ***5.3.3***).

5.3.1.2 К динамическим характеристикам относят следующие показатели:

---

[1] ***Методы оценки риска — в соответствии с ГОСТ Р ИСО 31000—2019 «Менеджмент риска. Принципы и руководство» и ГОСТ Р 58771—2019 «Менеджмент риска. Технологии оценки риска» (см. также [4]).***

- гибкости;
- вязкости;
- износа;
- предела прочности при растяжении.

Физическим характеристикам элементов аутентификации не должен наноситься ущерб в процессе производства продукции, интеграции ее с элементом аутентификации, а также во время хранения, транспортирования продукции.

Элемент аутентификации должен выбираться таким образом, чтобы учесть все требования к процессам, задействованным при производстве и дальнейшей обработке продукции.

Если при реализации процесса производства изменяются или повреждаются элементы аутентификации, они становятся бесполезными и приведут к отбраковке товара при окончательном производственном контроле. Поэтому элемент аутентификации следует выбирать с учетом всех требований процессов производства товара.

5.3.1.3 Критерии, связанные с характеристиками стойкости к внешним воздействиям. При обработке, хранении или эксплуатации продукции с элементом аутентификации условия окружающей среды не должны влиять на его физические характеристики таким образом, чтобы это привело к нарушению функционирования элемента аутентификации в ходе его жизненного цикла. Следует учитывать следующие виды условий:

- умеренные условия окружающей среды (учитываются климатические воздействия, такие, как температура и влажность);
- суровые условия окружающей среды (разрушающие факторы, такие как химическое воздействие и радиация, с добавлением климатических воздействий);
- механические воздействия, типичные для рассматриваемого товара; и
- старение материалов и устройств, которое может вылиться в нарушение функционирования элемента аутентификации в процессе жизненного цикла товара.

Разработчик требований к средствам аутентификации должен определить условия использования элементов, инструментов и методов аутентификации на основе необходимого анализа риска. Кроме того, следует учитывать особенности жизненного цикла товара, которые могут оказывать значительное влияние на сохранение способности к аутентификации.

5.3.1.4 Критерии, связанные с характеристиками продукции и условий ее оборота, влияющими на здоровье и окружающую среду. Данные характеристики включают:

- электромагнитное излучение;
- радиоактивность;
- химический состав и запрет на некоторые вещества;
- миграцию веществ;
- способность к рециклингу отходов продукции, упаковки, средств аутентификации.

Потенциальное влияние элементов и инструментов аутентификации на здоровье и окружающую среду должно учитываться, особенно в свете национальных, региональных и международных регламентов.

5.3.1.5 При выборе средств аутентификации следует учитывать физические характеристики, связанные с отличительными особенностями их применения, которые включают:

- возможность визуального контроля;
- распознаваемость техническими средствами;
- очевидность подделки;
- уникальность отношения элементов аутентификации и единиц продукции (один-к-одному, один-ко-многим).

Отличительную особенность можно признать уникальной в двух вариантах: «один-для-одного» или «один-для-многих». Уникальный признак, который подтверждает подлинность отдельного предмета и является уникальным только для этого предмета, признается как вариант «один-для-одного». Уникальный признак, который применим к нескольким предметам, признается как вариант «один-для-многих».

5.3.2 Критерии, связанные со стойкостью к агрессивным воздействиям. Эти критерии эффективности связаны со стойкостью элементов аутентификации к агрессивным воздействиям. Данная стойкость элемента аутентификации определяется как степень, в которой элемент аутентификации способен выдерживать агрессивные воздействия, описанные в ***5.3.2.1—5.3.2.7.***

Элементы аутентификации следует проектировать таким образом, чтобы потребовались экстраординарные усилия для их точного копирования, а в случае попытки копирования такой элемент должен содержать очевидные признаки копирования, видимые в процессе аутентификации.

5.3.2.1 Критерии, связанные со стойкостью к «обратному проектированию» (путем разборки законно изготовленного образца, изучения, проектирования и воспроизведения незаконного аналога) и копированию. Когда это возможно, следует обеспечить устойчивость элемента к «обратному проектированию». Информация об изготовлении элемента должна быть защищена таким образом, чтобы было весьма маловероятным ее получение для успешного изготовления элемента аутентификации и использования этого элемента с незаконной продукцией.

Для избежания имитации и эмуляции[1)] средств защиты продукции при проектировании средств защиты следует обеспечить невозможность или крайне малую вероятность создания фальсифицированного элемента аутентификации, который мог бы быть принят инспектором или инструментом как подлинный.

5.3.2.2 Критерии, связанные с сопротивлением подделке и обеспечению очевидности подделки. Сопротивление подделке представляет собой способность элемента аутентификации противостоять удалению, изменению или замене элемента, размещенного на товаре или его упаковке.

При разработке элемента аутентификации следует выбирать между прямой и опосредованной формами взаимозависимости между элементом аутентификации и товаром. Элемент аутентификации находится в прямой физической взаимозависимости, если при попытке его отделения от товара он разрушается либо претерпевает видимое и узнаваемое изменение, также изменения происходят с товаром. Опосредованная взаимозависимость имеет место в случае, когда элемент аутентификации имеет логическую ассоциацию или связь с товаром, которые невозможно уничтожить или продублировать.

