Международный Документ

OIML D 31

Издание 2019 (R)

Сводное издание,
включающее Поправки
Изменения 1 (08.09.2020)

INTERNATIONAL DOCUMENT

OIML D 31
Edition 2019 (E)

Общие требования к программно-управляемым средствам измерений

Dastur orqali boshqariladigan o‘lchash vositalariga qo‘yiladigan umumiy talablar

Exigences générales pour les instruments de mesure contrôlés par logiciel

General requirements for software controlled measuring instruments

---

ORGANISATION INTERNATIONALE
DE METROLOGIE LEGALE

INTERNATIONAL ORGANIZATION
OF LEGAL METROLOGY

МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ
ЗАКОНОДАТЕЛЬНОЙ МЕТРОЛОГИИ

XALQARO QONUNLASHTIRUVCHI
METROLOGIYA TASHKILOTI

Неофициальный перевод
английской версии ГУ «Уз НИМ»
под редакцией доцента А.Б. Садыкова

Содержание

Предисловие…… 4
1 Введение…….. 5
2 Область и сфера применения…… 5
3 Термины и определения…….. 6
3.1 Общая терминология…… 6
3.2 Сокращения…… 15
4 Инструкции по использованию настоящего Документа при составлении Рекомендаций МОЗМ…… 15
5 Оценка рисков…….. 16
6 Требования к средствам измерений в отношении применения программного обеспечения…… 17
6.1 Общие требования…….. 17
6.2 Требования, зависящие от конфигураций…… 22
7 Утверждение типа……... 37
7.1 Документация программного обеспечения, предоставляемая для утверждения типа…… 37
7.2 Требования к процедуре утверждения ……..... 38
7.3 Методы аттестации…… 39
7.4 Процедура оценки программного обеспечения…….. 48
7.5 Оборудование при тестировании (EUT)…… 48
8 Поверка средств измерений…… 49
8.1 Общее…… 49
8.2 Методы поверкии, тестовые элементы…..……... 49
Приложение A (Справочное) Библиография…….. 51
Приложение B (Справочное) Пример отчета об оценке программного обеспечения..……. 53
Приложение C (Справочное) Комментарии к терминологии по измерениям…….. 60
Приложение D Указатель…… 62

Предисловие

Международная Организация Законодательной Метрологии (OIML - МОЗМ) является всемирной, межправительственной организацией, основной целью которой является гармонизация правил метрологического контроля, применяемых национальными метрологическими службами или связанными с ними организациями государств-членов. Основными категориями публикаций МОЗМ являются:

- **Международные Рекомендации (OIML R - МОЗМ Р),** которые являются модельными правилами, устанавливающими метрологические характеристики, необходимые для определенных средств измерений, и которые определяют методы и оборудование для проверки их соответствия. Государства-члены МОЗМ должны выполнять эти Рекомендации в максимально возможной степени;
- **Международные Документы (OIML D - МОЗМ Д),** которые по своей природе являются информативными и предназначены для гармонизации и улучшения работы в области законодательной метрологии;
- **Международные Руководства (OIML G - МОЗМ Г),** которые также являются информативными по своей природе и предназначены для того, чтобы дать указания по применению определенных требований к законодательной метрологии;
- **Международные Основные Публикации (OIML B - МОЗМ Б),** которые определяют правила работы различных структур и систем МОЗМ.

Проекты Рекомендаций, Документов и Руководств МОЗМ разрабатываются проектными группами, связанными с Техническими комитетами или подкомитетами, в состав которых входят представители государств-членов МОЗМ. Некоторые международные и региональные институты также участвуют в консультациях. Соглашения о сотрудничестве были заключены между МОЗМ и некоторыми институтами, такими как ИСО и МЭК, с целью избежание противоречивых требований. Следовательно, производители и пользователи средств измерений, испытательных лабораторий и т.д. могут одновременно применять публикации МОЗМ и публикации других учреждений.

Международные рекомендации, документы, руководства и базовые публикации публикуются на английском языке (E) и переводятся на французский язык (F) и подлежат периодическому пересмотру.

Кроме того, МОЗМ участвует в совместных комитетах с другими организациями по разработке **Словарей (OIML V - МОЗМ С)** и **Совместных Руководств (G)**, а также периодически поручает экспертам по законодательной метрологии написание **Экспертных Отчетов (OIML E - МОЗМ Э)**. Экспертные Отчеты предназначены для предоставления информации и советов, и составляются исключительно с точки зрения их автора, без участия Технического Комитета или Подкомитета, ни МКЗМ. Таким образом, они не обязательно представляют точку зрения МОЗМ.

Настоящая публикация - OIML D 31, издание 2019 (E) - подготовлена Проектной Группой 3 в Техническом подкомитете МОЗМ ТС 5/SC 2 *Программное обеспечение.* Она была одобрена для окончательной публикации Международным Комитетом Законодательной Метрологии в 2020 году для официального утверждения.

Публикации МОЗМ можно скачать с вебсайта МОЗМ в PDF - формате. Дополнительную информацию по публикациям МОЗМ можно получить в штаб-квартире организации:

Bureau International de Métrologie Légale (*Международное бюро законодательной метрологии*)
11 rue Turgot - 75009 Paris – France (*ул. Тургo, 11 - 75009 Париж – Франция*)
Телефон: 33 (0)1 48 78 12 82
Факс: 33 (0)1 42 82 17 27
Электронная почта: biml@oiml.org
Интернет: www.oiml.org

Общие требования к программно-управляемым средствам измерений

1 Введение

Основная цель данного Международного Документа состоит в том, чтобы предоставить техническим комитетам и подкомитетам МОЗМ рекомендации по определению соответствующих требований к функциональным возможностям программного обеспечения в средствах измерений, на которые распространяются Рекомендации МОЗМ.

Кроме того, данный Международный Документ может послужить руководством для государств-членов МОЗМ по внедрению Рекомендаций МОЗМ в их национальные законодательства.

2 Область и сфера применения

2.1 Данный Международный Документ устанавливает общие требования к законодательно значимым функциональным возможностям и безопасности программного обеспечения в средствах измерений и предоставляет рекомендации по проверке соответствия средств измерений) данным требованиям.

2.2 Данный Документ должен рассматриваться техническими комитетами и подкомитетами МОЗМ как основа для установления конкретных требований к программному обеспечению и процедурам, описанным в Рекомендациях МОЗМ и применяемым к определенным категориям средств измерений (далее именуемых «соответствующие Рекомендации»).

2.3 Инструкции, содержащиеся в данном Документе, применяются только к программно-управляемым средствам измерений или их комплектующим.

Примечание 1: Данный Документ не описывает все технические требования, установленные для программно-управляемых средств измерений; эти требования должны быть приведены в соответствующей Рекомендации МОЗМ, например, для весов, счетчиков воды и т.д..

Примечание 2: Данный Документ затрагивает также некоторые аспекты, относящиеся к средствам защиты данных. Кроме того, необходимо учитывать национальные правила в этой сфере.

3 Термины и определения

Настоящий документ содержит определения, которые соответствуют определениям, приведенным в Международном Словаре по метрологии «Основные и общие понятия и соответствующие термины» издание 3 (OIML V 2-200:2012 [1]), Международном словаре терминов по законодательной метрологии (OIML V 1:2013 [6]), Международном документе МОЗМ «Общие требования к средствам измерений – Условия окружающей среды» (OIML D 11:2013 [2]) и некоторых Международных стандартах ИСО/МЭК. Для целей настоящего Документа применяются следующие определения и сокращения.

3.1 Общая терминология

3.1.1 Журнал контроля (audit trail)

Постоянный файл данных, содержащий информационный отчет о событиях с временными отметками, например, об изменениях в значениях параметров средства измерений или обновлениях программного обеспечения, или других юридически значимых действиях, способных повлиять на метрологические характеристики.

[OIML V 1:2013, 6.05]

3.1.2 Аутентификация (authentication)

Проверка заявленной или предполагаемой личности пользователя, процесса или средства измерений..

Примечание: Это может потребоваться при проверке того, что загруженное ПО исходит от владельца сертификата.

3.1.3 Подлинность (authenticity)

Результат процесса аутентификации (пройден или нет).

3.1.4 Специально сконструированное устройство (built-for-purpose device)

Устройство, сконструированное для решения конкретной метрологической задачи.

Примечание: Незаявленные интерфейсы к операционной системе на устройствах такого типа недоступны или отсутствуют.

3.1.5 Средства контроля (checking facility)

Средство, встроенное в средство измерений, которое позволяет выявлять существенные ошибки и принимать соответствующие меры.

Примечание: «Принимать соответствующие меры» относится к любому адекватному отклику средства измерения (световой сигнал, акустический сигнал, остановка процесса измерения и т.д.).

Адаптировано из [OIML V 1:2013, 5.07]

3.1.6 Коммуникационный интерфейс (communication interface)

Часть прибора, обеспечивающая передачу информации между средствами измерений, компонентами средств измерений или другими внешними системами.

Примечание 1: Интерфейсы связи могут быть проводными, оптическими, радио и т.д., и они обычно предназначены для использования определенного протокола.

Примечание 2: Это определение не включает в себя связь между программными модулями.

3.1.7 Криптографический сертификат (cryptographic certificate)

Данные, содержащие общедоступный ключ, принадлежащий средству измерений*И* или лицу, а также уникальная идентификация объекта, такая как регистрационный номер средства измерений или имя и персональный идентификационный номер (ПИН) личности. Данные подписываются заслуживающим доверия учреждением с помощью электронной подписи. Присвоение объекту общедоступного ключа можно проверить путем использования общедоступного ключа заслуживающего доверия учреждения и расшифровки подписи данного сертификата, плюс дата истечения срока действия.

3.1.8 Криптографические средства (cryptographic means)

Такие средства, как шифрование и дешифрование с целью сокрытия информации от неавторизованных лиц (см. 3.1.13), или случайные данные и подписи для обеспечения целостности и подлинности.

3.1.9 Область определения данных (data domain)

Размещение в памяти, которое необходимо для каждой программы обработки данных.

Примечание*:* Домены данных могут принадлежать только одному *программному модулю* или нескольким.

3.1.10 Параметр, зависящий от конкретного устройства (device-specific parameter)

Законодательно значимый параметр со значением, зависящим от конкретного средства измерений.

Примечание*:* Параметры, зависящие от устройства, включают параметры регулировки (например, регулировку чувствительности или другие регулировки, или поправки) и параметры конфигурации (например, максимальное значение, минимальное значение, единицы измерения и т.д.).

[OIML V 1:2013, 4.12]

3.1.11 Устойчивость (durability)

Способность средства измерений поддерживать свои рабочие характеристики в течение всего периода использования.

[OIML V 1:2013, 5.15]

3.1.12 Электронное средство измерений (electronic measuring instrument)

Средство измерений, предназначенное для измерения электрической или неэлектрической величины с помощью электронных средств и/или средств измерений, оборудованное электронными устройствами.

Примечание*:* В рамках данного Документа вспомогательное оборудование, при условии, что оно подлежит метрологическому контролю, считается частью средства измерений

[OIML D 11:2004, 3.1]

3.1.13 Электронная подпись (electronic signature)

Средство, которое добавляется к программному обеспечению или данным с целью подтверждения происхождения программного обеспечения или данных, т.е. подтверждения их аутентичности, или проверки того, что программное обеспечение или данные не подвергались изменениям, т.е. подтверждения их целостности.

Примечание 1*:* Для формирования электронной подписи обычно применяют систему с открытым ключом, основанную на использовании пары ключей, из которых только один ключ должен держаться в секрете; а другой может быть открытым.

Примечание 2: Секретный ключ используется применительно к защищенному программному обеспечению или данным. Открытый ключ используется, когда программное обеспечение или данные верифицируются перед использованием.

Примечание 3*:* В момент верификации может потребоваться криптографический сертификат (см. 3.1.7), чтобы быть уверенным в аутентичности открытого ключа.

3.1.14 Погрешность показания (error of indication)

Показание минус опорное (референтное) значение величины.

Примечание: Опорное (референтное) значение иногда называют (конвенциональным) истинным значением величины. См., однако, также МОЗМ V 2-200:2012, 2.12, Примечание 1).

[OIML V 1:2013, 0,04]

3.1.15 Журнал регистрации ошибок (error log)

Постоянный файл данных с записью информации об ошибках или значительных дефектах, которые влияют на метрологические характеристики средства измерений.

3.1.16 Событие (event)

Действие, при котором осуществляется модификация параметра средства измерений, поправочного коэффициента или обновление программного модуля.

[OIML V 1:2013, 6.06]

3.1.17 Счетчик событий (event counter)

Необнуляемый счетчик, увеличивающий свое значение на единицу при каждом событии.

3.1.18 Исполняемый код (executable code)

Цифровая информация, установленная в средстве измерений или компоненте (EPROM, жесткий диск и т.д.).

Примечание: Этот код интерпретируется центральным процессором (CPU) средства измерений и преобразуется в определенные логические, арифметические, декодирующие или транспортирующие данные операции.

3.1.19 Неисправность (fault)

Разница между погрешностью показания и основной погрешностью средства измерений.

Примечание 1: В принципе, неисправность является следствием непреднамеренного изменения данных, содержащихся или проходящих через электронный измерительный прибор.

Примечание 2: Как следует из определения, «неисправность» - это численная величина, которая выражается либо в единицах измерения, либо в виде относительной величины, например, в процентах.

[OIML V 1:2013, 5.12]

3.1.20 Хэш-функция (hash function)

(Математическая) функция, которая проецирует значения из большей (возможно очень большой) области на меньший диапазон.

Примечание: «Хорошая» хэш-функция такова, что результаты применения функции к (большому) набору значений в области определения данных будут распределены по меньшему диапазону равномерно (и предположительно случайно).

[ISO/IEC 9594-8:2014] [3]

3.1.21 Целостность (integrity) (программ, данных или параметров)

Гарантия того, что программы, данные или параметры не были подвергнуты никаким несанкционированным или непреднамеренным изменениям при использовании, передаче, хранении, ремонте или обслуживании.

3.1.22 Интерфейс (interface)

Общая граница между двумя функциональными блоками, определенная различными характеристиками, относящимися к функциям, физическим взаимосвязям, обмену сигналами и другим характеристикам блоков в зависимости от ситуации.

[ISO 2382-9:1995] [4]

3.1.23 Прерываемое измерение с накоплением результатов (interruptible cumulative measurement)

Измерительный процесс с прерыванием накоплением результатов, который может быть легко и быстро остановлен в нормальном режиме работы.

Примечание 1: Примеры включают: а) автоматическое средство измерений для взвешивания с прерывистым суммированием, б) дозатор топлива.

Примечание 2: См. также непрерываемое измерение с накоплением результатов (3.1.42).

3.1.24 Основная погрешность средства измерений (intrinsic error)

Погрешность показания, установленная при использовании средства в нормальных условиях.

[OIML V 11:2004, 0.06]

3.1.25 Законодательно значимый (legally relevant)

Предмет законодательного контроля.

3.1.26 Законодательно значимый параметр (legally relevant parameter)

Параметр средства измерений/компонента, (электронного) устройства, программного обеспечения или модуля, подлежащий законодательному контролю

Примечание: Различаются следующие типы юридически значимых параметров: параметры, зависящие от типа, и параметры, зависящие от устройства.

3.1.27 Законодательно значимая часть программного обеспечения (legally relevant software part)

Часть всех программных модулей средства измеренийИ/компонента, которые подлежат юридическому контролю.

3.1.28 Максимальная допускаемая погрешность (средства измерений) (maximum permissible error)

Предельное значение погрешности измерения по отношению к известному значению эталонной величины, допускаемое техническими условиями или правилами для данного измерения, средства измерения или измерительной системы.

Адаптировано из [OIML V 1:2013, 0.05]

3.1.29 Средство измерений (measuring instrument)

Устройство, предназначенное для проведения измерений, самостоятельно или в сочетании с дополнительным устройством (устройствами).

Адаптировано из [OIML V 1:2013, 0.10]

3.1.30 Измерение (measurement)

Процесс экспериментального определения одного или нескольких значений, которые могут быть обоснованно приписаны величине.

Примечание 1: Измерение не применимо к номинальным свойствам.

Примечание 2: Измерение предполагает сравнение величин или подсчет объектов.

Примечание 3: Измерение подразумевает описание величины, соизмеримой с предполагаемым использованием результата измерения, процедуры измерения и калиброванной измерительной системы, работающей в соответствии с установленной процедурой измерения, включая условия измерения.

Адаптировано из [OIML V 1:2013, 0.10]

3.1.31 Измерительные данные (measurement data)

Данные, используемые в процессе измерения.

Примечание: Измерительные данные включают данные, относящиеся к результатам измерений, и данные процесса измерений.

3.1.32 Погрешность измерения (measurement error)

Измеренное значение величины минус опорное значение величины.

Примечание 1: Понятие «погрешность измерения» может использоваться

а) когда имеется единственное опорное значение величины, на которое следует ссылаться, что имеет место, когда калибровка проводится с помощью эталона, а измеренное значение величины имеет незначительную неопределенность, или если задано нормальное значение величины, и в этом случае известна погрешность измерения известна, и

б) если измеряемая величина предположительно обладает единственным истинным значением или множеством истинных значений, располагаемых в пренебрежительно малом диапазоне, в этом случае погрешность измерения неизвестна.

Примечание 2: Измерение подразумевает сравнение количеств или подсчет объектов.

[OIML V 2-200:2012, 2.16]

3.1.33 Метаданные измерений (measurement metadata)

Метаданные, относящиеся к процессу измерений.

Примечание: Метаданные измерений включают метаданные, относящиеся к результатам измерений, и метаданные процесса измерения.

3.1.34 Данные процесса измерений (measurement process data)

Данные, используемые в процессе измерений для получения результата измерений.

Примечание: Примеры данных процесса измерений включают значения параметров измерения, значения настроек подключения или значения параметров сеанса.

3.1.35 Информация о процессе измерений (measurement process information)

Это набор значений качественных или количественных переменных, представляющих процесс измерений.

Примечание: Информация о процессе измерений включает данные и метаданные процесса измерений.

3.1.36 Метаданные процесса измерений (measurement process metadata)

Метаданные, относящиеся к процессу измерений.

Примечание: Примеры метаданных процесса измерений включают формат параметров измерения, формат настроек подключения или формат параметров сеанса.

3.1.37 Результат измерения (measurement result)

Набор значений, приписываемых измеряемой величине, вместе с любой другой доступной соответствующей информацией.

Примечание 1: Соответствующая информация может включать, например, неопределенность измерения, дату и время измерения, порядковый номер измерения, идентификацию датчика и, в случае, когда расчет цены является частью регулируемого законодательством программного обеспечения, цену за единицу и сумму к оплате.