Для создания необходимого сопротивления подделке различные формы взаимозависимости должны обеспечивать при агрессивных воздействиях немедленное и необратимое изменение одного или нескольких характеристик элементов аутентификации и товаров. Любые определимые изменения этих характеристик, возникшие в результате попыток упомянутого воздействия, должны быть отражены в протоколе проверки подлинности продукции. Для снижения доли ошибочной приемки или браковки следует обеспечивать стабильность взаимозависимых характеристик и их устойчивость к изменениям в условиях окружающей среды в процессе жизненного цикла товара.

5.3.2.3 Критерии, связанные со стойкостью к изменению. Элемент аутентификации должен противостоять изменению его характеристик или изменению информации, содержащейся в элементе. В случае, когда на элемент оказывалось воздействие, направленное на его изменение, это должно быть очевидным инспектору.

5.3.2.4 Критерии, связанные со стойкостью к агрессивным воздействиям и устойчивостью к утечке информации по побочным каналам. Необходимо исключить возможность получения подлежащей защите информации или определения характеристик элемента аутентификации посредством анализа его физического поведения в разных обстоятельствах, связанных с окружающей средой.

5.3.2.5 Критерии, связанные с перехватом информационных сообщений. Необходимо исключить возможность получения сведений, которые используются при агрессивных воздействиях, посредством перехвата сообщений между элементом аутентификации и инструментом, используемым для считывания или проверки этого элемента. Средство аутентификации должно проектироваться таким образом, чтобы информационный обмен был надежно защищен и не происходила утечка чувствительной к агрессивным воздействиям информации.

5.3.2.6 Критерии, связанные с устареванием. Разработчик средства аутентификации должен выполнить соответствующее исследование для определения потенциального срока службы элемента аутентификации, степени его эффективности в течение срока службы, а также спрогнозировать наличие материалов, технологий для его изготовления и поддержки в будущем.

[1)] ***Под эмуляцией понимается применение комплекса программных, аппаратных средств или их сочетания для копирования (или эмулирования) функций системы противодействия обороту фальсификаций и контрафакта, в том числе функций средств аутентификации, на другой, отличной от первой, незаконно применяемой вычислительной системе таким образом, чтобы эмулированное поведение как можно ближе соответствовало поведению оригинальной системы противодействия обороту фальсификаций и контрафакта.***

5.3.2.7 Критерии, связанные с повторным использованием элемента аутентификации. Необходимо исключить возможность повторно использовать элемент аутентификации без надлежащего разрешения.

5.3.3 Критерии, связанные с процессом интеграции. Данные критерии эффективности связаны с процессом интеграции элементов аутентификации с товаром, подлежащим защите.

5.3.3.1 В процессе интеграции должен быть реализован должным образом апробированный и утвержденный процесс обеспечения безопасности оборота продукции и использованы средства контроля безопасности. Необходимо выполнять оценивание компонентов системы производства и цепи поставок, чтобы обеспечить соответствие всем принятым решениям в области политики и процедур обеспечения безопасности оборота продукции.

5.3.3.2 Общие требования к процессам производства продукции и элементов аутентификации включают следующие ниже положения:

1) Поставщик должен обеспечить стабильность технологии производства и поставку необходимого количества элементов аутентификации на период производства продукции, а изготовитель конечной продукции должен обеспечить стабильность технологии интеграции товара и упаковки с элементом аутентификации.

2) Средства аутентификации должны поддерживать совместимость с объектами и процессами, такими как:

- товары и упаковка;
- производство и ***испытания***;
- логистика и ***материально-техническое обеспечение производства***.

Элемент аутентификации должен быть совместим с товаром и его упаковкой. Необходимо оценить влияние элемента аутентификации на процессы производства и распределения.

При выборе технологий аутентификации необходимо учитывать необходимость большого количества считываний и их потенциальные конфликты при недостаточной надежности считывания.

3) Технические средства, применяемые в производстве, должны быть защищены таким образом, чтобы был исключен несанкционированный доступ к защищаемой информации, относящейся к безопасности (см. [2], [3], [5]). Все выявленные попытки получить несанкционированный доступ к информации, относящейся к безопасности, должны быть документированы, а донесения представлены в установленные инстанции для принятия мер.

4) Должен проводиться контроль соответствия процесса производства требованиям к интеграции элементов аутентификации и продукции. Необходимо выполнять независимые аудиты с целью убедить заинтересованных участников в том, что все требования к интегрированию соблюдаются и могут быть верифицированы.

5) Должно проводиться обучение всех вовлеченных участников производства, чтобы персонал был способен выполнить требования к интеграции элементов аутентификации и применению средств аутентификации.

5.4 Критерии стойкости к агрессивным воздействиям для выбора инструментов аутентификации

5.4.1 Стойкость инструмента аутентификации к агрессивным воздействиям определяется как степень, в которой инструмент аутентификации способен обеспечить свойства, описанные в ***5.4.2—5.4.11.***

5.4.2 Стойкость к раскрытию, имитации аналогов средств аутентификации и эмуляции функций системы противодействия обороту фальсифицированной и контрафактной продукции в части аутентификации продукции. Средства аутентификации должны противостоять воздействиям, которые могут использоваться для раскрытия секретной или подлежащей защите информации, что может способствовать созданию аналога элемента аутентификации.

Чтобы избежать имитации и эмуляции, должны быть исключены все возможности создания поддельного средства аутентификации, которое инспектор может принять за подлинное средство. Эту задачу следует выполнять путем исследований и испытаний элементов и инструментов аутентификации.

5.4.3 Инструменты аутентификации должны обладать необходимым уровнем устойчивости к внешним агрессивным воздействиям и содержать признаки, которые позволят установить факт попытки воздействия. Инструменты должны быть необходимым образом защищены и/или должны реагировать на любую физическую попытку изменения их правил функционирования, нацеленную на незаконное получение информации во время ее обработки или передачи. Любую обнаруженную попытку воздей-

ствия на инструменты аутентификации необходимо документировать и сообщить о ней в установленные инстанции для принятия мер.

5.4.4 Инструменты аутентификации должны обладать необходимым уровнем устойчивости к использованию их и содержащихся в них данных для незаконного доступа во внешние базы.

5.4.5 Инструменты аутентификации должны обладать необходимым уровнем стойкости к утечке подлежащих защите данных, которая может возникнуть в результате обработки характеристик побочных явлений работы средства аутентификации ***(электромагнитного, оптического излучения и пр.).*** Необходимо исключить всякую возможность получения подлежащих защите данных или характеристик инструмента аутентификации посредством анализа его физического поведения или взаимодействия с элементом аутентификации в любых обстоятельствах, связанных с окружающей средой.

5.4.6 Инструменты аутентификации должны обладать средствами защиты информации от перехвата или подмены при ее передаче. Инструмент аутентификации должен быть защищен от несанкционированного обмена информацией между элементом аутентификации и инструментом и между инструментом и удаленными компонентами средства аутентификации или их аналогами и средствами эмуляции.

Защита обмена информацией должна быть предусмотрена во время процесса аутентификации и во время любого обмена информацией, необходимого для загрузки и выгрузки информации, актуализации данных или аварийных ситуаций.

5.4.7 Инструменты аутентификации должны обеспечивать безопасность системы. Если для аутентификации используется справочная база данных, она должна быть защищена от всех вторжений. О попытках и об успешном вторжении необходимо производить записи и сообщать в установленные инстанции для принятия мер.

5.4.8 Любой доступ в базу данных для процесса аутентификации должен быть защищен аутентификацией инспектора или инспектора и инструмента.

5.4.9 Должны быть обеспечены резервирование и перезапись данных. Следует обеспечить создание резервных баз данных для защиты от успешных попыток агрессивного воздействия. Кроме того, следует также рассмотреть создание дублирующей системы (данные и резервные средства обслуживания), чтобы избежать перерыва в обслуживании.

5.4.10 Следует управлять устареванием инструментов аутентификации таким образом, чтобы включение новых инструментов в состав средства аутентификации было возможно при поддержании уровня безопасности средства аутентификации.

Устареванием вычислительного оборудования и средств аутентификации надлежит управлять таким образом, чтобы совместимость с предшествующими системами и уровень безопасности были гарантированы на период времени, устанавливаемый разработчиком и заказчиком системы защиты.

5.4.11 Стойкость к агрессивным воздействиям средства следует определять посредством оценивания его уязвимости и стойкости ко всем типам воздействия (угроз), идентифицированным выше и основанным на анализе риска для продукции[1)].

5.5 Критерии выбора средств аутентификации

5.5.1 Набор критериев выбора средств аутентификации должен быть связан с условиями, в которых выполняется процесс аутентификации.

5.5.2 Критерий, связанный с функционированием в окружающей среде. Данный критерий эффективности связан с функционированием средства аутентификации в производственных условиях.

5.5.2.1 Критерий, связанный с необходимыми ресурсами. Средство аутентификации может потребовать разнообразных ресурсов для своей работы. Следует учитывать:

- требуемые источники энергии;
- требуемые коммуникации;
- обеспечивающие ***технические*** средства.

5.5.2.2 Критерий, связанный с условиями окружающей среды. Следует учитывать условия окружающей среды, приведенные ниже:

- температура (жарко, умеренно, холодно);
- влажность (сухо, влажно, мокро);
- загрязнения (чисто, пыльно, грязно);

[1)] ***В соответствии с требованиями ГОСТ Р ИСО 31000—2019, ГОСТ Р ИСО/МЭК 15408-1—2012, ГОСТ Р ИСО/МЭК 27002—2012.***

- электромагнитное излучение;
- электростатические и магнитные поля;
- давление воздуха.

5.5.2.3 Критерий, связанный с воздействием опасных условий:

- химическое, радиоактивное воздействие;
- взрывоопасная атмосфера.

5.5.2.4 Критерий, связанный с воздействием факторов, вызывающих ухудшение характеристик при штатной эксплуатации:

- износ;
- загрязнения;
- ***старение, а также различные химические, адсорбционные и диффузные эффекты.***

5.5.2.5 Критерий, связанный с эргономикой. В процессе аутентификации следует обеспечить максимальное удобство использования средства аутентификации, особенно в том случае, когда предполагается его применение неподготовленными инспекторами. Является желательным усиление возможностей восприятия органами чувств человека или адаптация инструмента для приспособления аутентификации к любым заданным условиям.