Примечание 2: Результат измерения (включая значение величины, измеренной в соответствии с OIML V 2:200:2012) используется для регулируемых законодательством целей, например, для заключения сделки.

Адаптировано из [OIML V 2-200:2012, 2.9]

3.1.38 Данные, относящиеся к результату измерений (measurement result relevant data)

Это данные, используемые в процессе получения результата измерений.

Примечание: Примеры данных, относящихся к результату измерений, включают цифровой номер или аналоговое значение, полученное от датчика или идентификатора измерительного прибора, в тех случаях, когда они являются частью результата измерений.

3.1.39 Метаданные, относящиеся к результату измерений (measurement result relevant metadata)

Это метаданные, имеющие отношение к получению результата измерений.

Примечание: Примеры метаданных, относящихся к результатам измерений, включают формат цифрового номера или аналогового значения, полученного от датчика, формат значения, измеренной в соответствии с OIML V 2:200:2012 величины или формат идентификатора измерительного прибора, в тех случаях, когда оно является частью результата измерений.

3.1.40 Информация, относящаяся к результату измерений (measurement result relevant information)

Это набор значений качественных или количественных переменных, относящихся к результату измерений.

Примечание: Информация, относящаяся к результатам измерений, включает данные и метаданные, относящиеся к результатам измерений.

3.1.41 Метаданные (metadata)

Это данные о данных или элементах данных, по возможности, включающие описание данных, а также данные о владельце данных, путях доступа, правах доступа и волатильности данных.

[ISO/IEC 2382:2015 Информационные технологии – Словарь]

3.1.42 Непрерываемое измерение с накоплением результатов (non-interruptible cumulative measurement)

Это измерительный процесс с накоплением результатов без определенного окончания, который не может быть остановлен и продолжен снова пользователем или оператором без фальсификации результата измерений

Примечание 1: Примеры включают: а) автоматическое средство измерений для взвешивания с непрерывным суммированием, б) счетчик тепла.

Примечание 2: См. также прерываемое измерение с накоплением результатов (3.1.23).

3.1.43 Защитный интерфейс (protective interface)

Законодательно контролируемый программный модуль, который обрабатывает весь поток данных, поступающих в законодательно контролируемую часть программного обеспечения для предотвращения недопустимых воздействий.

3.1.44 Опечатывание (sealing)

Средства для защиты средства измерений от любой несанкционированной модификации, перенастройки, удаления частей, программного обеспечения и т.д.

Примечание: Может производиться аппаратными средствами, программным обеспечением или их сочетанием.

[OIML V 1:2013, 2.20]

3.1.45 Защита (securing)

Предотвращение несанкционированного доступа к аппаратному или программному обеспечению.

3.1.46 Существенный дефект (significant defect)

Нежелательное событие, влияющее на соответствие измерительного прибора, или неисправность.

Примечание: Примеры существенных дефектов включают: а) удаление контрольного журнала; б) несанкционированные изменения параметров; в) несанкционированные обновления.

3.1.47 Экспертиза программного обеспечения (software examination)

Техническая операция, которая состоит из определения одной или более характеристик программного обеспечения в соответствии с определенной процедурой (например, анализ технической документации или запуск программы в контролируемых условиях).

3.1.48 Идентификация программного обеспечения (software identification)

Последовательность удобочитаемых символов (например, номер версии, контрольная сумма), неразрывно связанных с рассматриваемым программным обеспечением или программным модулем.

Примечание: Может быть проверена во время работы средства измерений.

3.1.49 Интерфейс программного обеспечения (software interface)

Программный код и выделенная область данных, приём, фильтрация или передача данных между программными модулями.

Примечание 1: Программный интерфейс не обязательно является законодательно значимым.

Примечание 2: Программный интерфейс – это интерфейс между двумя или более программными модулями, используемый для обмена данными и передачи команд.

[OIML V 1:2013, 6.03]

3.1.50 Программный модуль (software module)

Программные объекты, такие как программы, подпрограммы, библиотеки, показатель, набор данных и другие объекты, включая их области данных, которые могут быть связаны с другими объектами.

Примечание: Программное обеспечения средств измерений, электронных устройств или подузлов состоят из одного или более программных модулей.

3.1.51 Защита программного обеспечения (software protection)

Защита программного обеспечения средств измерений или области данных опечатыванием аппаратными или программными средствами.

Примечание: Такую печать необходимо снять, повредить или взломать, чтобы получить доступ и изменить программного обеспечения.

[OIML V 1:2013, 6.04]

3.1.52 Разделение программного обеспечения (software separation)

Разделение программного обеспечения в средствах измерений, которое может быть разделено на законодательно значимую часть и законодательно незначимую часть.

Примечание: Эти части связываются через интерфейс программного обеспечения.

[OIML V 1:2013, 6.02]

3.1.53 Исходный код (source code)

Компьютерная программа, написанная в удобочитаемой и редактируемой форме (на языке программирования).

Примечание: Исходный текст компилируется или преобразуется в исполняемый код.

3.1.54 Устройство хранения (storage device)

Место хранения, используемое чтобы сохранить данные измерения в готовом виде после завершения измерения для последующих законодательно значимых целей (например, заключения коммерческой сделки).

[OIML V 1:2013, 6.07]

3.1.55 Метка времени (time stamp)

Уникальное значение, например, в секундах или строка даты и времени, обозначающая дату и/или время, в которое произошел определенный инцидент (событие или измерение).

3.1.56 Передача данных измерения (transmission of measurement data)

Передача данных измерения с помощью сетей связи или других средств на удаленное электронное устройство, где они подвергаются дальнейшей обработке.

3.1.57 Оценка типа (образца) [type (pattern) evaluation]

Процедура оценки соответствия одного или нескольких образцов определенного типа средств измерений, результатом которой является протокол оценки или сертификат.

[OIML V 1:2013, 2.04]

3.1.58 Параметр, зависящий от типа средства измерений (type-specific parameter)

Законодательно значимый параметр, значение которого зависит только от типа средства измерений.

Примечание: Параметры, зависящие от типа - часть юридически значимого программного обеспечения.

[OIML V 1: 2013, 2.44]

Пример: В системе измерения расхода жидкостей (кроме воды), диапазон кинематической вязкости турбины – это параметр, зависящий от типа и установленный при утверждении типа турбины. Все турбины одного типа имеют одинаковый диапазон вязкости.

3.1.59 Универсальное устройство (universal device)

Устройство, которое не сконструировано для определенной цели, но которое может быть адаптировано к метрологической задаче с помощью программного обеспечения

Примечание: Обычно такое программное обеспечение основано на операционной системе, которая позволяет загружать и выполнять программное обеспечение для определенных целей.

3.1.60 Пользовательский интерфейс (user interface)

Интерфейс, обеспечивающий обмен информацией между пользователем и средством измерения или его аппаратными компонентами, или программными модулями.

Примечание: Типичными примерами пользовательских интерфейсов являются переключатели, клавиатура, мышь, дисплей, монитор, принтер, сенсорный экран, программное окно на экране, включая программное обеспечение для его создания.

3.1.61 Поверка (verification)

Предоставление объективных доказательств того, что данный предмет соответствует установленным требованиям.

[OIML V 1: 2013, 2.44]

3.1.62 Поверка средств измерений (verification of a measuring instrument)

Процедура оценки соответствия средств измерений (отличная от оценки типа), результатом которой является нанесение проверочного клейма и/или выдача свидетельства о поверке.

Примечание: см. также OIML V 2-200:2012, 2.44

[OIML V 1: 2013, 2.09]

3.2 Сокращения

EUT Тестируемое оборудование
IEC (МЭК) Международная электротехническая комиссия
ISO (ИСО) Международная организация по стандартизации
IT Информационная технология
MPE Максимальная допустимая погрешность
OIML (МОЗМ) Международная Организация Законодательной Метрологии
PG Проектная Группа

4 Инструкции по использованию настоящего Документа при составлении Рекомендаций МОЗМ

4.1 Положения данного Документа применимы только к новым Рекомендациям МОЗМ и пересматриваемым Документам МОЗМ. Проектные Группы МОЗМ (Технические комитеты и Подкомитеты) должны использовать этот руководящий Документ для определения требований к программному обеспечению в дополнение к другим техническим и метрологическим требованиям их применимых Рекомендаций МОЗМ.

4.2 Все упомянутые документы подлежат пересмотру, и пользователям данного Документа предлагается рассмотреть возможность применения последних редакций упомянутых документов.

4.3 Цель данного Документа состоит в том, чтобы предоставить Проектным Группам, отвечающим за составление Рекомендаций МОЗМ, ряд требований – частично разных (рисковых) уровней – которые могут распространяться на любые средства измерений и все области их применения. Проектные Группы должны определить, какой уровень риска является подходящим, и как включить соответствующие части данного документа в составляемую Рекомендацию МОЗМ. В Разделе 5 предложены некоторые вспомогательные средства для выполнения этой задачи.

4.4 Проектным группам (PGs) следует определить, какое влияние считается недопустимым для конкретных типов приборов.

4.5 Проектным группам (PGs) следует определить, какие данные, касающиеся измерений, должны соответствовать требованиям. При необходимости изготовитель документирует требуемые метаданные.

5 Оценка рисков

5.1 Данное положение предназначено в качестве руководства для определения набора уровней риска, которые должны обычно применяться для испытаний, проводимых на программно-управляемых средствах измерений. Он не предназначен в качестве классификации со строгими ограничениями, ведущими к специальным требованиям, как в случае классификации точности.

5.2 Более того, настоящий Документ не ограничивает Проектные Группы в преставлении оценок риска, отличающихся от тех, которые вытекают из рекомендаций, изложенных в настоящем Документе. Могут использоваться различные уровни риска в соответствии со специальными ограничениями, предписанными в соответствующих Рекомендациях.

5.3 При выборе уровней риска для конкретной категории инструментов и области применения (торговля, прямая продажа населения, здравоохранение, правоохранительные органы и т.д.) можно принять во внимание следующие аспекты:

a) риск мошенничества:

- последствия, а также социальное и общественное влияние неисправностей;
- стоимость товара, подлежащего измерению;
- используемая платформа (встроенные или универсальные устройства);
- подверженность источникам потенциального мошенничества (устройства самообслуживания без присмотра).

b) требуемое соответствие:

- практические возможности отрасли по соблюдению установленного уровня.

c) требуемой надежности:

- условия окружающей среды;
- последствия и влияния ошибок на общество и социальную сферу.

d) мотивация мошенника.

e) возможность повторить измерение или прервать его.

Проектные группы должны учитывать стандарты оценки риска при определении уровня риска, например, ISO/IEC 27005 [10].

Во всех пунктах требований (см.6) приводятся различные примеры приемлемых технических решений, иллюстрирующих базовый уровень защиты от мошенничества, соответствия, надежности и типа измерения (обозначены (I)). Там, где это уместно, также представлены примеры с усиленными контрмерами, которые учитывают повышенные уровень риска вышеописанных аспектов [обозначены (II)]

Уровень экспертизы и уровень риска связаны между собой. Глубокий анализ программного обеспечения должен проводиться, когда требуется повышенный уровень риска, чтобы обнаружить недостатки программного обеспечения или уязвимости безопасности. С другой стороны, механическая герметизация (например, герметизация коммуникационного порта или корпуса) должна учитываться при выборе уровня экспертизы.

6 Требования к средствам измерений в отношении применения программного обеспечения

6.1 Общие требования

На момент публикации данного Документа эти общие требования представляют современный уровень развития информационной технологии (IT). Они в принципе применимы ко всем видам программно-управляемых средств измерений и компонентов средств измерений. Они должны приниматься во внимание во всех Рекомендациях. В отличие от этих общих требований, требования для определенной конфигурации (6.2) относятся к техническим особенностям, которые не характерны для некоторых видов СИ или некоторых областей применения.

В примерах, где это используется, показан как нормальный, так и повышенный уровни жесткости (severity) испытаний. В данном Документе используется следующая система обозначений:

(I) Техническое решение, приемлемое при нормальном уровне риска;

(II) Техническое решение, приемлемое при повышенном уровне риска (см. 5).

6.1.1 Идентификация программного обеспечения

Программное обеспечения средства измерений / электронного устройства / компонента должно четко идентифицироваться по версии программного обеспечения или другому обозначению. Идентификационное обозначение может состоять из более чем одной части, но, как минимум, одна часть должна быть выделена для законодательных целей.

Идентификация программного обеспечения должна отображаться или печататься средством измерений:

- по команде; или
- во время эксплуатации; или
- при запуске средства измерений, который можно выключать и включать снова.

Если у средства измерений/компонента нет дисплея или принтера, обозначение должно быть направлено через интерфейс связи и показано/напечатано на другом компоненте.

В виде исключения приемлемым решением может быть распечатка идентификации программного обеспечения на приборе/электронном устройстве, если удовлетворены следующие условия:

(a) У интерфейса пользователя нет никакой возможности управления, чтобы активировать индикацию обозначения программного обеспечения на дисплее, или дисплей технически не позволяет отображать идентификацию программного обеспечения (аналоговое индикаторное устройство или электромеханический счетчик).

(b) Средство измерений/компонент не имеет интерфейса, чтобы передать информацию об идентификации программного обеспечения.

(c) После изготовления средства измерений/компонента изменение программного обеспечения невозможно, или возможно только при изменении аппаратной части или компонента аппаратной части.

Изготовитель аппаратной части или соответствующего компонента аппаратной части несет ответственность за то, чтобы обеспечить правильное указание идентификации программного обеспечения на соответствующем средстве измерений / компоненте.

Соответствующая Рекомендация должна разрешать или не разрешать данное исключение.

Если программное обеспечение каким-либо образом было модифицировано, требуется новая идентификация программного обеспечения.

Идентификация программного обеспечения и средства идентификации (например, версия программного обеспечения, хэш значение, контрольная сумма, CRC) должны быть указаны в сертификате. Инструкции, как отобразить или распечатать идентификацию программного обеспечения, должны содержаться в сертификате.

Примечание 1: Каждое используемое средство измерений должно соответствовать утвержденному типу. Идентификация программного обеспечения позволяет сотрудникам органов надзора и лицам, связанным с измерением, определять, соответствует ли данное средство измерений требованиям.

Примечание 2: Если не указано иное, термин «сертификат» означает МОЗМ сертификат освидетельствования типа.

Пример:

(I) Программное обеспечение содержит текстовую переменную или число, однозначно идентифицирующее инсталлированную версию. Эта переменная передается на дисплей средства измерений при нажатии кнопки, когда средство включено, или периодически контролируется с помощью таймера.

Номер версии может иметь следующую структуру: A.Y.Z. Принимая во внимание, что если рассматривается сумматор потока, то буква A обозначает версию базового программного обеспечения, считающего импульсы, буква Y обозначает версию функции преобразования («нет», «при 15 °C», «при 20 °C»), а буква Z обозначает язык интерфейса пользователя.

(II) Программное обеспечение рассчитывает контрольную сумму исполняемого кода и представляет результат как идентификацию вместо или в дополнение к переменной в (I).

6.1.2 Правильность алгоритмов и функций

Алгоритмы измерений и функции средства измерений должны соответствовать и быть функционально правильными для данного приложения и типа устройства (точность алгоритмов, расчет цены по определенным правилам, алгоритмы округления и т.д.).

Результат измерения и сопровождающая информация, требуемая конкретными Рекомендациями или национальным законодательством, должны быть правильно показаны или напечатаны.

Должна быть предусмотрена возможность проверки алгоритмов и функций либо с помощью метрологических тестов, тестов программного обеспечения, либо экспертизы программного обеспечения (как описано в 7.3).

Не должно быть никаких скрытых или недокументированных функций, или параметров.

6.1.3 Защита программного обеспечения

6.1.3.1 Предотвращение злоупотреблений

Средство измерений должно быть сконструировано таким образом, чтобы свести к минимуму возможность неумышленного, случайного или преднамеренного неправильного применения. В структуре данного Документа МОЗМ это относится особенно к программному обеспечению. Представление результатов измерения должно быть однозначным для всех участвующих сторон.

Примечание: Программно-управляемые средства измерений зачастую имеют сложный набор функциональных возможностей. Пользователю необходимо качественное руководство по правильному использованию и по получению правильных результатов измерения.

Пример:

Пользователь руководствуется меню. Законодательно значимые функции объединены в одну ветвь такого меню. Если какие-либо значения измерения могут быть потеряны при выполнении какого-либо действия, пользователя следует предупредить и попросить его выполнить другое действие прежде, чем будет выполнена данная функция. См. также 6.2.2.

6.1.3.2 Доказательство вмешательства

6.1.3.2.1 Программное обеспечение должно быть защищено таким образом, чтобы были доступны доказательства любого вмешательства (например, обновления программного обеспечения, изменения параметров). Программное обеспечение должно быть защищено от несанкционированной модификации, загрузки или внесения изменений путем замены запоминающего устройства. Для закрепления средств измерений может потребоваться механическое опломбирование или другие технические средства. Контрольные журналы считаются частью законодательно контролируемого программного обеспечения и должны быть защищены.

Пример:

(I) Измерительная система состоит из двух компонентов, один из которых содержит основные метрологические функции и заключен в корпус, который может быть опечатан. Другой компонент представляет собой универсальный компьютер с операционной системой. Некоторые функции, такие как индикация, находятся в программном обеспечении данного компьютера. Чтобы предотвратить замену программного обеспечения на универсальном устройстве, передача данных измерений между компонентом и универсальным устройством зашифрована. Ключ для декодирования скрыт в программе, которая является частью законодательно значимого программного обеспечения универсального устройства. Только эта программа знает ключ и способна прочитать, декодировать и использовать результаты измерений. Другие программы не могут использоваться для этой цели, поскольку они не могут декодировать результаты измерений (см. также пример в 6.2.2.2.4).

(I) / (II) Корпус, содержащий устройства памяти, опечатывается или устройство памяти опечатывается на печатной плате (PCB).

(II) Если используется устройство для многократной перезаписи, ввод разрешения записи блокируется переключателем, который может быть опечатан. Электрическая схема разрабатывается таким образом, чтобы защита от записи не могла быть отменена при коротком замыкании контактов.

6.1.3.2.2 Интерфейс пользователя (см. 7.1), может активировать только функции, точно указанные в документации, которые не влияют на метрологические характеристики прибора.

Примечание: Эксперт решает, приемлемы ли все указанные в документации команды.

Пример:

(I) / (II) Все входные сигналы с интерфейса пользователя переадресуются программе, фильтрующей поступающие команды. Она допускает и пропускает только те команды, которые указаны в документации, и отбрасывает все другие. Эта программа или программный модуль является частью законодательно значимого программного обеспечения.

6.1.3.2.3 Параметры, которые устанавливают законодательно значимые характеристики средства измерений, должны быть защищены от изменения. Если это необходимо для проверки, то должна быть обеспечена возможность отображения или печати текущей установки параметров.

Примечание 1: Параметры, определяющее конкретное средство измерений, могут настраиваться или выбираться после оценки типа. Они должны регулироваться/выбираться только в специальном рабочем режиме средства измерений.

Примечание 2: Параметры, определяющее конкретное средство измерений, могут настраиваться или выбираться только в специальном рабочем режиме средства измерений. Их можно разделить на параметры, которые должны быть защищены (оставаться неизменными) и те, к которым может получить доступ уполномоченное лицо, например, владелец средства измерений или продавец продукта.

Примечание 3: Параметры, определяющие тип средств измерений, имеют идентичные значения для всех приборов данного типа. Они фиксируются в свидетельстве об утверждении ти законодательно па данного средства измерений.

Пример:

(I) / (II) Параметры конкретного средства измерений, которые защищены, хранятся в энергонезависимой памяти. Разрешение на запись в память блокируется переключателем, который может быть опечатан.
См. примеры 6.1.3.2.4 (1) к (3) в этом пункте.

6.1.3.2.4 Защита программного обеспечения включает соответствующее опечатывание механическими, электронными и/или криптографическими средствами, что делает невозможным или очевидным несанкционированное вмешательство

Примечание: Может использоваться криптографический сертификат. Программное обеспечение должно быть подписано надежным учреждением, имеющим электронную подпись. Подлинность подписанного программного обеспечения может быть проверена с помощью открытого ключа надежного учреждения и расшифровки подписи сертификата.

Пример:

1) (I) Электронное опечатывание. Законодательно значимые параметры средств измерений могут вводиться и настраиваться с помощью пункта меню. Программного обеспечения распознает каждое изменение и с каждым событием данного вида увеличивает отсчет на счетчике событий. Это значение счетчика событий может быть отображено. Первоначальное показание счетчика событий должно быть зарегистрировано. Если отображенное значение отличается от зарегистрированного, средства измерений находится в непроверенном состоянии (равнозначно сорванной пломбе).

2) (I) / (II) Программное обеспечение средства измерений разработано так (см. Пример 6.1.3.2.1), что нет никакой возможности модифицировать параметры и законодательно значимую конфигурацию, кроме как с помощью меню, защищенного переключателем. Такой переключатель механически опечатан в неактивном положении, не допуская изменения параметров и юридически значимой конфигурации.

Чтобы изменить параметры и конфигурацию, переключатель следует переключить, при этом пломба будет неизбежно сорвана.

3) (II) Программное обеспечение средства измерений разработано так, что нет никакой возможности получить доступ к параметрам и законодательно значимой конфигурации ни для кого, кроме уполномоченных лиц. Если кто-то хочет войти в пункт меню параметра, он должен вставить свою смарт-карту, содержащую ПИН как часть криптографического сертификата. Программное обеспечение средства измерений может проверить подлинность ПИН по сертификату и позволить ввести пункт меню параметра. Доступ регистрируется в журнале контроля, включая идентификацию личности (или, по крайней мере, используемой смарт-карты).

6.1.4 Поддержка аппаратных средств

6.1.4.1 Выявление существенных неисправностей

Соответствующая Рекомендация может потребовать наличия функций выявления существенных дефектов. В этом случае изготовитель средства измерений обязан ввести в программное обеспечение или в аппаратную часть средства проверки, или обеспечить наличие средств, которыми аппаратные средства могут поддерживаться программной частью средства измерений.

Если программное обеспечение задействовано в обнаружении неисправности, от него требуется соответствующая реакция. Например, соответствующая Рекомендация может предписывать, что в случае выявления неисправности, средство измерений / компонент должно быть выключено, либо должен прозвучать сигнал тревоги / сделана запись в журнале регистрации ошибок.

Документация, предоставляемая для оценки типа, должна содержать список существенных неисправностей, распознаваемых программным обеспечением и ожидаемой реакции программного обеспечения, а также, если это нужно для понимания, описание алгоритма распознавания неисправностей.

Пример:

(I) При каждом запуске законодательно значимая программа рассчитывает контрольную сумму для кода программы и юридически значимых параметров. Номинальное значение этих контрольных сумм рассчитывается заранее и сохраняется в данном средстве измерений. Если рассчитанные и сохраненные значения не соответствуют друг другу, программа останавливает работу.

В случае непрерываемого совокупного измерения, контрольная сумма рассчитывается периодически и контролируется таймером программного обеспечения. В случае выявления отказа, программное обеспечение отображает сообщение об ошибке или включает индикатор отказа и записывает время ошибки в журнале регистрации ошибок.

(II) При каждом запуске законодательно контролируемая часть программного обеспечения определяет значение криптографической хэш-функции программного кода и законодательно контролируемых параметров. Номинальное значение хэша было рассчитано заранее и сохранено в приборе. Если вычисленные и сохраненные значения не совпадают, программа перестает действовать.

В случае непрерываемого измерения с накоплением результатов, значение хэша вычисляется циклически и контролируется программным таймером. В случае обнаружения сбоя программное обеспечение сообщает об ошибке или включает индикатор сбоя и записывает время существенного дефекта в файл регистрации ошибок.

6.1.4.2 Поддержка работоспособности

Производитель по своему выбору может реализовать средства поддержки работоспособности, описанные в OIML D 11:2013 [2] (5.1.3 (b) и 5.4), программными или аппаратными средствами, или позволить, чтобы аппаратные средства поддерживались программным обеспечением. Приемлемые решения могут быть предложены в соответствующей Рекомендации.

Если программное обеспечение участвует в защите работоспособности, от него требуется соответствующая реакция. Например, Рекомендация может предписывать, чтобы - в случае опасности для работоспособности – средства измерений/ компонента либо выключалось, либо генерировался сигнал тревоги / соответствующее сообщение.

Пример:

(I) / (II) Некоторые виды средств измерений требуют настройки после установленного интервала времени для гарантии работоспособности и устойчивости измерений. Программное обеспечение генерирует предупреждение по истечении этого интервала между циклами техобслуживания и даже останавливает измерения, если их количество для определенного интервала времени было превышено.

6.1.5 Метка времени

Метка времени должна иметь согласованный формат, позволяющий легко сравнивать две разные записи и отслеживать прогресс с течением времени.

Метка времени должна считываться с часов устройства. В зависимости от вида средства измерений или области приложения, установка часов может быть законодательно значимой и должны быть предприняты соответствующие меры защиты в зависимости от применяемого уровня жесткости (см. 6.1.3.2.3).

Внутренние часы автономного средства измерений обычно имеют довольно большую погрешность, поскольку нет возможности синхронизировать их во всемирным координированным временем (UTC). В тех случаях, когда конкретная область применения требует высокоточной информации о точном времени измерения, может потребоваться повысить надежность внутренних часов с помощью специальных средств.

При необходимости проектные группы могут устанавливать требования и методы тестирования внутренних часов.

Пример:

(II) Надежность внутренних кварцевых часов средства измерений увеличена за счет избыточности: таймер увеличивает значение с помощью часов микроконтроллера, полученного из другого кварцевого кристалла. Когда значение таймера достигает ранее заданного значения, например, 1 секунда, устанавливается определенный флажок микроконтроллера, и законодательно значимая часть программного обеспечения обработки прерывания увеличивает значение второго счетчика. По окончании, например, одного дня, программное обеспечение считывает значение кварцевых часов и вычисляет разницу в секундах, подсчитанную программным обеспечением. Если разница лежит в рамках ранее заранее заданных пределов, программный счетчик перезагружается, и процедура повторяется; но если разница выходит за эти пределы, программное обеспечение выдает соответствующую реакцию на ошибку.

6.2 Требования, зависящие от конфигураций

6.2.1 Общие положения

Требования, приведенные в данном пункте, основаны на типичных технических решениях в области информационных технологий, хотя они могут не быть общепринятыми во всех областях законодательного применения. Соблюдение этих требований дает возможность реализации таких технических решений, которые имеют ту же степень защиты и соответствия типу, как и программно-управляемые средства измерений.

Следующие специальные требования необходимы, если в измерительных системах используются определенные средства измерений. Их следует принимать во внимание в дополнение к требованиям, описанным в 6.1.

В примерах, где это применимо, показаны как обычные, так повышенные уровни риска испытаний. В этом документе используются следующие обозначения:

(I) Техническое решение, приемлемое при нормальном уровне риска испытаний;

(II) Техническое решение, приемлемое при повышенном уровне риска (см. 5).

6.2.2 Спецификация и разделение законодательно значимых частей, и спецификация интерфейсов

Это требование применяется, если средство измерений /компонент, кроме законодательно важных частей внутри средства измерений /компонента, имеет интерфейсы для связи с другими электронными устройствами, с пользователем, или с другими частями программного обеспечения.

Законодательно значимые части средства измерений, будь то программные или аппаратные части, не должны подвергаться недопустимому влиянию других частей средства измерений.

В рекомендациях может быть указано программное обеспечение/аппаратное обеспечение/данные или часть программного обеспечения /аппаратного обеспечения/данных, которые имеют законодательно значение.

6.2.2.1 Разделение комплектующих

6.2.2.1.1 Комплектующие средства измерений, выполняющие законодательно значимые функции, должны быть идентифицированы, четко определены и документированы. Они представляют законодательно значимую часть средства измерений.

Примечание: Эксперт решает, является ли эта часть полной и можно ли исключить из дальнейшей оценки другие части средства измерений.

Примеры:

(1) (I) / (II) Счетчик электроэнергии оборудован оптическим интерфейсом для подключения электронного устройства, чтобы считывать измеренные результаты. Счетчик сохраняет все соответствующие результаты и обеспечивает доступ для считывания значений в течение достаточного временного диапазона. В этой системе законодательно значимым устройством является только счетчик электроэнергии. Другие законодательно незначимые устройства могут присутствовать и быть связаны с интерфейсом средства измерений, если соблюдается требование 6.2.2.1.2. Защита самой передачи данных (см. 6.2.5) не требуется.

(2) (I) / (II) Измерительная система состоит из следующих компонентов:

- цифровой датчик, рассчитывающий массу или объем;

- универсальное устройство, рассчитывающее цену;

- принтер, распечатывающий значение измерения и цену к оплате.

Все комплектующие связаны локальной сетью. В этом случае цифровой датчик, универсальное устройство и принтер являются законодательно значимыми комплектующими и могут быть при желании связаны с системой управления товарными запасами, которая не является юридически значимой. Законодательно значимые комплектующие должны соответствовать требованию 6.2.2.1.2 и – в силу передачи по сети - также требованиям, содержащимся в 6.2.5.

6.2.2.1.2 Следует продемонстрировать, что значимые функции и данные подузлов и электронных устройств не могут подвергаться недопустимому влиянию команд, получаемых через интерфейс.

Это означает однозначное назначение каждой команды по отношению ко всем инициированным функциям или изменениям данных в подузле или электронном устройстве.

Примечание: Если «законодательно значимые» комплектующие взаимодействуют с другими «законодательно значимыми» комплектующими, см. 6.2.5.

Пример:

(I) / (II) Программное обеспечение счетчика электроэнергии (см. пример (1) в 6.2.2.1.1.a выше) способно получать команды для выбора требуемых величин. Оно отправляет результат измерений (включая дополнительную информацию, связанную – например, меткой времени, единицей измерений) и отсылает данный массив данных обратно на запрашивающее устройство. Программное обеспечение принимает только команды для выбора действующих позволенных величин и отбрасывает любые другие команды, отправляя сообщение об ошибке. Могут присутствовать средства защиты содержания массива данных, но они не требуются, поскольку передаваемый массив данных не подлежит законодательному контролю.

(I) / (II) Внутри корпуса, который опечатывается, имеется переключатель, который определяет режим работы счетчика электроэнергии: одна установка переключателя обозначает защищенный режим, а другая - свободный режим (возможны средства защиты помимо механического опечатывания; см. примеры 6.1.3.2.1 и 6.1.3.2.4). При интерпретации полученных команд программное обеспечение проверяет положение переключателя: в свободном режиме набор принимаемых программным обеспечением команд может быть расширен по сравнению с защищенным режимом, описанным выше; например, можно настроить коэффициент калибровки с помощью команды, которая не принимается в проверяемом режиме.

6.2.2.2 Определение и разделение частей программного обеспечения

6.2.2.2.1 Все программные модули (программы, подпрограммы, объекты и т.д.), которые выполняют законодательно значимые функции или содержат законодательно значимые измерительные данные, являются законодательно значимой частью программного обеспечения средства измерений / компонента. К этой части применяется требование соответствия, и эта часть должна быть идентифицируемой, как описано в 6.1.1.

Если разделение программного обеспечения невозможно или не требуется, программное обеспечение в целом является законодательно значимым.

Пример:

(I) Средство измерений состоит из нескольких цифровых датчиков, связанных с персональным компьютером, который отображает измеренные значения. Законодательно значимая часть программного обеспечения на персональном компьютере отделяется от законодательно незначимых частей путем трансляции (компиляции) всех процедур, реализующих законодательно значимые функции (включая представление результатов) в динамически компонуемую библиотеку. Функции в этой библиотеке могут вызывать одно или несколько законодательно незначимых приложений. Эти функции получают измеренные данные с цифровых датчиков, рассчитывают результат измерения и отображают его в окне программного обеспечения.

6.2.2.2.2 Если законодательно значимая часть программного обеспечения связывается с другими частями программного обеспечения, должен быть определен интерфейс программного обеспечения. Вся связь должна осуществляться исключительно через данный интерфейс. Законодательно значимая часть программного обеспечения и интерфейс должны быть четко документированы. Все законодательно значимые функции и области данных программного обеспечения должны быть описаны, чтобы органу, осуществляющему оценку типа, принять правильное решение о разделении программного обеспечения.

Интерфейс программного обеспечения состоит из программного кода и выделенных областей данных. Части программного обеспечения обмениваются определенными закодированными командами или данными, одна часть программного обеспечения сохраняет их в выделенной области данных, а другая считывает их оттуда. Код программы записи и считывания является частью интерфейса программного обеспечения.

Примечание: Защита от прерываний (задержка выполнения или блокировка другими процессами) рассматривается в разделе 6.2.2.2.4.

Пример:

(I) В примерах 6.2.2.2.1 и 6.2.2.2.3 законодательно незначимое приложение управляет запуском законодательно значимых процедур в библиотеке. Игнорирование этих процедур очевидно препятствует выполнению законодательно значимых функции системы. В этой связи система, приведенная в примере, предусматривает, что: Цифровые датчики отправляют данные измерений в зашифрованном виде. Ключ для расшифровки спрятан в библиотеке. Только процедуры в библиотеке знают ключ и могут считывать, расшифровывать данные измерений и отображать результаты измерений.

6.2.2.2.3 В законодательно значимой части программного обеспечения должно быть осуществлено однозначное назначение каждой команды для всех инициируемых функций или данных изменений. Функции, которые запускаются через интерфейс программного обеспечения, должны быть задекларированы и документированы. Только функции, указанные в документации, могут быть активированы через интерфейс программного обеспечения.

Пример:

(I) В примере, описанном в разделе 6.2.2.2.1, программный интерфейс состоит из процедур в библиотеке, их параметров и возвращаемых значений. Интерфейс нельзя обойти, например, посредством ссылки на внутренние данные. Количество и вид процедур, параметры, и возвращаемые значения фиксируются во время компиляции.

(II) Законодательно значимые и законодательно незначимые части программного обеспечения управляются разными виртуальными механизмами одного универсального устройства. Оба механизма конфигурированы таким образом, что любая связь между обеими программными частями может осуществляться только через определенный программный интерфейс. Настройка виртуальных механизмов, включая способ связи между ними, является частью законодательно контролируемого программного обеспечения. Операционная система гарантирует, что конфигурация не может быть изменена без нарушения пломбы.

6.2.2.2.4 Если законодательно значимое программное обеспечение было отделено от незначимой части программного обеспечения, у законодательно значимого программного обеспечения должен быть приоритет по сравнению с незначимым программным обеспечением. Не допускается прерывание законодательно значимого процесса законодательно не относящимся к делу программного обеспечения. Процесс измерения (реализуемый законодательно значимой частью программного обеспечения) не должен быть отложен или заблокирован другими процессами.

Пример:

(I) Уровень приоритета присваивается законодательно значимым функции, более высокий по сравнению с функцией для обычных процессов, который не может быть понижен пользователем/оператором измерительного прибора.

(I) ПО электронного счетчика электроэнергии считывает необработанные значения измерения с аналогово-цифрового конвертера (ADC). Для правильного расчета измеренного результата решающее значение имеет задержка между событием «данные готовы» в ADC до окончания буферизации значений измерения. Необработанные значения считываются программой обработки прерывания, запущенной сигналом «данные готовы». СИ может связываться через интерфейс с другими электронными устройствами, параллельно обслуживаемыми другой программой обработки прерываний (законодательно незначимая связь). Приоритет программы обработки прерываний для обработки значений измерения должен быть выше приоритета программы связи.

(III) Законодательно значимые и законодательно незначимые части программного обеспечения управляются разными виртуальными механизмами одного универсального устройства. Конфигурация операционной системы гарантирует, что виртуальный механизм управления законодательно значимой частью программного обеспечения всегда имеет достаточные системные ресурсы, доступные для законодательно значимых процессов.

Примеры с 6.2.2.2.1, 6.2.2.2.2, 6.2.2.2.3 (I) по 6.2.2.2.4 1)/2)(I) приемлемы как техническое решение только для обычного уровня риска (I). Если необходима повышенная защита от мошенничества или повышенная степень соответствия (см. 8), не достаточно только одного разделения программного обеспечения, и требуются дополнительные средства либо все программные обеспечения в целом должно рассматриваться как попадающее под правовое регулирование.

6.2.3 Совместно используемые индикаторы

Для предоставления как информации от законодательно значимой части программного обеспечения, так и другой информации могут использоваться дисплей или распечатка. Их содержание и формат характерны для данного вида средств измерений и области приложения и должны быть определены в соответствующей Рекомендации. Если дисплей или распечатка используются как для законодательно значимых, так и для законодательно незначимых выходных данных, юридически значимая информация всегда должна быть читаемой и четко отличимой от другой информации.