Критерий, связанный с условиями освещения. Необходимо определить условия освещения, при котором будут функционировать элемент и инструмент аутентификации. Условия освещения не должны мешать считыванию элементов аутентификации или считыванию результатов, если контроль выполняется с помощью инструмента.

Критерий, связанный с погодой и осадками (дождь/влажность/снег). Необходимо определить условия при дожде, влажности и снеге, при которых будут функционировать элемент и инструмент аутентификации. Погодные условия не должны мешать считыванию элементов аутентификации или считыванию результатов, если контроль выполняется в штатных условиях с помощью инструмента.

Критерий, связанный с температурой. Необходимо определить температурные условия, при которых будут функционировать элемент и инструмент аутентификации. Если контроль должен проводиться в жестких температурных условиях, эргономика инструмента должна быть адаптирована к индивидуальному снаряжению и одежде инспекторов.

Критерий, связанный с ветром. Необходимо определить ветровые условия, при которых будут функционировать элемент и инструмент аутентификации. Ветер не должен мешать применению средства аутентификации, соответствующего инструмента и/или анализу результатов исследования, если это штатные условия применения.

5.5.2.6 Следует установить перечисленные ниже параметры процесса аутентификации:

- продолжительность цикла аутентификации. Необходимо установить время, необходимое для проведения аутентификации;
- частота. Необходимо установить количество последовательных точных аутентификаций в единицу времени, выполняемое средством аутентификации;
- количество одновременных аутентификаций. Необходимо установить зависимость времени отклика от количества одновременно выполняемых аутентификаций (этот критерий касается только средств аутентификации онлайн);
- время отклика. Необходимо установить время отклика, требующееся для получения результата аутентификации.

5.5.3 Критерии, связанные с жизненным циклом. При выборе средства аутентификации требуется провести анализ требований жизненного цикла средства аутентификации в отношении защищаемого товара. Необходимо рассмотреть факторы воздействия окружающей среды, влияющие как на материальный товар, так и на средство аутентификации. Кроме того, необходимо выполнить анализ для определения характеристик жизненного цикла используемого в процессе контроля инструмента аутентификации. Такие факторы могут включать потенциальное устаревание инструмента, техническое устаревание средства аутентификации, неудачи компании и систем обеспечения, потребность в резервных элементах аутентификации и в их установке на товаре или его упаковке.

Для товаров с коротким жизненным циклом анализ может иметь минимальный горизонт прогнозирования. Для товаров с длительным жизненным циклом и/или критическими требованиями к характеристикам анализ может потребовать расширенного горизонта прогноза и сложных методов исследований, а также привлечения других заинтересованных участников оборота продукции, чтобы гарантировать безопасность данных на протяжении всего жизненного цикла рассматриваемого средства.

5.5.4 Перечисленные ниже критерии эффективности связаны с процессом внедрения средства аутентификации.

5.5.4.1 Критерии, связанные с политикой обеспечения безопасности. Необходимо установить общую политику обеспечения безопасности средства аутентификации. Это касается всех компонентов рассматриваемого средства, связей между ними и процессов. Сюда также входит безопасность цепи поставок и используемых информационных технологий.

Политика обеспечения безопасности должна соответствовать международным, национальным стандартам, нормативным документам или признанным в промышленности методам.

5.5.4.2 Критерии, связанные с соответствием нормативным документам.

Средство аутентификации должно соответствовать требованиям существующих нормативных документов государственных и регулирующих органов, международным требованиям, а также возможным требованиям частных организаций.

Должен проводиться аудит на соответствие требованиям контроля качества и обеспечения безопасности. Эффективность методов обеспечения безопасности и качества, подтверждаемая при проверке, должна являться критерием при выборе средства аутентификации. Аудиты следует выполнять в соответствии с требованиями международных и национальных стандартов в области систем менеджмента качества, систем информационной безопасности, требованиями к органам, проводящим аудит[1)], а также в соответствии с условиями соглашений.

5.5.4.3 Перечисленные ниже критерии эффективности связаны с функционированием:

- время начала применения. Время запуска средства аутентификации (включение в холодном состоянии или «пробуждение») должно соответствовать требованиям спецификаций на средство аутентификации;
- способность процесса к адаптации. Должна быть возможность адаптации протокола аутентификации, чтобы приспособиться к увеличенному объему аутентификации;
- возможность модернизации. Средство аутентификации должно быть модернизируемым без ущерба для его эффективности;
- подотчетность и контроль качества. Необходимо внедрить процедуры для проверки производства элементов аутентификации в отношении качества и количества элементов и инструментов аутентификации согласно технической документации на средства аутентификации;
- возможность многократного использования. Может оказаться выгодным создать один инструмент, способный выполнять многократные операции по аутентификации или выполнять разные функции. Если инструмент используется для верификации различных товаров в одно и то же время, то при этом верификация одного товара не должна препятствовать верификации других товаров;
- точность результатов. Разработчиком требований к инструментам должны быть определены приемлемые доли ошибочной приемки и ошибочной браковки. Эти уровни должны сохраняться в границах изменчивости окружающих рабочих условий, определенных изготовителем.
- нормальный/резервный режим. Для инструментов с собственным источником питания или инструментов, которые работают в режиме онлайн, необходимо определить, приемлем ли режим работы с пониженной функциональностью. При этом определении следует учитывать, имеются ли различные уровни у таких режимов работы (разряженная батарея, отсутствие сети и т. д.) или альтернативный протокол, который может иметь доступ к элементу аутентификации другого типа или к отдельному дублирующему средству. Для того чтобы получить услугу наилучшего качества, следует учитывать надежность, среднее время между отказами, калибровку и профилактическое техническое обслуживание компонентов средства аутентификации;
- условия снабжения и обслуживания инструмента. Должны быть приняты во внимание рабочие параметры системы снабжения и технического обслуживания рассматриваемых инструментов, особенно с точки зрения:

1) контроля и поддержания годности;

2) наличия ремонтного центра;

3) безопасности, связанной с цепью поставки инструментов;

- обучение. На надежность результата аутентификации в общем случае оказывает влияние компетентность инспектора; чем лучше он подготовлен, тем надежнее результат аутентификации. Курс обучения должен выбираться согласно определенному уровню доступа. Средство аутентификации мо-

---

[1)] В соответствии с ГОСТ Р ИСО/МЭК 17021-1—2017 «Оценка соответствия. Требования к органам, проводящим аудит и сертификацию систем менеджмента. Часть 1. Требования».

жет потребовать определить особую политику обучения для инспекторов каждого уровня. При необходимости должна проводиться регулярная актуализация обучения;

- здоровье и окружающая среда. Необходимо учитывать потенциальное влияние средства аутентификации на здоровье людей и окружающую среду.

6 Оценка эффективности средства аутентификации

6.1 Следует учитывать, что эффективность средства аутентификации зависит от правильного анализа риска и анализа критериев, которые устанавливают ряд требований к соответствию. Оценка эффективности является способом установить, соответствует ли средство аутентификации установленным стандартам и дает ли оно измеримый результат. В дополнение к общей эффективности средства аутентификации следует выполнить оценку на основе спецификации для каждой категории критериев. Средства аутентификации являются ключевыми для выявления подделок и, следовательно, поддерживают соответствующее исследование и борьбу с фальсификациями, а также обеспечивают получение подтверждающих доказательств. Они также могут способствовать обороту фальсифицированной продукции, делая ее оборот технически и финансово затрудненным для фальсификаторов. Следует учитывать, что средство аутентификации не защитит от всех рисков и одни метрики оценки могут не подходить для всего многообразия решений по аутентификации.

6.1.1 Оценка эффективности средства аутентификации

Следует определить стратегию оценивания в отношении соответствия техническим требованиям, которые введены разработчиком с учетом статуса поддельности товара. Товар может иметь статус подделки на основе следующих категорий:

а) Товар уже поступил на рынок, и он подделан. В этих условиях материальный товар подделывается, и степень фальсификации может быть известна или неизвестна поставщику товара. Когда уровень фальсификации известен, то оценка эффективности может быть основана на сокращении количества известных подделок, если это сокращение можно эффективно привязать к средству аутентификации. Когда уровень фальсификации неизвестен, то оценка количества подделок должна выполняться с помощью расследования и/или статистического анализа. На основе такого анализа можно провести оценку эффективности средства аутентификации.

б) Материальный товар уже поступил на рынок и подделки не обнаружено. Статус такого товара может вытекать из целого ряда факторов:

- товар очень сложно подделать;
- выгода от подделки незначительна или вообще ее нет;
- эффективное средство уже действует; или
- исследование не было проведено должным образом, то есть подделки есть, но не выявлены, или сообщение о подделках не было должным образом распространено.

Следует выполнить анализ риска, чтобы определить угрозу фальсификации, и существуют ли финансовые, правовые, социальные последствия, проблемы здравоохранения, безопасности и регулирования, которые необходимо обсудить, чтобы определить, необходимо ли средство аутентификации для данного материального товара. Разработка оценки эффективности для средства, которое используется как защита от фальсификации, или оценки, показывающей отсутствие подделок, является сложной задачей, которая потребует оценивания на основе вышеуказанных факторов.

в) Товар еще не поступил на рынок. Перед выпуском товара на рынок следует выполнить анализ риска, чтобы определить вероятность фальсификации и наличие или отсутствие финансовых, правовых, социальных проблем, проблем здравоохранения, безопасности и регулирования, которые требуют применения средства аутентификации. Оценки эффективности средств аутентификации могут быть основаны на двух изложенных выше категориях ***(см. перечисления а), б)).***

Если товар уже на рынке, то изменчивость кривой сбыта может отражать развитие ситуации с фальсификациями. Однако отклик на проблемы фальсификации нуждается в большем количестве эффективных индикаторов, притом что внешние (не технические) действия тоже могут привести к изменчивости кривой сбыта.

Следует принимать во внимание, что стандарт не определяет уникальные протоколы оценки эффективности средств аутентификации.