Пример:

(I) В средствах измерений, описанных в примерах 6.2.2.2.1 – 6.2.2.2.4, результаты измерения отображаются в отдельном окне программного обеспечения. Средства, описанные в 6.2.2.2.4, гарантируют, что только законодательно значимая часть программного обеспечения может прочитать и отобразить результат измерения. Прибор оснащен операционной системой с многооконным интерфейсом с несколькими окнами. Окно, отображающее законодательно значимые данные, генерируется и контролируется в соответствии с процедурами в законодательно значимой динамически компонуемой библиотеке (см. 6.2.2.2). Во время измерения эти процедуры циклически проверяют, что соответствующее окно все еще находится поверх всех других открытых окон; в противном случае процедуры помещают его поверх остальных.

(II) В измерительном приборе, описанном в примерах 6.2.2.2.1-6.2.2.2.4, приложение для измерений работает в режиме киоска. Весь дисплей управляется законодательно значимой частью программного обеспечения. Законодательно незначимые данные представлены в специальной части дисплея, помеченные как законодательно незначимые.

Если необходима повышенная защита от мошенничества (II), неприемлемо использовать только распечатку в качестве индикации, а также должны быть рассмотрены дополнительные меры предосторожности в виде аппаратного и/или программного обеспечения. Требуется наличие компонента со средствами повышенной защиты, который может отобразить значения измерения.

6.2.4 Хранение данных

6.2.4.1 Общие положения

Если данные измерений сохраняются для использования в законодательно значимых целях, применяются требования пунктов 6.2.4.2-6.2.4.4.

Проектные группы могут выбрать подходящие условия сохранения в зависимости от применения данных.

6.2.4.2 Полнота хранимых данных

Сохраненное или переданное значение измерения должно сопровождаться всей значимой информацией, необходимой для будущего юридически значимого использования.

Пример:

(I) / (II) Сохраненный набор данных результатов измерений может включать следующие записи:

- **значение измерения, включая единицу измерения;**
- **отметку времени измерения (см. 6.1.5);**
- **место измерения или идентификацию СИ, которое использовалось для измерения;**
- **однозначную идентификацию измерения, например, последовательные числа, позволяющие осуществлять назначение значений, напечатанных в счете.**

6.2.4.3 Защита хранимых данных

Сохраненные данные измерений должны быть защищены средствами программного обеспечения, чтобы гарантировать подлинность, целостность и, при необходимости, правильность информации в отношении времени измерения. Программное обеспечение, которое отображает или проводит дальнейшую обработку данных измерений и сопровождающих данные или результат измерений, должно проверить время измерения, подлинность и целостность данных, после считывания их с небезопасного места хранения или получения их из хранилища. Если обнаружена неисправность, данные должны быть отброшены или помечены, как непригодные.

Программные модули, которые готовят данные для хранения или проверяют данные после считывания, относятся к законодательно значимой части программного обеспечения.

Примечание: Целесообразно требовать повышенного уровня риска при рассмотрении вопроса о свободном доступе к хранилищу.

Повышенный уровень риска может потребовать применения криптографических методов. При необходимости должны быть предусмотрены средства, благодаря которым криптографические ключи могут вводиться или считываться только в том случае, если защита оказывается взломанной. Пример (I) относится к локальной памяти, а пример (II) относится к свободно доступной памяти.

Пример:

(I) Программа хранящего устройства рассчитывает контрольную сумму CRC32 набора данных, и прилагает ее к набору данных. Она использует секретное начальное значение для данного вычисления вместо значения, приводимого в стандарте. Это начальное значение используется как ключ и сохраняется как константа в программном коде. Программа чтения также сохраняет это начальное значение в своем программном коде. Прежде чем использовать набор данных, программа чтения рассчитывает контрольную сумму и сравнивает ее с контрольной суммой, сохраненной в наборе данных. Если оба значения совпадают, набор данных не был сфальсифицирован. В противном случае программа считает, что произошла фальсификация и отбрасывает этот набор данных.

(II) Программа хранения, которая является частью законодательно значимого программного обеспечения, генерирует электронную подпись для сохраненного набора данных. Она прилагается к сохраняемому набору данных. Закрытый и открытый ключи, используемые для подписи, генерируются в аппаратном модуле безопасности, который защищает закрытый ключ от манипуляций или чтения и экспортирует открытый ключ. Программа чтения проверяет подпись с помощью открытого ключа, чтобы проверить подлинность и целостность набора данных. Чтобы доказать происхождение набора данных, программа чтения должна знать, действительно ли открытый ключ принадлежит программе хранения. Таким образом, открытый ключ отображается на дисплее измерительного прибора и может быть однократно зарегистрирован, например, вместе с заводским номером прибора при поверке на местах эксплуатации.

6.2.4.4 Автоматическое хранение

6.2.4.4.1 Когда для приложения требуется хранение данных, данные измерения должны автоматически сохраняться по завершении измерения, т.е. когда сгенерировано окончательное измерительное значение, используемое в законодательных целях.

Устройство хранения должно быть достаточно устойчивым, чтобы гарантировать, что при нормальных условиях хранения измерительные данные не будут искажены. Для любого конкретного приложения должно быть предназначено достаточно места в памяти.

Примечание 1: В случае измерений с накоплением результатов может случиться так, что одна и та же область данных (программная переменная) используется повторно. В этом случае запоминающее устройство может не быть законодательно обоснованным.

Примечание 2: Сохраненные данные не обязательно должны быть физически локализованы в одном блоке памяти, если соблюдаются все требования.

Примечание 3: РГ могут определять данные, последние значения которых должны быть сохранены.

6.2.4.4.2 Сохраненные данные могут быть удалены, если:

- транзакция произведена; или

- эти данные напечатаны печатным устройством, подлежащим правовому регулированию.

Примечание: Другие общие национальные правила (например, для налоговых целей) могут содержать строгие ограничения в отношении удаления сохраненных данных или результатов измерений. РГ может определять альтернативные условия для удаления данных.

6.2.5 Передача через системы связи

Если данные измерений передаются перед тем, как они используются для законодательно контролируемых целей, применяются следующие требования:

6.2.5.1 Полнота передаваемых данных

Передаваемые данные измерений должны сопровождаться всей соответствующей информацией, необходимой для последующего законодательно обоснованного использования.

Пример:

(I) / (II) Переданный набор данных по результатам измерений включает следующее:

- измеренное значение, включая единицу измерения;

- отметка времени измерения (см. 6.1.5);

- место проведения измерения или идентификация средства измерений используемого для измерения;

- однозначная идентификация измерения, например, последовательность чисел, позволяющая соотносить его с данными, напечатанными в чеке.

6.2.5.2 Защита передаваемых данных

Передаваемые данные должны быть защищены программными средствами, гарантирующими аутентичность, целостность и, при необходимости, правильность информации, касающейся времени измерения. Программное обеспечение, которое отображает или дополнительно обрабатывает данные измерений и сопутствующие данные, должно проверять время измерения, аутентичность и целостность данных, полученных по каналу передачи. В случае обнаружения несоответствия данные должны быть удалены или помечены как непригодные для использования.

Программные модули, которые подготавливают данные измерений для передачи или проверяют полученные данные измерений, относят к законодательно значимой части программного обеспечения.

Примечание: Для открытой сети требование о применении повышенного уровня риска является обоснованным.

Повышенный уровень риска может потребовать применения криптографических методов. Должны быть предусмотрены средства, благодаря которым криптографические ключи могут вводиться или считываться только в случае, если защита оказывается взломанной.

Примеры:

(I) Законодательно значимая часть программного обеспечения устройства, осуществляющего передачу данных, вычисляет сумму CRC32 набора данных и дополняет ею набор данных. Для этого расчета используется секретное первоначальное значение вместо значения, указанного в стандарте. Это первоначальное значение используется в качестве ключа и запоминается как некая постоянная в программном коде. Программа, являющаяся частью законодательно контролируемого программного обеспечения принимающего устройства, также сохраняет это первоначальное значение в своем программном коде. Перед использованием набора данных программа вычисляет контрольную сумму и сравнивает ее с суммой, хранящейся в наборе данных. Если оба значения совпадают между собой, то данный набор данных считается не фальсифицированным. В противном случае программа считает данные фальсифицированными и удаляет данный набор данных.

(II) Законодательно значимая часть программного обеспечения устройства, осуществляющего передачу данных, формирует электронную подпись для передаваемого набора данных, которая добавляется к переданному набору данных. Закрытый и открытый ключи, используемые для подписи, формируются в аппаратном модуле безопасности, который защищает закрытый ключ от манипуляций или чтения и передает открытый ключ. Программа, являющаяся частью законодательно значимого программного обеспечения принимающего устройства, проверяет подпись с помощью открытого ключа для проверки аутентичности и целостности набора данных. Чтобы проверить происхождение набора данных, принимающая программа должна знать, действительно ли открытый ключ принадлежит передающей программе. Поэтому открытый ключ воспроизводится на дисплее измерительного прибора и может быть однократно зарегистрирован, например, вместе с заводским номером прибора при его поверке на месте эксплуатации.

6.2.5.3 Задержка или прерывание передачи

Задержка или прерывание передачи данных не должны оказывать недопустимого влияния на процесс измерения. Если сетевые службы становятся недоступными или очень медленными, данные измерений не должны быть потеряны. Во избежание потерь данных процесс измерения может быть остановлен. Проектной группе следует определить соответствующие требования и механизмы, обеспечивающие сохранение измерительных данных в случае возможных перебоев в передаче данных в процессе применения средства измерений

Примечание 1: Следует учитывать различие между статическими и динамическими измерениями.

Примечание 2: В зависимости от области применения и в случаях, когда измерения легко воспроизводимы, может быть допустима потеря передаваемых данных.

Примеры:

(I) / (II) Передающее устройство/компонент ожидает, пока получатель не отправит подтверждение правильного получения набора данных. Передающее устройство/компонент сохраняет набор данных в буфере до получения этого подтверждения. Буфер имеет емкость, превышающую один набор данных, и организован по принципу простой очереди FIFO (Первый на входе-первый на выходе).

6.2.6 Совместимость операционных систем и аппаратного обеспечения

6.2.6.1 Общие положения

Если операционная система является частью средства измерений, требования в соответствии с 6.2.6.2-6.2.6.7 должны быть выполнены.

Выполнение каждого требования к операционной системе должно обеспечиваться на эксплуатационном уровне, на уровне операционной системы или комбинации того и другого.

Например, защитный интерфейс может быть реализован в законодательно значимом приложении, операционной системе, физическом уровне и т.д..

6.2.6.2 Аппаратные интерфейсы

Аппаратные интерфейсы, не оснащенные защитным программным интерфейсом, не должны иметь возможности недопустимо влиять на законодательно значимую часть программного обеспечения (например, запрет на использование интерфейса посредством опломбирования).

Примеры:

(I) При законодательно обоснованном применении рутинно проверяются все открытые физические интерфейсы на наличие входящего трафика. В случае наличия несанкционированного ввода измерения прекращаются.

(II) Все открытые интерфейсы физически защищены или заблокированы операционной системой.

6.2.6.3 Процесс загрузки

6.2.6.3.1 Если для обеспечения защиты законодательно значимой части программного обеспечения необходим безопасный процесс загрузки, применяются требования пунктов 6.2.6.3.2-6.2.6.3.5.

6.2.6.3.2 Для обеспечения целостности и аутентичности законодательно значимой части программного обеспечения должна быть установлена цепочка доверия между отдельными компонентами процесса загрузки.

6.2.6.3.3 Обработка цепочки доверия может быть прервана до тех пор, пока сохраняется ее целостность.

6.2.6.3.4 Конфигурация загрузки должна быть защищена от изменений.

6.2.6.3.5 Загрузка через открытые интерфейсы должна быть запрещена.

Примеры:

(I) Устройство загрузки обеспечивается средствами защиты, например, защищенным паролем.

(II) TPM (платформа модуля доверия) проверяет подпись загрузочного устройства, затем загрузочное устройство проверяет операционную систему, которая, в свою очередь, проверяет и запускает законодательно значимые операции.

6.2.6.4 Системные ресурсы

Комбинация законодательно значимой части программного обеспечения и операционной системы должна обеспечивать наличие достаточных ресурсов для выполнения законодательно значимых функций.

Примеры:

(I) Для выполнения законодательно значимых операций гарантированно имеются все необходимые ресурсы.

(II) Используется минимальный перечень компонентов операционной системы, необходимых для выполнения измерений.

6.2.6.5 Защита в процессе использования

6.2.6.5.1 Не являющееся законодательно значимым программное обеспечение не может не допустимо влиять на законодательно значимые операции.

6.2.6.5.2 Комбинация законодательно значимой части программного обеспечения и операционной системы должна обеспечивать возможность для распознавания законодательно значимого дисплея.

6.2.6.5.3 Контроль доступа должен иметь конфигурацию, не позволяющую оказывать недопустимое влияние на реализацию предписанных функций.

6.2.6.5.4 Выполняемые законодательно значимой частью программного обеспечения функции управления должны быть защищены.

Примеры:

(I) Все законодательно контролируемые файлы защищены от записей, а разрешения на доступ в обязательном порядке проверяются законодательно контролируемой частью программного обеспечения. Изменения разрешений регистрируются в контрольном журнале.

(II) Не являющееся законодательно контролируемым программное обеспечение фактически работает в обособленной среде.

6.2.6.6 Связь с законодательно значимой частью программного обеспечения

Связь с законодательно значимой частью программного обеспечения должна осуществляться через защитные интерфейсы.

Примеры:

(I) Законодательно значимый программный модуль оценивает все команды, поступающие в законодательно значимую программную часть, и отбрасывает неприемлемые.

(II) Связь через открытые программные интерфейсы защищена средствами операционной системы.

6.2.6.7 Идентификация и прослеживаемость

6.2.6.7.1 Конфигурация операционной системы должна быть идентифицируемой.
Идентификатор должен отображаться измерительным прибором:
посредством команды; или
в процессе работы.

Примеры:

1) **В операционной системе типа UNIX конфигурация состоит из законодательно значимых:**
   - **модулей ядра**
   - **перечня установленных пакетов**
   - **библиотек**
   - **учетных записей и привилегий пользователей**
   - **паролей**

- конфигурационных файлов

- разрешений на чтение/запись/выполнение файлов.

Все вышеперечисленное идентифицируется посредством контрольной суммы.

2) В операционной системе Windows конфигурация состоит из законодательно значимых:

- модулей ядра

- перечня установленных пакетов

- библиотек

- учетных записей и привилегий пользователей

- паролей

- конфигурационных файлов

- разрешений на чтение/запись файлов

- регистрационных ключей

Каждое из вышеперечисленных идентифицируется посредством контрольной суммы.

6.2.6.7.2 Параметры конфигурации операционной системы должны быть защищены, чтобы иметь возможность для обнаружения несанкционированного вмешательства.

Пример:

(I) / (II) Все изменения конфигурации операционной системы регистрируются в контрольном журнале. Каждая запись в контрольном журнале содержит метку о времени изменения, а также идентификатор новой конфигурации.

6.2.6.8 Приемлемая среда

Производитель должен определить подходящее окружение для аппаратных средств и программного обеспечения. Минимальные ресурсы и подходящая конфигурация (например, процессор, паять, определенный тип связи, версия операционной системы и т.д.), необходимые для правильного функционирования должны быть заявлены производителем и указаны в свидетельство утверждения типа.

6.2.6.9 Ограничения для эксплуатации

В законодательно значимом программном обеспечении должны быть обеспечены технические средства, чтобы предотвратить операцию, если не соблюдены минимальным требования к ресурсам или подходящей конфигурации. Система должна работать только в условиях, установленных производителем для ее правильного функционирования.

Фиксацию аппаратных средств, операционной системы или системной конфигурации универсального устройства или даже исключение использования, поставляемого со склада универсального устройства необходимо рассматривать в следующих случаях:

- если требуется высокая степень соответствия;

- если должны использоваться криптографические алгоритмы или ключи (см. 6.2.4 и 6.2.5).

6.2.7 Соответствие произведенных устройств утвержденному типу

Производитель должен производить устройства и **законодательно** значимое программное обеспечение, которые соответствует утвержденному типу и предоставленной документации.

6.2.8 Обслуживание и смена конфигурации

6.2.8.1 Общие положения

Обновление законодательно значимого программного обеспечения средств измерений в эксплуатации следует рассматривать как:

- модификацию средств измерений при замене программного обеспечения другой утвержденной версией; или
- ремонт средств измерений при повторной установке той же самой версии.

Средство измерений, которое было модифицировано или отремонтировано при работе может потребовать начальной или последующей проверки в зависимости от национальных правил.

Программное обеспечение, которое не выполняет законодательно важные функции средства измерений, не требует проверки после обновления.

6.2.8.2 Применимость требований к обновлению

Разрешается использовать только версии части законодательно значимого программного обеспечения, которые соответствуют утвержденному типу (см. 6.2.7). Они должны быть указаны в свидетельстве. Применимость следующих требований зависит от вида средств измерений и должна устанавливаться в соответствующей Рекомендации. Варианты 6.2.8.3 и 6.2.8.4 ниже представляют собой равноценные альтернативы. В случае, если речь идет о параметрах, зависящих от конкретного устройства (особенно о параметрах калибровки), следует выполнять только проверенное обновление.

Эта проблема касается проверки средств измерений, находящегося в эксплуатации. См пункт 8 по дополнительным ограничениям.

6.2.8.3 Подтвержденное обновление

Программное обеспечение, которое будет обновлено, может быть загружено локально, то есть непосредственно на средстве измерений или дистанционно через сеть. Загрузка и установка могут быть двумя разными этапами (как показано в рис. 1), или могут быть объединены в один этап в зависимости от особенностей технического решения. Чтобы запустить обновление, необходимо сломать печать. На месте установки средства измерений должен присутствовать человек, чтобы проверить эффективность обновления. После обновления законодательно значимой части программного обеспечения средства измерений (замена на другую сертифицированную версию или повторная установка) средство измерений не должно использоваться по узаконенному назначению до проведения поверки средства измерений, как описано в пункте 0, и средства защиты были обновлены и вновь активированы (если не указано иное в соответствующей Рекомендации или в сертификате).6.2.8.4 Прослеживаемое обновление

6.2.8.4.1 Программное обеспечение вводится в средства измерений согласно требованиям к отслеживаемому обновлению (6.2.8.4.2 – 6.2.8.4.8), если оно соблюдает требования соответствующей Рекомендацией. Прослеживаемое обновление - это процедура смены программного обеспечения в поверенном средстве измерений или комплектующем, после которой не требуется последующая проверка. Это означает, что прослеживаемое обновление не должно влиять на существующие параметры. Программное обеспечение, которое будет обновлено, может быть загружено локально, то есть непосредственно на средстве измерений или дистанционно через сеть. Обновление программного обеспечения регистрируется в журнале контроля (см. 3.1.1). Процедура прослеживаемого обновления включает несколько шагов: загрузка, проверка целостности, проверка происхождения (установление подлинности), установка, регистрация в системе и активация.