Оценка эффективности должна являться оценкой выполнения требований выбранным средством по критериям выбора, т. е. оценкой того, насколько хорошо выбранное средство соответствует критериям эффективности средств аутентификации, определенных в следующих областях ***(см. 5.2)***:

- физические характеристики;
- сопротивление воздействиям;
- интеграция с продукцией, ***упаковкой, условиями оборота продукции***;
- взаимодействие с инфраструктурой участников оборота продукции и окружающей средой;
- процессы внедрения ***и применения***.

Оценка эффективности может быть выполнена перечисленными ниже способами:

1) Оценивание физических характеристик.

Данный способ предполагает контроль соответствия физических характеристик средств аутентификации установленным значениям: размеров, предела прочности при растяжении, размерной стабильности, гибкости и т. д. Следует учитывать, являются ли характеристики измеряемыми и должным образом определенными в технических требованиях, может ли быть обеспечено поддержание постоянных значений характеристик в условиях производства и применения для обеспечения качества.

2) Оценивание сопротивления агрессивным воздействиям.

Данный способ предполагает проведение проверки соответствия средства аутентификации установленным критериям сопротивления агрессивным воздействиям: копированию, взлому, вскрытию и т.д. Следует учитывать, являются ли характеристики измеряемыми и должным образом определенными в технических требованиях, может ли быть обеспечено поддержание постоянных значений характеристик в условиях производства и применения для обеспечения качества.

3) Оценивание процесса интеграции ***с продукцией, упаковкой, условиями оборота продукции.***

Данный способ предполагает проведение проверки обеспечения успешной интеграции средства аутентификации в процессе производства. Следует учитывать, являются ли характеристики измеряемыми и должным образом определенными в технических требованиях, может ли быть обеспечено поддержание постоянных значений характеристик в условиях производства и применения для обеспечения качества.

4) Оценивание взаимодействия с инфраструктурой участников оборота продукции и окружающей средой.

Данный способ предполагает проведение проверки соответствия средства аутентификации критериям функционирования в условиях оборота продукции и окружающей среды, опасных условиях и т. д. Следует учитывать, являются ли характеристики измеряемыми и должным образом определенными в технических требованиях, может ли быть обеспечено поддержание постоянных значений характеристик.

5) Оценивание процесса внедрения ***и применения.***

Данный способ предполагает проведение проверки успешности процесса внедрения с учетом всех заданных характеристик средства аутентификации. Следует учитывать, являются ли характеристики измеряемыми и должным образом определенными в технических требованиях, может ли быть обеспечено поддержание постоянных значений характеристик.

Оценка эффективности средства аутентификации должна определяться на основе проведения оценки всех критериев процесса выбора, с учетом особенностей среды фальсификации рассматриваемого товара и анализа ожидаемого риска.

6.2 Оценка эффективности производства элементов аутентификации

В процессе производства средств аутентификации должны выполняться требования нормативных документов к качеству продукции. Поставщики средств аутентификации должны поддерживать систему менеджмента качества. Контроль качества следует проводить в рамках аудитов качества.

Для средств аутентификации должны быть рассмотрены и учтены вопросы безопасности. Должны быть рассмотрены все процессы — от создания элемента аутентификации до отгрузки защищенных товаров. Следует учитывать, что процессы, для которых не имеется протоколов и процедур обеспечения безопасности, могут повлиять на общую эффективность средства аутентификации. Методы обеспечения безопасности должны быть документированы и проверены.

При нестабильности процесса производства большие вариации значений характеристик и большие различия в качестве производства или интеграции элементов аутентификации в товары будут затруднять принятие инспектором решения о подлинности или поддельности товара.

Для оценки эффективности применяют следующие показатели:

- количество ошибочных браковок при контроле качества принимаемой готовой продукции по завершении производства, означающее, что параметры элементов аутентификации выходят за поле

допуска или какое-либо несоответствие процесса производства делает элемент аутентификации несчитываемым;

- количество ошибочных браковок в системе распределения товара, означающее, что характеристики элементов аутентификации или связь элемента с товарами неустойчивы;

- количество ошибочных приемок. Такое определение требует конкретной методики контроля. Методика должна включать подбор ложных элементов аутентификации, которые могут успешно преодолеть контроль аутентификации. Как правило, такой контроль выполняет независимая лаборатория.

6.3 Оценка эффективности в типовой ситуации верификации/аутентификации

Оценивание в типовых ситуациях контроля может касаться:

а) инспектора(ов), в том числе:
1) права доступа к данным идентификации/аутентификации;
2) обучения;

б) инструмента, в том числе:
1) применения для аутентификации;
2) работы при пониженной функциональности;
3) технического обслуживания, калибровки;
4) загрузки программ и данных;
5) возможности фальсификации;

в) линий коммуникаций и обмена данными (если требуется), в том числе:
1) успешно принятых и отвергнутых входов в систему (логины);
2) качества обслуживания;

г) результатов исследований, в том числе:
1) объемов выборки;
2) количества выявлений: подлинности/поддельности;
3) количества неинтерпретируемых элементов аутентификации (“не определено”).

В зависимости от типа внедренного средства аутентификации указанные оценки можно получать с помощью средств автоматизированного сбора данных или с помощью заключений инспекторов.