6.2.8.4.2 Отслеживаемое обновление программного обеспечения должно быть автоматическим. Если некоторые элементы защиты прибора отключены при проведении обновления, они должны быть снова включены сразу после обновления, вне зависимости от результата процесса обновления.

Примечание: Для запуска прослеживаемого процесса обновления может потребоваться вмешательство/действия пользователя измерительного прибора.

6.2.8.4.3 Программное обеспечение должно быть защищено таким образом, чтобы можно было проследить любое вмешательство. При обновлении любая информация контрольного журнала и значение счетчика событий должны быть сохранены.

Пример:

(I) При запуске средства измерений вычисляется контрольная сумма законодательно значимой части программного обеспечения и сравнивается с номинальным значением. Средство измерений включается только в том случае, если значения совпадают. В противном случае счетчик событий увеличивается на 1 Во время обновления, номинальное значение изменяется в соответствии с новой частью программного обеспечения. Значение счетчика событий сохраняется и обрабатывается новым программным обеспечением таким же образом, как и раньше.

6.2.8.4.4 Должны использоваться технические средства, гарантирующие подлинность загруженного программного обеспечения, т.е. факт его получения от владельца свидетельства.

Пример:

(II) Проверка подлинности осуществляется средствами криптографии, такими как система общедоступного ключа. Владелец свидетельства (производитель средства измерений) генерирует электронную подпись исправленного программного обеспечения или его части, которое будет обновлено, используя секретный ключ в предприятии. Общедоступный ключ хранится в законодательно значимой встроенной части программного обеспечения средства измерений, получающего подписанное исправленное программное обеспечение. Подпись проверяется с помощью общедоступного ключа при загрузке исправленного программного обеспечения в средство измерений. Если подпись загруженного программного обеспечения в порядке, оно устанавливается и активируется; если она не проходит проверку, загруженное исправленное программное обеспечение отказывается от него и использует предыдущую версию программного обеспечения или переключается в нерабочий режим.

6.2.8.4.5 Должны использоваться технические средства, чтобы гарантировать целостность загруженного программного обеспечения, т.е. оно не было недопустимо изменено перед загрузкой. Это достигается добавлением контрольной суммы или хэш-кода в загружаемое программное обеспечение и их проверкой во время процедуры загрузки.

6.2.8.4.6 Должен использоваться журнал контроля, чтобы гарантировать, что отслеживаемые обновления законодательно значимого программного обеспечения адекватно отслеживаются внутри средства измерений для последующей проверки и надзора или инспекции.

Журнал контроля должен содержать как минимум следующую информацию:

- успех / неудача процедуры обновления;
- идентификация программного обеспечения установленной версии;
- идентификация программного обеспечения предыдущей установленной версии;
- метка времени события;
- идентификация загружающей стороны при её наличии.

Запись производится для каждой попытки обновления независимо от ее результата.

Устройство хранения, которое поддерживает отслеживаемое обновление, должно иметь достаточную емкость, чтобы гарантировать возможность проведения отслеживаемых обновлений законодательно значимой части программного обеспечения, по крайней мере, между двумя последовательными поверками средства измерений при эксплуатации / контроле. После достижения предела хранения для журнала контроля, техническими средствами должно быть гарантировано, что дальнейшие загрузки будут невозможны без нарушения пломбы.

Контрольный журнал должен отображаться или печататься по команде. В сертификате должно быть описано, как может быть отображен или распечатан контрольный журнал.

Примечание: Данное требование позволяет контролирующим органам, отвечающим за метрологический надзор за законодательно контролируемыми средствами измерений, отслеживать историю отслеживаемых обновлений законодательно значимого программного за соответствующий промежуток времени (в зависимости от национального законодательства).

6.2.8.4.7 В зависимости от потребностей и национального законодательства, может потребоваться согласие пользователя или владельца средства измерений на прослеживаемое обновление. У средства измерений должны быть функции для пользователя или владельца, чтобы он мог выразить свое согласие, например, кнопка, которую нужно нажать перед запуском обновления. Должна быть предусмотрена возможность включить и отключить эти функции, например, с помощью переключателя, который может быть опечатан или с помощью параметра. Если функции включены, каждая загрузка должна быть инициирована пользователем или владельцем. Если они отключены, от пользователя или владельца не требуется выполнять каких-либо действий, чтобы выполнить обновление.

6.2.8.4.8 Если загруженное программное обеспечение не проходит проверку на целостность (6.2.8.4.5) или проверку подлинности (6.2.8.4.4), следует отказаться от новой версии и использовать предыдущую версию программного обеспечения или переключиться в нерабочий режим. В этом режиме функции измерения должны быть заблокированы. Единственной возможностью остается возобновление процедуры загрузки или отображения ошибки.

Если контрольный журнал полностью заполнен (6.2.8.4.6), а пользователь или владелец не дают согласия (6.2.8.4.7), процедура обновления вообще не должна начинаться.

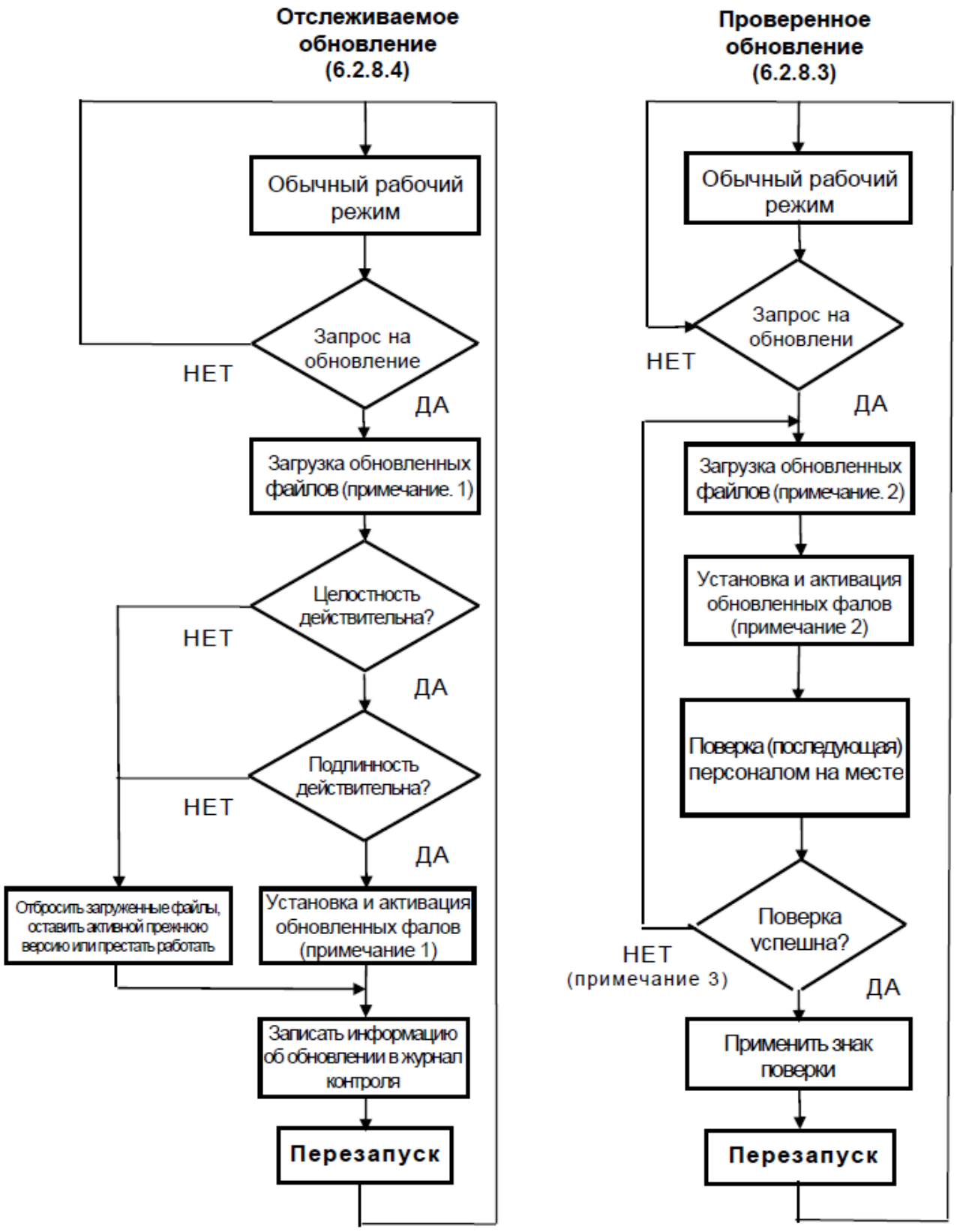


Рисунок 1 – Процедура обновления программного обеспечения

Примечание 1:(1) В случае отслеживаемого обновления процесс обновление делится на два этапа: «загрузка» и «установка/активация». Это означает, что программное обеспечение временно сохраняется после загрузки без активации, потому что должна быть возможность отказаться от загруженного программного обеспечения и вернуться к старой версии, если проверки не будут пройдены.

Примечание 2: В случае проверенного обновления программного обеспечения может также быть загружено и временно сохранено перед установкой, но в зависимости от технического решения загрузку и установку можно также выполнить в один этап.

Примечание 3: Здесь рассматривается только непрохождение поверки средства измерений из-за обновления программного обеспечения. Непрохождение по другим причинам не требует перезагрузки и переустановки программного обеспечения, обозначенных веткой НЕТ.

6.2.8.5 Рекомендация может содержать требование, касающееся специфических параметров конкретных приборов, которые должны быть доступны пользователю. В этом случае прибор должен быть оснащен устройством, позволяющим в автоматическом режиме фиксировать не допускать удаления любой информации о корректировке специфических параметров конкретного устройства, например, контрольного журнала. Прибор должен быть способен отображать записанные данные.

Примечание: Контрольные журналы являются юридически значимой частью программного обеспечения, см. 6.1.3.2.1.

6.2.8.6 При обновлении программного обеспечения контрольный журнал не может стираться или перезаписываться.

7 Утверждение типа

7.1 Документация программного обеспечения, предоставляемая для утверждения типа

7.1.1 Общие положения

Для утверждения типа производитель средства измерений должен заявить и документировать все программные функции, значимые структуры данных и интерфейсы программного обеспечения законодательно значимой части программного обеспечения, реализованные в средстве измерений. Команды и их эффекты должны быть описаны полностью в документации на программное обеспечение, которая будет представлена для утверждения типа.

Кроме того, заявление на оценку типа должно сопровождаться документом или другим доказательством, которое поддерживает предположение, что проект и характеристики программного обеспечения средства измерений соответствуют требованиям соответствующей Рекомендации, в которую были включены общие требования данного документа.

7.1.2 Содержание документации

Типичная документация (для каждого средства измерений/компонента), в основном включает следующее:

- описание законодательно значимого программного обеспечения и то, как соблюдаются требования:
  - список программных модулей, относящихся к законодательно значимой части (Приложение B), включая заявление о том, что в описание включены все юридически значимые части;
  - описание интерфейсов программного обеспечения законодательно значимой части программного обеспечения, команд и потоков данных через данный интерфейс, включая утверждение о полноте;
  - в зависимости от метода оценки, выбранного в соответствующей Рекомендации (см. 7.3 и 7.4), исходный код должен быть доступен органам, проводящим тестирование, если согласно соответствующей Рекомендации МОЗМ требуется высокая степень соответствия или высокая степень защиты;
  - список защищаемых параметров и описание средств защиты;

- описание подходящей системной конфигурации и минимальных требуемых ресурсов (см. 6.2.6);
- описание средств защиты операционной системы (пароль, и т.д., если применимо);
- описание методов опечатывания (программного обеспечени);
- краткий обзор аппаратных средств системы, например, блок-схема топологии, тип компьютера, тип сети и т.д. Если аппаратный компонент считаются законодательно значимым или если он выполняет законодательно значимые функции, это также должно быть указано;
- описание точности алгоритмов (например, фильтрование результатов аналого-цифровой, расчет цены, алгоритм округления и т.д.);
- описание интерфейса пользователя, меню и диалогов;
- идентификация программного обеспечения и инструкции о том, как получить ее от средства измерений во время работы;
- список команд каждого аппаратного интерфейса средства измерений / компонента;
- список ошибок работоспособности, которые выявляются программным обеспечением, в случае необходимости понимания - описание алгоритмов их выявления;
- описание сохраняемых и передаваемых наборов, данных;
- если в программном обеспечении обнаружены существенные дефекты, список обнаруженных существенных дефектов и описание алгоритма обнаружения;
- если выявление ошибки реализовано в программном обеспечении, список выявляемых ошибок и описание алгоритма выявления;
- если в программном обеспечении используется контрольный журнал, описание того, как получить доступ к контрольному журналу;
- руководство по эксплуатации.

7.2 Требования к процедуре утверждения

7.2.1 Общие положения

В рамках оценки типа процедуры испытаний основаны на четко определенных установках и условиях испытаний и могут опираться на метрологически прослеживаемые сравнительные измерения. Точность или правильность программного обеспечения вообще не могут быть измерены с точки зрения метрологии, хотя существуют стандарты, которые предписывают, как «измерить» качество программного обеспечения [например. ISO/IEC 25040:2011 series [5]]. Описанные здесь процедуры учитывают, как потребности законодательной метрологии, так и хорошо известные методы оценки и поверки в разработке программного обеспечения, которые имеют разные цели (например, разработчик программного обеспечения ищет ошибки, но также оптимизирует работу). Как показано в 7.4 каждое программное требование требует индивидуальной адаптации соответствующих процедур оценки. Проведение процедуры должно отражать уровень риска.
Цель состоит в том, чтобы убедиться, что сертифицируемое средство измерений соответствует требованиям соответствующей Рекомендации. Для программно-управляемых средств измерений процедура оценки включает экспертизы, анализ и тестирование, и соответствующая Рекомендация должна включать соответствующий выбор методов, описанных ниже.

Методы, описанные ниже, сосредоточены на оценке типа. Поверки каждого отдельного прибора, используемого в полевых условиях, не охватываются этими методами оценки. Для получения дополнительной информации обратитесь к разделу 8 «*Поверка средства измерений*».

Методы оценки программного обеспечения описаны в 7.3. Комбинации этих методов, составляющие полную процедуру оценки программного обеспечения, адаптированную ко всем требованиям, определенным в пункте 6, указаны в 7.4.

Производитель должен подтвердить отсутствие скрытых или недокументированных свойств (например, параметров, команд, функций)

Настоящий документ не предусматривает дополнительных деклараций производителя относительно того, что документация является правильной и полной. Однако любая страна может потребовать такую декларацию в рамках установленной процедуры проверки программного обеспечения.

7.2.2 Информация, подлежащая включению в сертификат

В сертификат должна быть включена следующая информация:

- идентификация всех сертифицированных версий программного обеспечения;
- способ отображения идентификации программного обеспечения на сертифицированном средстве измерений в процессе использования;
- средства обеспечения безопасности, а также средства подтверждения вмешательства и метода их проверки (например, аппаратные пломбы, счетчики событий, контрольные журналы).;
- программные модули, подлежащие правовому регулированию;
- если применимо:
  - средства проверки целостности защиты;
  - операционная среда программного обеспечения.

7.3 Методы аттестации

7.3.1 Обзор методов и их применения

Выбор и последовательность следующих методов не предписаны и могут варьироваться в процедуре оценки программного обеспечения в зависимости от конкретного случая.

Это приблизительный обзор. Более подробную информацию см. в разделе 7.3.2.

Таблица 1 – Обзор отдельных предлагаемых методов аттестации

Сокраще-ние	**Описание**	**Применение**	**Предварительные условия, инструменты для применения**	**Специальные навыки для выполнения**
AD	Анализ документации и аттестация проекта (7.3.2.1)	Всегда	Документация	-
VFTM	Поверка путем функционального тестирования метрологических функций (7.3.2.2)	Правильность алгоритмов, погрешность, алгоритмы компенсации и корректировки, правила расчета цены	Документация, образец	

VFTSw	Поверка путем функционального тестированием функций программного обеспечения (7.3.2.3)	Правильное функционирование связи, индикации, доказательство вмешательства, защита от ошибок функционирования, защита параметров, выявление существенных неисправностей	Документация, образец	-
DFA	Метрологический анализ потока данных (7.3.2.4)	Разделение программного обеспечения, оценка воздействия команд на функции средства измерений	Исходный код, инструменты для анализа исходного кода	Знание языков программирования. Инструктаж по необходимому методу.
CIWT	Проверка кода и критический разбор программы (7.3.2.5)	Все цели	Исходный код, инструменты для анализа исходного кода	Знание языков программирования, протоколов, и других вопросов ИТ
SMT	Тестирование программного модуля (7.3.2.6)	Все цели, когда можно четко определить информацию на входе и выходе	Исходный код, среда тестирования	Знание языков программирования, протоколов, и других вопросов ИТ. Инструктаж по использованию необходимых средств.