6.4 Оценка эффективности в чрезвычайной ситуации верификации/аутентификации

В чрезвычайной ситуации, когда объемы обнаруженного фальсификата достигают определенного порога, следует адаптировать обычные методы оценки или применить специальные методы аутентификации, направленные на исследование проблемы, связанной с подделкой, и принять соответствующие меры противодействия.

Оценка эффективности должна рассматриваться в этом случае как ключевой элемент проверки результативности этих мер противодействия фальсификатам.

6.5 Итоговая оценка эффективности

Оценка эффективности средства аутентификации зависит от требований, предъявленных к этому средству, и является уникальной для каждой группы требований.

Следует учитывать, что оценка эффективности средств аутентификации является сложной задачей и включает оценивание множества значений критериев выбора, как указано в данном стандарте. Значения показателей могут быть простыми, как ответ «да или нет», или такими же сложными, как технические требования к проектируемому устройству. В большинстве случаев показателем оценки эффективности может быть ответ на вопрос о выполнении средством или элементом аутентификации задачи, возложенной на него в процессе аутентификации.

Оценка эффективности средства аутентификации не должна основываться только на наиболее очевидных признаках. Следует оценивать эффективность с учетом всех требований, условий и процессов. Элемент аутентификации, показавший себя эффективным в одной группе условий, может не сработать в процессе аутентификации, если он не был оценен по всей совокупности технических требований в соответствии с критериями, описанными в настоящем стандарте.

Приложение А
(рекомендуемое)

Таблица данных для оценки средств аутентификации

А.1 В данном приложении представлена таблица А.1 данных для оценки средств аутентификации согласно критериям, определенным в разделе 5.

А.2 Данная таблица предназначена для выбора из перечня критериев эффективности тех критериев, которые необходимо рассмотреть применительно к разрабатываемым средствам аутентификации, а также содержит уровень критичности каждого критерия.

Критичность является субъективной мерой важности этих критериев со стороны разработчика.

Таблица А.1 — Данные для оценки средств аутентификации

Критерии оценки	Поставленные цели	Оцениваемые параметры	Критичность				Оценка
			Высокая	Средняя	Низкая	Не применяется	
1 Физические характеристики элемента аутентификации	Установить характеристики элемента аутентификации в его окружении						
1.1 Статические характеристики		Геометрические размеры (высота, ширина)					
		Толщина					
		Масса					
1.2 Динамические характеристики		Гибкость					
		Вязкость					
		Износ					
		Предел прочности при растяжении					
1.3 Характеристики долговечности		Умеренные условия окружающей среды					

Продолжение таблицы А.1

Критерии оценки	Поставленные цели	Оцениваемые параметры	Критичность				Оценка
			Высокая	Средняя	Низкая	Не применяется	
		Суровые условия окружающей среды					
		Механические воздействия					
		Старение материалов и устройств					
1.4 Влияние на здоровье и окружающую среду		Электромагнитное излучение					
		Радиоактивность					
		Химический состав и запрет на некоторые вещества					
		Миграция веществ					
		Способность к рециклингу отходов продукции, упаковки, средств аутентификации					
1.5 Физические характеристики, связанные с отличительными особенностями применения		Возможность визуального контроля					
		Распознаваемость техническими средствами					
		Очевидность подделки					
		Уникальность отношения элементов аутентификации и единиц продукции					

Продолжение таблицы А.1

Критерии оценки	Поставленные цели	Оцениваемые параметры	Критичность				Оценка
			Высокая	Средняя	Низкая	Не применяется	
2 Стойкость элементов аутентификации к агрессивным воздействиям	Установить эффективность элемента аутентификации в отношении различных типов агрессивных воздействий						
2.1 Стойкость к «обратному проектированию» (путем разборки законного образца и воспроизведения незаконного аналога)		Оценка стойкости к «обратному проектированию»					
		Копирование					
		Имитация, эмуляция					
2.2 Сопротивление подделке и обеспечение очевидности подделки		Сопротивление подделке					
		Очевидность подделки					
2.3 Стойкость к изменению							
2.4 Сопротивление утечке информации по побочным каналам							
2.5 Перехват информационных сообщений							
2.6 Устаревание							

Продолжение таблицы А.1

Критерии оценки	Поставленные цели	Оцениваемые параметры	Критичность				Оценка
			Высокая	Средняя	Низкая	Не применяется	
2.7 Бесконтрольное повторное использование							
3 Процесс интеграции	Установить эффективность элемента аутентификации при интеграции с товаром						
3.1 Безопасность		Политика обеспечения безопасности					
		Безопасность цепи поставок					
3.2 Производство		Наличие средств аутентификации					
		Совместимость с товаром/ упаковкой					
		Совместимость с процессом					
		Совместимость с логистикой					
		Целостность и защита данных					
3.3 Соответствие требованиям к интеграции							
3.4 Обучение							
4 Сопротивление инструментов аутентификации агрессивным воздействиям	Установить характеристики инструмента аутентификации при агрессивных воздействиях						
4.1 Стойкость к раскрытию секретов, имитации и эмуляции		Стойкость к раскрытию секретов					
		Стойкость к имитации, эмуляции					