Таблица 2 - Рекомендации по комбинации методов оценки и поверки для различных требований к программному обеспечению (акронимы определены в Таблице 1)

Требование		**Уровень экспертизы A (обычный уровень экспертизы)**	**Уровень экспертизы B (расширенный уровень экспертизы)**	**Комментарий**
Общие требования				
6.1.1	Идентификация программного обеспечения	AD + VFTSw	AD + VFTSw + CIWT	Выберите “B”, если требуется высокая степень соответствия
6.1.2	Правильность алгоритмов и функций	AD + VFTM	AD + VFTM + CIWT/SMT	
Защита программного обеспечения				
6.1.3.1	Предотвращение	AD + VFTSw	AD + VFTSw	
6.1.3.2	Доказательство вмешательства	AD + VFTSw	AD + VFTSw + DFA/CIWT/SMT	Выберите “B” в случае высокого риска мошенничества
Поддержка аппаратных особенностей				
6.1.4.1	Выявление существенных неисправностей	AD + VFTSw	AD + VFTSw + CIWT + SMT	Выберите “B”, если требуется высокая надежность
6.1.4.2	Поддержка защиты работоспособности	AD + VFTSw	AD + VFTSw + CIWT + SMT	Выберите “B”, если требуется высокая надежность
6.1.5	Временные метки	AD + VFTSw	AD + VFTSw + SMT	Выберите “B”, если требуется высокая надежность
Определение и разделение законодательно значимых частей и указание интерфейсов частей				
6.2.2.1	Разделение компонентов	AD	AD + DFA/CIWT	

Требование		Уровень экспертизы A (обычный уровень экспертизы)	Уровень экспертизы B (расширенный уровень экспертизы)	Комментарий
6.2.2.2	Определение и разделение частей программного обеспечения	AD	AD + DFA/CIWT	
6.2.3	Совместно используемые индикаторы	AD + VFTM/VFTSw	AD + VFTM/VFTSw + DFA/CIWT	
6.2.4	Хранение данных	AD + VFTSw	AD + VFTSw + CIWT/SMT	Выберите “B”, если предусмотрено хранение данных измерения в незащищенной системе
6.2.4.2	Сохраненные измеренные данные должны сопровождаться всей значимой информацией, необходимой для будущего законодательно значимого использования	AD + VFTSw	AD + VFTSw + CIWT/SMT	Выберите “B” в случае высокого риска мошенничества
6.2.4.3	Данные должны быть защищены средствами программного обеспечения, чтобы гарантировать подлинность, целостность и при необходимости правильность информации о времени измерения	AD + VFTSw	/	
6.2.4.4	Автоматическое хранение	AD + VFTSw	AD + VFTSw + SMT	
6.2.5	Передача по линиям связи	AD + VFTSw	AD + VFTSw + CIWT/SMT	Выберите “B” в случае передачи данных измерений в открытой системе
6.2.5.1	Переданные измеренные данные должны сопровождаться всей значимой информацией, необходимой для будущего законодательно значимого использования	AD + VFTSw	AD + VFTSw + CIWT/SMT	Выберите “B” в случае высокого риска мошенничества
6.2.5.2	Переданные данные должны быть защищены средствами программного обеспечения, чтобы гарантировать подлинность, целостность и при необходимости правильность информации о времени измерения	AD + VFTSw	AD + VFTSw + SMT/	
6.2.5.3	Задержка или прерывание передачи	AD + VFTSw	AD + VFTSw + SMT	Выберите “B” в случае высокого риска мошенничества, например, передачи в открытых
6.2.6.7	Прерывание передачи	AD + VFTSw	AD + VFTSw + SMT	Выберите “B” в случае высокого риска мошенничества, например, передачи в открытых системах
6.2.6	Совместимость операционных систем и аппаратных средств	AD + VFTSw	AD + VFTSw + SMT	
.6.2.6.2	Аппаратные интерфейсы, не оснащенные защитным программным интерфейсом, не должны иметь возможности недопустимо влиять на законодательно значимую часть программного обеспечения.	AD + VFTSw	AD + VFTSw + SMT	

Требование		Уровень экспертизы A (обычный уровень экспертизы)	Уровень экспертизы B (расширенный уровень экспертизы)	Комментарий
6.2.6.3	Если для обеспечения защиты законодательно значимой части программного обеспечения необходим безопасный процесс загрузки, применяются следующие требования.	AD + VFTSw	AD + VFTSw + SMT	
6.2.6.4	Комбинация юридически значимой части программного обеспечения и операционной системы должна обеспечивать наличие доста точного количества ресурсов для работы юридически значимого приложения.	AD + VFTSw	AD + VFTSw + SMT	
6.2.6.5	Защита во время использования	AD + VFTSw	AD + VFTM/ VFTSw + DFA	
6.2.6.6	Связь с законодательно значимой частью программного обеспечения должна осуществляться через защитные интерфейсы.	AD + VFTSw	AD + VFTM/ VFTSw + DFA	
6.2.6.7	Идентификация и прослеживаемость	AD + VFTSw	AD + VFTSw + SMT	
6.2.6.8	Изготовитель должен определить подходящую аппаратную и программную среду. Минимальные ресурсы и подходящая конфигурация, необходимые для правильного функционирования, должны быть заявлены изготовителем.	AD + VFTSw	AD + VFTSw + SMT	
6.2.6.9	В законодательно значимом программном обеспечении должны быть предусмотрены технические средства для предотвращения работы, если не соблюдены минимальные ресурсы или подходящая конфигурация.	AD + VFTSw	AD + VFTSw + SMT	
Техобслуживание и смена конфигурации				
6.2.8.3	Проверенное обновление	AD	AD	
6.2.8.4	Отслеживаемое обновление	AD + VFTSw	AD + VFTSw + CIWT/SMT	Выберите “B” в случае высокого риска мошенничества

7.3.2 Описание отобранных методов аттестации

7.3.2.1 Анализ документации, спецификации и оценки архитектуры приложения (AD):

Применение:

Основная процедура для оценки программного обеспечения.

Условия:

Процедура основана на документации производителя средств измерений. В зависимости от требований такая документация должна иметь соответствующую область применения:

1) Спецификация внешне доступных функций средств измерений в общей форме (Подходит для простых средств измерений без интерфейсов помимо дисплея, все особенности поддаются проверке функциональным тестированием, низкий риск мошенничества);

2) Спецификация функций программного обеспечения и интерфейсов (необходима для средств измерений с интерфейсами и для функций средств измерений, которые не могут быть функционально проверены, а также в случае повышенного риска мошенничества). Описание должно представить в явном виде и объяснить все функции программного обеспечения, которые могут повлиять на метрологические особенности;

3) В отношении интерфейсов документация должна включать полный список команд или сигналов, которые программное обеспечение может интерпретировать. Эффект каждой команды должен быть подробно документирован. Должен быть описан способ, которым средства измерений реагирует на недокументированные команды;

4) При необходимости, для понимания и оценки функций программного обеспечения должна быть предоставлена дополнительная документация на программное обеспечение для сложных алгоритмов измерения, криптографических функций, или критических временных ограничений.

Общее условие для экспертизы - полнота документации и четкая идентификация оборудования при тестировании EUT, то есть пакетов программ, которые обеспечивают метрологические функции (см. 7.1.1).

Описание:

Эксперт оценивает функции и особенности средств измерений, используя устное описание и решает, соответствуют ли они требованиям соответствующей Рекомендации. Должны быть рассмотрены и оценены метрологические требования, а также функциональные требования к программному обеспечению, определенные в Разделе 6 (например, доказательство вмешательства защита параметров регулировки, запрещенные функции, связь с другими устройствами, обновление программного обеспечения, выявление существенных ошибок и т.д.). Эту задачу может выполнять формат Отчета об оценке программного обеспечения (см. Приложение B).

Результат:

Процедура дает результат по всем особенностям средств измерений при условии, что производителем была представлена соответствующая документация. Результат должен быть указан в разделе, относящемся к программному обеспечению в Отчете об оценке программного обеспечения (см. Приложение B), включенный в формат Отчета об оценке соответствующей Рекомендации.

Дополнительные процедуры:

Должны быть применены дополнительные процедуры, если экспертиза документации не может обеспечить подтвержденные результаты аттестации. В большинстве случаев дополнительной процедурой является «Поверка метрологических функций путем функционального тестирования» (см. 7.3.2.2).

Ссылки:

IEC 61508-5:2010 [7].

7.3.2.2 Поверка метрологических функций путем функционального тестирования (VFTM)

Применение

Для проверки правильности алгоритмов вычисления результата измерения по данным измерений, для линеаризации характеристики, компенсации влияния окружающей среды, округления при расчете цены и т.д.

Условия:

Руководство по эксплуатации, функционирующий образец, метрологические ссылки, испытательное оборудование, тестовые примеры, инструкции для испытательного оборудования.

Если нет понимания, как следует проводить проверку функционирования отдельных частей программного обеспечения, ответственность за разработку соответствующей методики должна быть возложена на производителя. Кроме того, проверяющий должен иметь возможность воспользоваться услугами программиста для получения ответов на возможные вопросы.

Описание:

Большая часть методов одобрения и тестирования, описанных в Рекомендациях, основаны на сравнительных измерениях в различных условиях. Их применение не ограничено определенной технологией средства измерений. Хотя тестирование не имеет основной целью аттестацию программного обеспечения, результат тестирования может интерпретироваться как аттестация некоторых частей программного обеспечения в целом, даже самых важных с точки зрения метрологии. Если тесты, описанные в соответствующей Рекомендации, позволяют рассмотреть все значимые с точки зрения метрологии особенности средства измерений, соответствующие части программного обеспечения могут считаться аттестованными. В целом, чтобы утвердить метрологические особенности средства измерений, нет необходимости применять какой-либо дополнительный анализ программного обеспечения или тестирование.

Результат:

Правильность алгоритмов аттестована или не аттестована. Значения измерения при всех условиях лежат в пределах минимально допускаемой погрешности MPE или нет.

Дополнительные процедуры
:

Этот метод обычно служит расширением 7.3.2.1. В определенных случаях может быть легче или эффективнее объединить метод с экспертизами, основанными на исходном коде (7.3.2.5) или путем симуляции входных сигналов (7.3.2.6), например, для динамических измерений.

Ссылки:

Различные конкретные Рекомендации

7.3.2.3 Поверка функций программного обеспечения путем функционального тестирования (VFTSw)

Применение:

Например, для оценки защиты параметров, индикация идентификации программного обеспечения, поддерживаемые программным обеспечением функции по выявлению существенных неисправностей, конфигурации системы (особенно среды программного обеспечения), и т.д.

Условия:

Руководство по эксплуатации, документация на программное обеспечение, функционирующий образец, испытательное оборудование, тестовые примеры, инструкции для испытательного оборудования.

Если нет понимания, как следует проводить проверку функционирования отдельных частей программного обеспечения, ответственность за разработку методики должна быть возложена на производителя. Кроме того, проверяющий должен иметь возможность воспользоваться услугами программиста для получения ответов на возможные вопросы.

Описание:

Необходимые особенности, описанные в руководстве по эксплуатации, документации на средство измерений или документации на программное обеспечение, проверяются на практике. Если они контролируются программно и правильно функционируют, они должны рассматриваться как аттестованные без дальнейшего анализа программного обеспечения. Рассматриваемые здесь особенности включают как пример включают в себя следующее:

- Нормальная работа средства измерений, если его работа контролируется программными методами. Следует использовать все переключатели или ключи и описанные комбинации и оценить реакцию средства измерений. В графических интерфейсах пользователя должны быть активированы и проверены все меню и другие графические элементы;
- Может быть проверена эффективность защиты параметра путем активации средства защиты и попытки изменить параметр;
- Может быть проверена эффективность защиты хранимых данных путем изменения некоторых данных в файле с последующей проверкой на предмет того, будет ли это обнаружено программным обеспечением
- Отображение идентификации программного обеспечения могут быть проверены в ходе практической проверки;
- Если выявление неисправности поддерживается программным обеспечением, соответствующие части программного обеспечения могут быть проверены путем провокации, ввода или моделирования неисправности и проверки правильной реакции средства измерений;
- Под защитой понимается получение свидетельств несанкционированного вмешательства при внесении изменений в программное обеспечение, параметры, контрольные журналы и т.д. Для проверки следует внести изменения и убедиться, что это приводит к появлению свидетельств вмешательства.

Результат:

Рассматриваемая программно-управляемая характеристика может быть в порядке или не в порядке.

Дополнительные процедуры:

Некоторые особенности или функции программно-управляемого средства измерений не могут быть на практике проверены описанными способами. Если у средства измерений имеются интерфейсы, обычно невозможно обнаружить наличие несанкционированных команд путем введения произвольных команд. Помимо этого, для генерации этих команд требуется отправитель. Для обычного уровня экспертизы метод по 7.3.2.1 может охватывать это требование. Для расширенного уровня экспертизы необходим анализ ПО, как в 7.3.2.4 или 7.3.2.5.

Ссылки:

WELMEC Guide 2.3, Section 3 [8]; WELMEC Guide 7.2, Sections 4.2 and 52[9].

7.3.2.4 Метрологический анализ потока информации (DFA)

Применение:

Для анализа конструирования программ, касающихся управления потоком данных измерительной информации через области данных, которые подлежат правовому регулированию, включая проверку разделения программного обеспечения.

Условия:

Документация на программное обеспечение, исходный код, редактор, программа текстового поиска или специальные инструменты. Знание языков программирования.

Описание:

Цель данного метода - найти все части программного обеспечения, которые участвуют в вычислении результата измерения, или могут влиять на него. Начиная с аппаратного порта, где становятся доступными необработанные данные измерения от датчика, проверяется подпрограмма, которая считывает их. Эта подпрограмма сохраняет их в виде переменной, возможно, после проведения некоторых вычислений. С этой переменной другой подпрограммой считывается промежуточное значение и т.д., пока окончательное значение измерения не будет выведено на дисплей. Все переменные, которые используются для хранения промежуточных результатов измерений, и все подпрограммы, обрабатывающие и транспортирующие эти данные, можно найти в исходном коде, просто используя текстовый редактор и программу текстового поиска, чтобы найти все другие вхождения переменной или имени подпрограммы.

С помощью этого метода могут быть найдены другие потоки данных, например, от интерфейсов до программы интерпретации полученных команд. Кроме того, может быть обнаружен обход интерфейса программного обеспечения (см. 6.2.2.2).

Результат:

Можно проверить, является ли разделение программного обеспечения в соответствии с пунктом 7.2.2.2 приемлемым или неприемлемым.

Можно проверить, является ли документированный список команд для каждого интерфейса полным или нет.

Дополнительные процедуры:

Данный метод рекомендуется, если реализовано разделение программного обеспечения и если требуется высокая степень соответствия или надежная защита от манипуляций. Это расширение до 7.3.2.1 через 7.3.2.3 и до 7.3.2.5.

Ссылка:

IEC 61131-3.

7.3.2.5 Проверка кода и критический разбор программы (CIWT)

Применение:

Этим методом может быть проверена любая особенность ПО, если требуется экспертиза повышенной интенсивности.

Условия:

Исходный код, текстовый редактор, инструменты. Знание языков программирования.

Описание:

Эксперт проводит критический последовательный разбор исходного кода, оценивая соответствующую часть кода, чтобы определить, соблюдены ли требования и соответствуют ли документации функции программы и ее особенности.

Эксперт может также сосредоточить свое внимание на алгоритмах или функциях, которые он идентифицировал как сложные, подверженные ошибкам, недостаточно описанные в документации и исследовать соответствующую часть исходного кода, анализируя и проверяя ее.

Перед этими этапами экспертизы эксперт идентифицирует законодательно значимую часть программного обеспечения, например, применяя метрологический анализ потока данных (см. 7.3.2.4). В целом, проверка кода или критический разбор программы этим и ограничивается.

Результат:

Исполнение совместимо с документацией на программное обеспечение и соответствует требованиями или нет.

Дополнительные процедуры:

Это расширенный способ в дополнении к 7.3.2.1 и 7.3.2.4. Обычно он применяется только в выборочных проверках.

Ссылка:

IEC 61508-5:2010 [7].

7.3.2.6 Тестирование программного модуля (SMT)

Применение:

Данный метод используется в исключительных случаях. Он применяется, когда функции программного обеспечения не могут быть изучены исключительно на основе письменной информации. Он является приемлемым и эффективным при проверке динамических алгоритмов измерения.

Условия:

Исходный код, инструменты разработки, функционирующая среда тестируемого программного модуля, входящий набор данных и соответствующий номинальный набор эталонных данных на выходе или инструменты для автоматизации. Навыки в ИТ, знании языков программирования. Рекомендуется сотрудничество с программистом тестируемого модуля.

Описание:

Тестируемый программный модуль интегрирован в среду проведения испытаний, то есть определенный тестовый модуль программы, который вызывает тестируемый модуль и предоставляет ему все необходимые входные данные. Тестовая программа получает выходные данные от испытываемого модуля и сравнивает их с ожидаемыми эталонными значениями.

Результат:

Правильны или нет тестируемый модуль.

Дополнительные процедуры:

Это расширенный метод в дополнение к 7.3.2.2 или 7.3.2.5.

Ссылка:

IEC 61508-5:2010 [7].

7.4 Процедура оценки программного обеспечения

Процедура оценки программного обеспечения включает сочетание методов оценки и поверки. Соответствующая Рекомендация может определять детали процедуры аттестации, включая:

a) какой из методов аттестации, описанных в 6.3, будет применяться для рассматриваемого требования;

b) как будет проводиться оценка результатов тестирования;

c) какой результат должен быть включен в отчет об испытаниях и какой должен быть включен в свидетельство об испытаниях (см. Приложение B).

В таблице 2 определены два альтернативных уровня экспертизы - обычный (A) и расширенный (B) для процедур оценки программного обеспечения. Методы DFA, CIWT и SMT предусмотрены только для уровня B. Уровень B подразумевает расширенную экспертизу по сравнению с A. Выбор уровня B должен быть обоснован рабочей группой вместе с доказательствами снижения риска. Выбор между процедурами аттестации типа A и B может быть сделан в соответствующей Рекомендации МОЗМ – различны ли они или равны для каждого требования – в соответствии с ожидаемыми:

- риском мошенничества;
- областью приложения;
- необходимым соответствием утвержденному типу;
- риском неправильного измерения из-за операционных ошибок.

См. раздел 4 для получения предварительных указаний по оценке рисков.

7.5 Оборудование при тестировании (EUT)

Обычно, тестирование проводится на полном средстве измерений (функциональное тестирование). Если размер или конфигурация средства измерений не позволяют тестировать его в целом, или если речь идет только об отдельном компоненты средства измерений или программном модуле, соответствующая Рекомендация может указать, что испытания, или определенные виды тестирования, должны быть проведены на компонентах или программных модулях по отдельности при условии, что при испытании работающих устройств эти компоненты или программные модули включены в моделируемую среду, в достаточной степени представляющую их нормальную работу. Заявитель на получение утверждения отвечает за предоставление всего необходимого оборудования и компонентов.

8 Поверка СИ

8.1 Общее

Если в стране требуется проведение метрологического контроля СИ, необходимо наличие средств проверить в полевых условиях во время работы идентичность ПО, действительность настроек и соответствие утвержденному типу.

Соответствующая Рекомендация может требовать проведения проверки программного обеспечения на одном или более этапах в зависимости от природы рассматриваемого средства измерений.

Поверка программного обеспечения должна включать:

- экспертизу соответствия программного обеспечения утвержденной версии (например, поверка идентификации программного обеспечения, поверка средств защиты);
- проверка совместимости конфигурации с заявленной минимальной конфигурацией, если она указана в сертификате утверждения;
- проверка входов/выходов средства измерений для подтверждения того, что они не имеют нежелательных побочных эффектов, и;
- экспертиза правильности определенных параметров устройства (особенно параметров настройки).

PGS должна учитывать следующий подпункт при разработке специфических для конкретного инструмента процедур верификации. Методы, приведенные в разделе 8.2, предлагаются в качестве стандартной процедуры.

8.2 Методы поверки, тестовые элементы

Следующие методы включают этапы поверки, обязательные для проверки соответствия требованиям пунктов 6.1 и 6.2. Аспекты, содержащиеся в пунктах 8.2.1-8.2.4, должны быть проверены в соответствии с инструкциями, перечисленными в нижеприведенном подпункте.

8.2.1 Документы

Начальный этап верификации любого программного обеспечения состоит из проверки EUT на соответствие сертификату и приложениям к нему:

- проверьте, действителен ли сертификат;
- проверьте, соответствует ли EUT типу, описанному в сертификате и приложениях к нему;
- проверьте наличие руководства по эксплуатации (при необходимости).

8.2.2 Целостность программного обеспечения

Целостность программного обеспечения может быть проверена одним из двух способов:

- непрямая проверка: Проверьте наличие, правильность месторасположения и целостность всех, перечисленных в сертификате пломб;
- прямая проверка: Проверьте идентификаторы программного обеспечения в соответствии с требованиями сертификата.

Примечание: Второе требование совпадает с первым требованием пункта 8.2.4.

Пример:

Вычисление контрольной суммы программного кода, которая сравнивается с номинальным значением.

8.2.3 Параметры

8.2.3.1 Корректность

Корректность параметров может быть проверена следующим образом:

- непрямая метрологическая поверка параметров: Выполните измерение и сравните результаты с опорным значением;
- проверьте, все ли устанавливаемые параметры находятся в допустимом диапазоне.

8.2.3.2 Целостность

Целостность параметров может быть проверена следующим образом:

- проверьте целостность пломб, защищающих параметры;
- проверьте журнал регистрации событий или контрольный журнал на наличие записей, касающихся параметров.

8.2.4 Идентификация программного обеспечения

Идентификация программного обеспечения может быть проверена следующим образом:

- убедитесь, что идентификатор программного обеспечения, прилагаемый к EUT, указан в сертификате как допускаемый к применению;
- проверьте записи контрольного журнала, касающиеся зафиксированных обновлений (см. 6.2.8.4.6).

Примечание: Первое требование совпадает со вторым требованием пункта 8.2.2.

Приложение А
(Справочное)

Библиография

На момент публикации настоящего документа, перечисленные в нем издания были действующими. Все упомянутые документы могут быть пересмотрены, в связи с чем пользователям настоящего Документа рекомендуется рассмотреть возможность применения их последних редакций, указанных ниже. Члены МЭК и ИСО ведут реестры действующих в настоящее время международных стандартов.

Фактический статус упомянутых стандартов также можно найти в Интернете:

IEC Publications: http://www.iec.ch/searchpub/cur_fut.htm

ISO Publications: http://www.iso.org

OIML Publications: https://www.oiml.org/en/publications/

(с бесплатной загрузкой PDF-файлов).

Во избежание недоразумений настоятельно рекомендуется, чтобы все ссылки на стандарты в Международных рекомендациях и Международных документах относились к соответствующей версии (с указанием года или даты).

	Стандарты и справочные документы	**Описание**
[1]	OIML V 1:2012 Международный словарь по метрологии. Основные и общие понятия и соответствующие термины (VIM) 3 издание	Словарь разработан Объединенным Комитетом по подготовке Руководящих документов в области метрологии (JCGM)
[2]	OIML D 11:2013 Общие требования к средствам измерений - Условия окружающей среды	Руководство по разработке требований по проверке метрологических характеристик применительно к величинам, влияющим на работу измерительных приборов, подпадающих под действие Рекомендаций МОЗМ (электромагнитные, климатические, механические воздействия).
[3]	ISO/IEC 9594-8:2017 Информационные технологии -- Взаимосвязь открытых систем – Справочник: Часть 8: Структуры сертификатов открытых ключей и атрибутов	ISO/IEC 9594-8:2017 устанавливает рамки и перечень данных, которые могут использоваться для аутентификации и защиты коммуникации между двумя объектами, например, между двумя служебными объектами или между веб-браузером и веб -сервером. Объекты данных также могут быть использованы для подтверждения происхождения и целостности структур данных, таких как документы с цифровой подписью.
[4]	ISO/IEC 2382-9:2015 Информационные технологии – Словарь - Часть 9: Передача данных	Предназначен для облегчения связи в области международной передачи данных. Содержит термины и определения отдельных понятий, относящихся к области передачи данных, идентифицирует взаимосвязи между записями.
[5]	ISO/IEC 25040: серия 2011 Информационные технологии - Оценка программного продукта	Стандарты серии ISO/IEC 25040:2011 содержат методы измерений, проверки и оценки качества программного продукта. Они не описывают методы оценки процессов производства программного обеспечения, или методы прогнозирования затрат (оценка качества программного продукта, конечно, может использоваться для этих целей).

[6]	OIML V 1:2013 Международный словарь терминов по законодательной метрологии (VIML)	VIML включает в себя только понятия, используемые в области законодательной метрологии. Эти понятия применимы к деятельности служб законодательной метрологии, соответствующим документам, проблемам, связанным с этой деятельностью. В Словарь также включены отдельные понятия общего характера, взятые из VIM.
[7]	IEC 61508-5:2010 Функциональная безопасность электрических / электронных/ программируемых электронных систем, связанных с безопасностью – Часть 5: Примеры методов определения уровней целостности безопасности	Содержит информацию о базовых понятиях риска и взаимосвязи риска и целостности защиты (см. Приложение A); методы обеспечения соответствующих уровней защиты целостности для E/E/PE систем безопасности, другие технологические системы, связанные с безопасностью и средствами уменьшения внешних рисков, должны быть определены (см. приложения, B, C, D и E). Предназначен для использования Техническими Комитетами при подготовке стандартов в соответствии с принципами, содержащимися в Руководстве IEC 104 и Руководстве ISO/IEC 51
[8]	Руководство WELMEC 2. 3, май 2005 г. Издание 3 Руководство по проверке программного обеспечения (Средства измерения веса)	Данное руководство определяет основные требования к программному обеспечению, применимые для свободно программируемых модулей на базе ПК или периферийных устройств, которые связаны с NAWIs или являются их частью, подлежащей законодательному контролю.
[9]	Руководство WELMEC 7.2, Издание 2018 Руководство по программному обеспечению (Измерительные приборы Директива 2014/32/EC)	Данный документ содержит рекомендации, связанные с применением Директивы по средствам измерений (Европейская директива 2014/32/EU; MID), в том числе оснащенным программным обеспечением. Он предназначен как для производителей измерительных приборов, так и для уполномоченных органов, осуществляющих за оценку соответствия средств измерений. Соответствие требованиям Руководства позволяет обеспечить также соответствие требованиям к программному обеспечению, устанавливаемым MID
[10]	ISO/IEC 27005:2018 Информационные технологии - Методы защиты - - Управление рисками информационной безопасности	Данный документ содержит руководящие принципы управления рисками информационной безопасности. Он включает общие понятия, определяемые в ISO/IEC 27001, и призван облегчить внедрение систем информационной безопасности, основанных на принципах управления рисками. Знание концепций, моделей, процессов и терминологии, описанных в стандартах ISO/IEC 27001 и ISO/IEC 27002, необходимо для полного понимания данного документа. Документ может быть использован любыми организациями (например, коммерческими предприятиями, государственными учреждениями, некоммерческими организации), которые намерены создать систему управления рисками, относящимися к информационной безопасности организации.

Приложение B
(Справочное)

Пример отчета об оценке программного обеспечения

Примечание: Технические комитеты и подкомитеты, разрабатывающие Рекомендации МОЗМ, должны решить, какая информация должна быть включена в Отчет об испытаниях и Сертификат соответствия МОЗМ. Например, в Свидетельстве об испытаниях должны быть включены название, версия и контрольная сумма исполняемого файла из примера ниже.

Отчет об испытаниях № XYZ122344

Аттестация программного обеспечения расходомера Tournesol Metering модель TT100

Программное обеспечение средства измерений аттестовано и соответствует требованиям Рекомендации OIML R-xyz.

Аттестация основана на отчете в международном документе МОЗМ D-SW, в котором раскрыты основные требования к программному обеспечению. Этот отчет описывает процесс экспертизы программного обеспеченрия, необходимый для подтверждения соответствия с R-xyz.

Производитель	**Заявитель**
Tournesol Metering	Новая компания
А/я 1120333	Нова Стрит 123
100 Клоу	1000 Лас Допикос
Сидави	Сан Теодород
Поручитель: Гн Трифон Турнесол	Поручитель: Арчибальд Хэддок

Объект испытаний

Счетчик TT100 Tournesol Metering – это средство измерений, предназначенное для измерения потока жидкостей. Предполагаемый диапазон - от 1 L/s до 2000 L/s. Основные функции средства измерений:

- измерение потока жидкостей,
- индикация измеренного объема,
- интерфейс преобразователя.

Расходомер описывается как созданное для определенной цели средство измерений (встраиваемая система) с устройством хранения, содержащим юридически значимые данные.

Расходомер TT100 - это независимое средство измерений с подключенным преобразователем. Преобразователь включает функцию температурной компенсации. Возможна регулировка скорости потока с помощью параметров калибровки, которые хранятся в энергонезависимой памяти преобразователя. Он крепится к средству измерений и не может быть отсоединен. Измеренный объем отображается на дисплее. Связь с другими устройствами невозможна.

Встроенное программное обеспечение средства измерений было разработано

Tournesol Metering, А/я 1120333, 100 Клоу, Силдави.

Название исполняемого файла - «tt100_12.exe».

Аттестованная версия данного программного обеспечения - V1.2c. Версия программного обеспечения отображается на дисплее после запуска устройства и при нажатии кнопки «уровень» в течение 4 секунд.

Исходный код включает следующие законодательно значимые файлы:

• main.c	12301 байт	23 ноября 2003;
• int.c	6509 байт	23 ноября 2003;
• filter.c	10897 байт	20 октября 2003;
• input.c	2004 байт	20 октября 2003;
• display.c	32000 байт	23 ноября 2003;
• ethernetc	23455 байт	15 июня 2002;
• driver.c	11670 байт	15 июня 2002;
• calculate.c	6788 байт	23 ноября 2003.

Исполняемый файл «tt100_12.exe» защищен от модификации методом контрольной суммы. Значение контрольной суммы по алгоритму XYZ -составляет 1A2B3C.

Аттестация проведена на основании следующих документов, полученных от производителя:

- ТТ 100 Руководство пользователя Выпуск 1.6;
- ТТ 100 Руководство по техобслуживанию Выпуск 1.1;
- Описание ПО ТТ100 (документ по внутреннему проекту от 22 ноября 2003 г);
- Электронная принципиальная схема ТТ100 (чертеж № 222-31 от 15 октября 2003 г).

Окончательный вариант тестируемого объекта был доставлен в Национальную лабораторию по тестированию и измерениям 25 ноября 2003 г.

Результаты аттестации

Аттестация проводилась согласно OIML D 31:YYYY. Аттестация проводилась между 1 ноября и 23 декабря 2003г. Обзор проекта проводился 3 декабря К. Фехлером в главном офисе компании Tournesol Metering в Клоу. Другая работа по аттестации проводилась в Национальной лаборатории по тестированию и измерению К. Фехлером и С. Проблемом.

Были аттестованы следующие требования:

- идентификация программного обеспечения;
- правильность алгоритмов и функций;
- защита программного обеспечения;
- предотвращение случайных злоупотреблений;
- доказательство вмешательства;
- поддержка аппаратных особенностей;
- хранение данных, передача через системы связи.

Применялись следующие методы аттестации и поверки:

- анализ документации и аттестация проекта;
- аттестация путем функционального тестирования метрологических особенностей;
- критический разбор программы, проверка кода;
- тестирование программного модуля calculate.c с помощью SDK XXX.

Результат

Были подтверждено соответствие следующим требованиям OIML D 31:YYYY,

6.1.1, 6.1.2, 6.1.3, 6.1.4, 6.2.4 и 6.2.5., никаких ошибок не обнаружено.

Результат относится только к протестированному образцу с серийным номером 1188093-B-2004.

Заключение

Программное обеспечение Tournesol Metering TT100 V1.2c соответствует требованиям OIML R-xyz.

Национальная Лаборатория по тестированию и измерению

Отдел программного обеспечения

Подписи

Д-р КЕЙН Фехлер	гн. САНС Проблем
Технический менеджер	Технический специалист

Пункт	Требование	прой-дено	не прой-дено	приме-чания
6.1 6.1.1	**Общие требования** **Идентификация программного обеспечения** Программное обеспечения средств измерений/компонентов должно быть четко идентифицировано.			
6.1.2	**Правильность алгоритмов и функций** Измерительные алгоритмы и функции СИ должны быть правильными и функционально корректными для данного приложения и типа устройства.			
6.1.3 6.1.3.1	**Защита ПО** Предотвращение злоупотреблений Средства измерений – особенно программное обеспечение – должно быть разработано таким способом, при котором возможности для неумышленного, случайного злоупотреблений минимальны.			
6.1.3.2 6.1.3.2.1	**Доказательство вмешательства** Программное обеспечение должно быть защищено таким образом, чтобы были доступны доказательства любого вмешательства (например, обновления программного обеспечения, изменения параметров). Программное обеспечение должно быть защищено от несанкционированной модификации, загрузки или внесения изменений путем замены запоминающего устройства.			
6.1.3.2.2	Только четко документированные функции могут быть активированы интерфейсом пользователя, которые не влияют на метрологические			
6.1.3.2.3	Параметры, которые устанавливают законодательно значимые особенности средств измерений, должны быть защищены от несанкционированной модификации. В случае необходимости для поверки, должна быть предусмотрена возможность отобразить или напечатать текущие настройки параметра.			
6.1.3.2.4	Защита программного обеспечения включает соответствующее опечатывание механическими, электронными и/или криптографическими средствами, благодаря которым несанкционированное вмешательство будет невозможным или очевидным.			
6.1.4 6.1.4.1	**Поддержка аппаратных особенностей** Обнаружение существенных дефектов Производитель СИ обязан разработать и включить средства проверки в ПО или аппаратные средства или обеспечивать средства, с помощью которых аппаратные части могут поддерживаться частями ПО СИ.			
6.1.4.2	Поддержка защиты работоспособности Производитель может по своему выбору реализовать защиту работоспособности программными или аппаратными средствами или разрешить поддержку аппаратных средств средствами программного обеспечения.			
6.1.5	**Временные метки** Временная метка должна считываться с часов прибора. Соответствующие средства защиты должны быть приняты в соответствии с уровнем риска, который должен быть применен.			
6.2 6.2.2	**Требования, предъявляемые к конфигурациям** Спецификация и разделение законодательно значимых частей и спецификация интерфейсов Законодательно значимые части средства измерений не должны подвергаться недопустимому влиянию других частей средства измерений.			
6.2.2.1 6.2.2.1.1	**Разделение компонентов** Компоненты средства измерений, которые выполняют законодательно значимые функции, должны быть идентифицированы, четко определены и задокументированы.			
6.2.2.1.2.	Должно быть продемонстрировано, что функции и данные законодательно значимых компонентов не могут влиять на команды, полученные через интерфейс к другим, юридически не относящимся к делу частям.			

6.2.2.2 6.2.2.2.1	**Спецификация и разделение частей программного обеспечения** Требование соответствия относится к законодательно значимой части программного обеспечения средства измерений (см. 6.2.6), и программное обеспечение должно быть идентифицируемым, как описано в 6.1.1.			
6.2.2.2.2	Если законодательно значимая часть программного обеспечения связана с другими частями программного обеспечения, должен быть определен интерфейс программного обеспечения. Вся связь должна осуществляться исключительно через данный интерфейс. Законодательно значимая часть программного обеспечения и интерфейс должны быть четко описаны в документации. Все законодательно значимые функции и области данных программного обеспечения должны быть описаны, чтобы позволить органам утверждения типа принять решение по правильному разделению программного обеспечения.			
6.2.2.2.3	Должно быть однозначное назначение каждой команды ко всем инициируемым функциям или изменениям данных в юридически значимой части программного обеспечения. Команды, которые передаются через интерфейс программного обеспечения, должны быть задекларированы и описаны в документации. Только команды, указанные в документации, могут быть активированы через интерфейс программного обеспечения. Производитель должен подтвердить полноту документирования команд.			
6.2.2.2.4	Если законодательно значимое программное обеспечение отделено от незначимого, у законодательно значимого программного обеспечения должен быть приоритет в использовании ресурсов по отношению к незначимому программному обеспечению. Законодательно контролируемый процесс не может быть прерван посредством программного обеспечения, не являющегося законодательно значимым.			
6.2.3	**Разделение показаний** Если дисплей или печатающее устройство используются для отображения как законодательно значимых, так и законодательно незначимых результатов, законодательно значимая информация всегда должна быть четко читаемой и отличимой от любой другой информации.			
6.2.4 6.2.4.2	**Хранение данных** Сохраненное или переданное значение измерения должно сопровождаться всей значимой информацией, необходимой для будущего законодательно значимого использования.			
6.2.4.3	Данные должны быть защищены средствами программного обеспечения, чтобы гарантировать подлинность, целостность и в случае необходимости правильность информации времени измерения. Программное обеспечение, которое отображает или проводит дальнейшую обработку измеренного значения и сопровождающих данных, должно проверить время измерения, подлинность и целостность данных, считав их с небезопасного места хранения или получив их от небезопасного канала передачи. Если будет обнаружена ошибка, данные должны быть отброшены или помечены как непригодные.			
6.2.4.4 6.2.4.4.1	**Автоматическое хранение** Когда требуется хранение данных, данные измерений должны быть сохранены автоматически по завершении измерения. Запоминающее устройство должно обладать достаточной надежностью, чтобы гарантировать, что данные измерений не будут повреждены при нормальных условиях хранения. Должно быть достаточно места в памяти для предполагаемого			
6.2.4.4.2	Сохраненные данные могут быть удалены, если: транзакция проведена; или эти данные напечатаны устройством печати, подлежащим законодательному контролю.			
6.2.5 6.2.5.1	**Передача по коммуникационным линиям** Передаваемые измерительные данные должны сопровождаться соответствующей информацией, необходимой для последующего законодательно контролируемого применения			