Продолжение таблицы А.1

Критерии оценки	Поставленные цели	Оцениваемые параметры	Критичность				Оценка
			Высокая	Средняя	Низкая	Не применяется	
4.2 Сопротивление воздействию/ очевидность воздействия							
4.3 Сопротивление Изменению и доступу к данным							
4.4 Сопротивление утечке данных путем анализа побочных явлений							
4.5 Возможность перехвата сообщений							
4.6 Защита обмена данными							
4.7 Безопасность доступа в базы данных							
4.8 Резервирование данных, дублирование системы							
4.9 Устаревание инструментов аутентификации							
4.10 Уязвимость ко всем типам воздействий							
5 Критерии выбора средств аутентификации	Установить эффективность средств аутентификации в среде применения						

Продолжение таблицы А.1

Критерии оценки	Поставленные цели	Оцениваемые параметры	Критичность				Оценка
			Высокая	Средняя	Низкая	Не применяется	
5.1 Функционирование в условиях производство/ окружающая среда							
5.1.1 Необходимые ресурсы		Источники энергии					
		Коммуникации					
		Обеспечивающие средства					
5.1.2 Условия окружающей среды		Температура					
		Влажность					
		Загрязнения					
		Электромагнитное излучение					
		Электростатические и магнитные поля					
		Давление воздуха					
5.1.3 Воздействие опасных условий		Химическое					
		Радиоактивное					
		Взрывоопасная среда					
5.1.4 Нарушение нормального использования		Износ, ***старение, а также различные химические, адсорбционные и диффузные эффекты***					
		Загрязнения					

Продолжение таблицы А.1

Критерии оценки	Поставленные цели	Оцениваемые параметры	Критичность				Оценка
			Высокая	Средняя	Низкая	Не применяется	
5.1.5 Эргономика		Условия освещения					
		Дождь, влажность, снег					
		Температура					
		Ветер					
5.1.6 Параметры аутентификации		Продолжительность цикла аутентификации					
		Частота					
		Количество одновременных аутентификаций					
		Время отклика					
5.2 Жизненный цикл							
6 Процесс внедрения	Установить эффективность средства аутентификации в применении						
6.1 Политика обеспечения безопасности							
6.2 Соответствие		Соответствие требованиям					
		Аудит соответствия					
6.3 Применение		Начало применения					
		Способность процесса к адаптации					

Окончание таблицы А.1

Критерии оценки	Поставленные цели	Оцениваемые параметры	Критичность				Оценка
			Высокая	Средняя	Низкая	Не применяется	
		Возможность модернизации					
		Подотчетность и контроль качества					
		Возможность многократного использования					
		Точность результатов					
		Нормальный/ резервный режимы					
		Снабжение и обслуживание инструмента					
		Обучение					
		Здоровье, окружающая среда					

Приложение В
(рекомендуемое)

Таблица средств контроля доступа

Назначение таблицы В.1 заключается в предоставлении средств для определения стратегии борьбы с фальсификациями с учетом методов контроля элементов аутентификации. Для получения высокого уровня защиты следует использовать сочетание различных приемов и технологий. К различным уровням элементов аутентификации не следует допускать инспекторов любой категории. Разработчики средств аутентификации должны определить, кто к чему может иметь доступ.

Таблица В.1 — Таблица разграничения доступа к данным

Применяемый инспектором элемент аутентификации	Конечный пользователь	Сети поставок и распределения	Орган надзора	Персонал, имеющий разрешение от правообладателя	Аккредитованная/ уполномоченная лаборатория
Открытый Проверяемый независимо органами восприятия человека					
Скрытый Требует технических средств					
Специальный лабораторный анализ Требует оценки в лаборатории					

Приложение ДА
(справочное)

Сведения о соответствии ссылочных национальных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте

Таблица ДА.1

Обозначение ссылочного национального стандарта	Степень соответствия	Обозначение и наименование ссылочного международного стандарта
ГОСТ Р ИСО 9000—2015	IDT	ISO 9000:2015 «Системы менеджмента качества. Основные положения и словарь»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта: IDT— идентичный стандарт.		

Библиография

[1] ВТО. Аспекты прав интеллектуальной собственности, касающиеся торговли [Trade related aspects of intellectual lpropertyrights (TRIPS)]

[2] ИСО/МЭК 15408-1 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. Часть 1. Введение и общая модель

[3] ИСО/МЭК 27002 Информационная технология. Методы и средства обеспечения безопасности. Свод правил по управлению защитой информации

[4] ISO Guide 73:2009 Менеджмент риска. Словарь

[5] Североамериканская организация продукции в области безопасности, (NASPO) и Альянс по защите документации, (DSA). Официальное сообщение в письменном виде: Как выбрать характеристики безопасности

УДК 004.056+005]:62:34:006.354 ОКС 13.310, 03.140

Ключевые слова: фальсификации, контрафакт, критерии, эффективность, аутентификация

БЗ 1—2020/124

Редактор *П.К. Одинцов*
Технический редактор *И.Е. Черепкова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 04.12.2019. Подписано в печать 17.01.2020. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 4,18. Уч.-изд. л. 3,34.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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

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

gost.e-ecolog.ru