6.2.5.2	Передаваемые данные должны быть защищены программными средствами, гарантирующими аутентичность, целостность и, при необходимости, достоверность информации, касающейся времени проведения измерений. Программное обеспечение, которое отображает или дополнительно обрабатывает данные измерений и сопутствующие данные, должно проверять время проведения измерения, аутентичность и целостность данных, полученных по каналу передачи. В случае обнаружения несоответствия данные должны быть удалены или помечены как непригодные для использования.			
6.2.5.3	**Задержка или прерывание передачи** Задержка или прерывание передачи не должна недопустимо влиять на измерение. Если сетевые службы становятся недоступными или работают очень медленно, никакие данные измерений не должны быть потеряны.			
6.2.6 6.2.6.2	Совместимость операционной системы и аппаратных средств Аппаратные интерфейсы, не оснащенные защитным программным интерфейсом, не должны иметь возможности для несанкционированного влияния на законодательно значимую часть программного обеспечения.			
6.2.6.3 6.2.6.3.1 6.2.6.3.2 6.2.6.3.3 6.2.6.3.4 6.2.6.3.5	**Процесс загрузки** Если для обеспечения защиты законодательно значимой части программного обеспечения необходим безопасный процесс загрузки, применяются следующие требования. Для обеспечения целостности и аутентичности законодательно значимой части программного обеспечения должна быть создана цепочка доверия между отдельными компонентами процесса загрузки. Обработка цепочки доверия может быть приостановлена если сохраняется ее целостность. Конфигурация загрузки должна быть защищена от изменений. Загрузка через открытые интерфейсы должна быть запрещена			
6.2.6.4	**Системные ресурсы** Сочетание законодательно значимой части программного обеспечения с операционной системой должно обеспечивать необходимые ресурсы для законодательно значимого применения.			
6.2.6.5 6.2.6.5.1 6.2.6.5.2 6.2.6.5.3 6.2.6.5.4	**Защита во время использования** Работа не являющегося законодательно значимым программным обеспечением не должна влиять на законодательно значимое применение. Сочетание законодательно значимой части программного обеспечения и операционной системы должно обеспечивать возможность отличать законодательно значимую информацию, отображаемую на дисплее. Контроль доступа должен исключить возможность несанкционированного влияния на предполагаемое применение. Управление законодательно значимой частью программного обеспечения и законодательно значимой частью операционной системы должны быть защищено.			
6.2.6.6	Коммуникация с законодательно значимой частью программного обеспечения Коммуникация с законодательно значимой частью программного обеспечения должна осуществляться через защитные интерфейсы.			
6.2.6.7 6.2.6.7.1 6.2.6.7.2	**Идентификация и прослеживаемость** Конфигурация операционной системы должна быть идентифицируемой. Идентификатор должен отображаться измерительным прибором по команде или во время работы. Защита параметров конфигурации операционной системы обеспечивается возможностью отслеживать любые несанкционированные вмешательства.			
6.2.6.8	Производитель должен определить подходящие аппаратные средства и среду программного обеспечения. Производитель должен определить минимальные ресурсы и подходящую конфигурацию, необходимые для правильного функционирования			

6.2.6.9	Должны быть обеспечены технические средства, чтобы не допустить операцию, если не соблюдены минимальные требования к конфигурации.			
6.2.8 6.2.8.2	**Обслуживание и изменение конфигурации** Допускается использовать только версии законодательно значимого программного обеспечения, которые соответствуют утвержденному типу.			
6.2.8.3	**Проверенное обновление** После обновления законодательно значимого программного обеспечения средства измерений (замены другой одобренной версией или переустановки) средство измерений не может использоваться в законодательных целях пока не будет проведена поверка данного средства измерений, и обновлены средства защиты.			
6.2.8.4 6.2.8.4.2 6.2.8.4.3 6.2.8.4.4 6.2.8.4.5	**Отслеживаемое обновление** Отслеживаемое обновление программного обеспечения должно быть автоматическим. Если какие-либо элементы защиты прибора отключены при проведении обновления, они должны быть снова включены сразу после обновления, независимо от результатов процесса обновления. Защиту программного обеспечения должна обеспечивать возможность отслеживать несанкционированные вмешательства. При обновлении любая существующая информация контрольного журнала и показания счетчика событий должны быть сохранены. Должны использоваться технические средства, чтобы гарантировать подлинность загруженного программного обеспечения. Должны использоваться технические средства, чтобы гарантировать целостность загруженного программного обеспечения, т.е. то, что оно не было недопустимо изменено перед загрузкой.			
6.2.8.4.6 6.2.8.4.7 6.2.8.4.8	Контрольный журнал должен использоваться для обеспечения того, чтобы отслеживаемые обновления законодательно значимой части программного обеспечения были адекватно прослеживаемы в рамках средства измерений. В зависимости от особенностей национального законодательства может потребоваться согласие пользователя или владельца средства измерений. Если загруженное программное обеспечение не пройдет проверку подлинности, то средство измерений должно отказаться от него и использовать предыдущую версию программного обеспечения или переключиться в нерабочий режим.			
6.2.8.5	Средство измерений должно быть оснащено средством для автоматической нестираемой записи любой регулировки параметра, зависящего от устройства, например, журнала контроля. Средство измерений должно иметь возможность предоставлять записанные данные.			
6.2.8.6	Данные контрольных журналов не должны быть изменены при обновлении программного обеспечения.			

Приложение C
(Справочное)

Комментарии к терминологии по измерениям

Примечание: Настоящее информативное Приложение содержит пояснения по терминам и определениям, связанным с процессом измерений, используемым в данном документе МОЗМ.

Главным образом, настоящий документ МОЗМ устанавливает различие между данными и метаданными измерений. При их одновременном использовании, данные измерений помещаются в контекст, а затем, после объединения с метаданными, они становятся информацией об измерениях. Поскольку получение результата измерений предполагает использование значения, приписываемого измеряемой величине (обозначается символом ■ для удобства последующего использования на рисунках), вместе с другой дополнительной информацией, результат измерения должен включать данные, относящиеся к результату измерений (символ ♣), и метаданные, относящиеся к результату измерений (символ**), а также значение измеренной величины. Измеренное значение, относящееся к измеряемой величине, также состоит из данных и метаданных, которые квалифицируются как данные измерения и метаданные измерения соответственно.

Тем не менее, могут быть и другие данные и метаданные, имеющие отношение к процессу измерений, которые не являются частью результата измерений. Для отличия используемых данных от метаданных, в настоящем Документе МОЗМ вводятся производные понятия: «данные, относящиеся к результатам измерений ♣», «метаданные, относящиеся к результатам измерений ♣», «данные процесса измерений ♥» и «метаданные процесса измерений ♦», см. рисунок А.1.

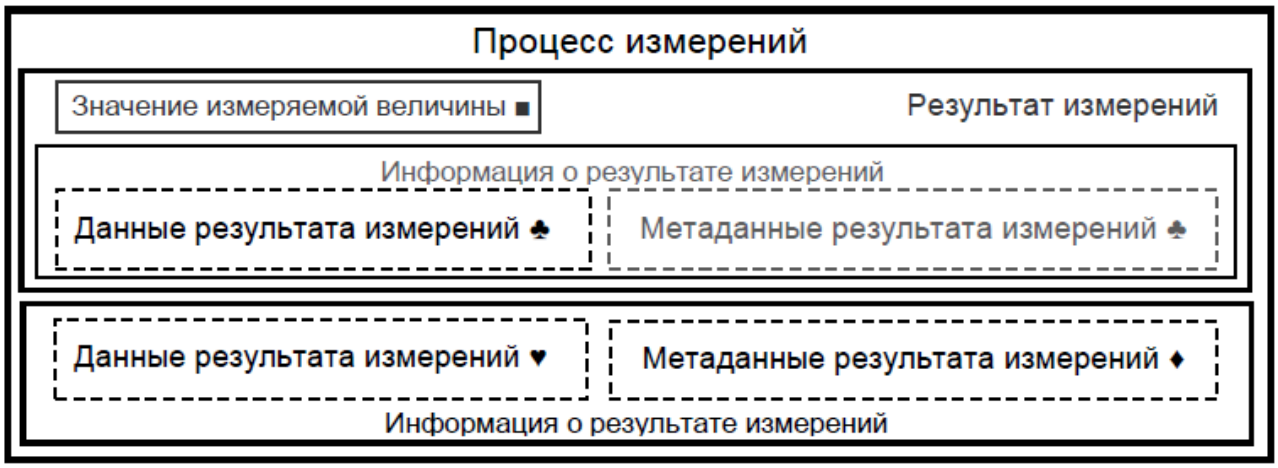


Рисунок А.1 – Визуальное представление процесса измерений и результата измерений, относящихся к соответствующим данным и метаданным.

Таким образом, данные измерений включают данные, относящиеся к результатам измерений, и данные процесса измерений, тогда как метаданные измерений включают метаданные, относящиеся к результатам измерений, и метаданные процесса измерений.

Рисунок А.2 содержит блок-схему, иллюстрирующую различие между терминами, относящимися к результату или к процессу измерений, используемыми для описания измерений.

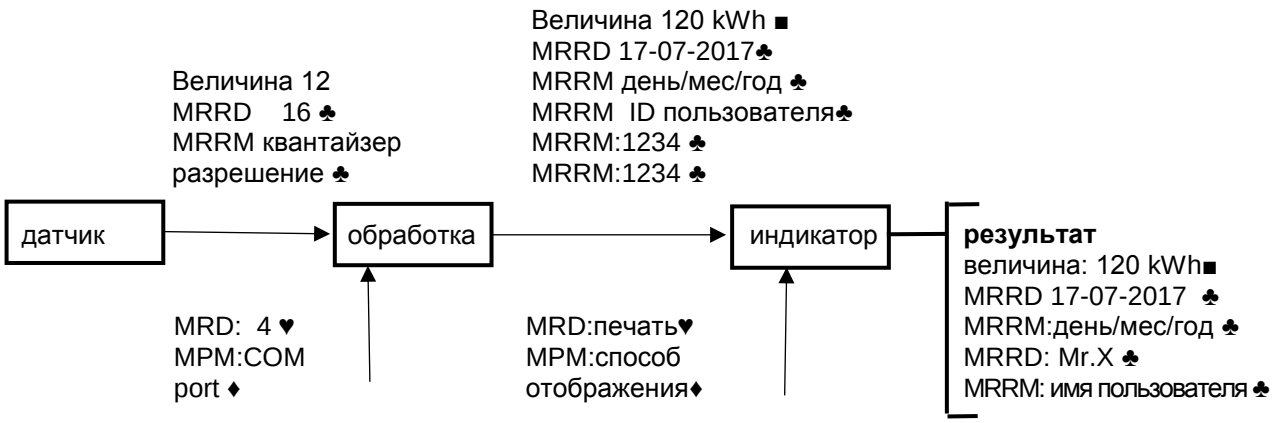


Рисунок А.2 – Блок-схема процесса измерений с примерами применения различных терминов.

На рисунке А.2 показан пример процесса измерений. Для каждого логического шага (от сбора данных до индикации результата) в качестве примеров приводятся значение измеренной величины (■), данные, относящиеся к результату измерения (MRRD, ♣), и метаданные, относящиеся к результату измерения (MRRM, ♣), а также данные процесса измерений (MPD, ♥) и метаданные процесса измерений (MPM, ♦).

Когда датчик выдает необработанное значение 12, дополнительной информацией, относящейся к результату измерений, может быть разрешение квантора ADC 16 бит, где 16 – данные (♣), а «разрешение квантора» - метаданные (♣), необходимые для интерпретации данных (♣). Аналогичным образом, при обработке величина может быть преобразовано в значение измеренной величины (■) (величина + единица) с дополнительными данными, относящимися к результату измерения (♣), где 17-07-2017 - отметка времени, формат которой (день-месяц-год) можно рассматривать как метаданные (♣). В обоих случаях данные измерений (♣) необходимы для обработки значения и формирования части результата, в то время как метаданные(♣) необходимы для правильной интерпретации данных (♣).

Другая часть информации об измерениях (данные + метаданные) связана с фактическим процессом измерения: Для получения необработанного значения может использоваться COM Port номер 4, где 4 - данные процесса измерений (♥) и метаданные процесса измерений (♦) «COM-Port» помогает понять элемент данных (♥). В данном примере индикация результата может быть с помощью дисплея или печати. Более того, данные процесса (♥) «печать» с необходимыми метаданными процесса (♦) «метод отображения» необходимы для процесса измерений, но они не станут частью результата измерений. Это свидетельствует о том, что в рамках данного процесса измерений существуют по крайней мере два различных информационных потока, где оба могут быть законодательно контролируемыми.

При определенных обстоятельствах данные процесса измерений (♥) могут стать данными, относящимися к результатам измерений (♣). В данном примере COM-Port номер 4 связывает измеренное значение величины (■) с идентификатором пользователя 1234, тем самым превращая данные процесса измерений в данные (♥), относящиеся к результату измерения (♣) в процессе обработки.

Приложение D

Указатель

Приемлемое решение: 6.1.1.

Журнал контроля: 3.1.1; 3.1.46; 6.1.3.2.4; 6.2.8.4; 6.2.8.4.3; 6.2.8.4.6; 6.2.8.4.8; 6.2.8.5; 6.2.8.6; 7.1.2; 7.2.2; 7.3.2.3; 8.2.3.2; 8.2.4

Установление подлинности: 3.1.2; 3.1.3; 6.2.8.4.1.

Подлинность: 3.1.3; 3.1.8; 3.1.13; 6.1.3.2.4; 6.2.4.3; 6.2.5.2; 6.2.6.3.2; 6.2.8.4.4; 6.2.8.4.8.

Проверка средства: 3.1.5; 6.1.4.1.

Команды: 3.1.49; 6.1.3.2.2; 6.2.2.1.2; 6.2.2.2.2; 6.2.2.2.3; 6.2.6.6 7.1.1; 7.1.2; 7.2.1; 7.3.1; 7.3.2.1; 7.3.2.3; 7.3.2.4.

Коммуникация: 3.1.6; 3.1.56; 5.2; 6.1.1; 6.2.2.2.2; 6.2.2.2.3; 6.2.2.2.4; 6.2.5; 6.2.6.6; 6.2.6.8; 7.3.1; 7.3.21.

Интерфейс связи: 3.1.6; 6.1.1.

Криптографическое свидетельство: 3.1.7; 3.1.13; 6.1.3.24.

Криптографические средства: 3.1.8; 6.1.3.2.4; 6.2.8.44.

Область данных: 3.1.9; 3.1.49; 3.1.50; 3.1.51; 6.2.2.2.2; 6.2.4.4.1; 7.3.2.4.

Параметр, зависящий от устройства: 3.1.10; 3.1.26; 6.1.3.2.3; 6.2.8.2; 6.2.8.5; 8.1.

Длительность: 3.1.11; 6.1.4.2; 7.1.2; 7.3.1.

Электронное СИ: 3.1.12; 3.1.19.

Электронная подпись: 3.1.8; 3.1.13; 6.1.3.2.4; 6.2.4.3; 6.2.5.2; 6.2.8.4.4.

Ошибка (индикации): 3.1.14; 3.1.19; 3.1.24.

Ошибочная регистрация: 3.1.15; 6.1.4.1.

Оценка: 3.1.57; 3.1.58; 3.1.62; 6.1.3.2.3; 6.1.4.1; 6.2.2.1.1; 6.2.2.2.2; 7.1.1; 7.1.2; 7.2.1; 7.3.1; 7.3.2.1; 7.3.2.2; 7.3.2.3; 7.4.

Событие: 3.1.1; 3.1.16; 3.1.17; 3.1.46; 3.1.55; 6.1.3.2.4; 6.2.2.2.4; 6.2.8.4.6.

Счетчик событий: 3.1.17; 6.1.3.2.4; 6.2.8.4.3; 7.2.2.

Исполняемый код: 3.1.18; 3.1.53; 6.1.1.

Ошибка: 3.1.19; 3.1.46; 7.1.2; 7.3.2.3.

Хэш-функция: 3.1.20; 6.1.4.1.

Целостность (программ, данных или параметров): 3.1.13; 0; 6.2.4.3; 6.2.5.2; 6.2.6.3.2; 6.2.6.3.3; 6.2.8.4; 6.2.8.4; 6.2.8.4.5; 6.2.8.4.5; 6.2.8.4.8; 6.2.8.4.8; 7.2.2;

Интерфейс: 3.1.4; 3.1.22; 3.1.59; 6.1.1; 6.2.2; 6.2.2.1.1; 6.2.2.1.2; 6.2.2.2.4; 6.2.6.2; 6.2.6.3.5; 7.1.2; 7.3.1; 7.3.2.1; 7.3.2.3.

Основная погрешность: 3.1.19; 3.1.24.

Законодательно значимый: 2.1; 3.1.1; 3.1.10; 3.1.25; 3.1.26; 3.1.27; 3.1.37; 3.1.43; 3.1.49; 3.1.52; 3.1.54; 3.1.58; 6.1.3.1; 6.1.3.2.1; 6.1.3.2.2; 6.1.3.2.3; 6.1.3.2.4; 6.1.4.1; 6.1.5; 6.2.2; 6.2.2.1.1; 6.2.2.1.2; 6.2.2.2.1; 6.2.2.2.2; 6.2.2.2.3; 6.2.2.2.4; 6.2.3; 6.2.4.2; 6.2.4.3; 6.2.4.4.1; 6.2.5.1; 6.2.5.2; 6.2.6.1; 6.2.6.2; 6.2.6.3.1; 6.2.6.3.2; 6.2.6.3.5; 6.2.6.4; 6.2.6.5.1; 6.2.6.5.2; 6.2.6.5.4; 6.2.6.6; 6.2.6.7.1; 6.2.6.9; 6.2.7; 6.2.8.1; 6.2.8.2; 6.2.8.3; 6.2.8.4.3; 6.2.8.4.4; 6.2.8.4.6; 6.2.8.5; 7.1.1; 7.1.2; 7.3.1; 7.3.2.5.

Законодательно значимый параметр: 3.1.10; 3.1.26; 3.1.58; 6.1.3.2.4; 6.1.4.1.

Законодательно значимое программное обеспечение: 2.1; 3.1.27; 3.1.37; 3.1.43; 3.1.52; 3.1.58; 6.1.3.2.1; 6.1.3.2.2; 6.1.4.1; 6.1.5; 6.2.2; 6.2.2.2.1; 6.2.2.2.2; 6.2.2.2.3; 6.2.2.2.4; 6.2.3; 6.2.4.3; 6.2.5.2; 6.2.6.2; 6.2.6.3.1; 6.2.6.3.2;.6.2.6.4; 6.2.6.5.1; 6.2.6.5.4; 6.2.6.6; 6.2.6.9; 6.2.7; 6.2.8.1; 6.2.8.2; 6.2.8.3; 6.2.8.4.3; 6.2.8.4.4; 6.2.8.4.6; 6.2.8.5; 7.1.1; 7.1.2; 7.3.1; 7.3.2.5.

Максимальная допускаемая ошибка: 3.1.28; 3.2; 7.3.2.2.

Средство измерений: 1; 2.1; 2.2; 2.3; 3; 3.1.1; 3.1.2; 3.1.5; 3.1.6; 3.1.7; 3.1.10; 3.1.11; 3.1.12; 3.1.15; 3.1.16; 3.1.18; 3.1.19; 3.1.26; 3.1.27; 3.1.28; 3.1.29; 3.1.38; 3.1.39; 3.1.44; 3.1.46; 3.1.50; 3.1.51; 3.1.52; 3.1.57; 3.1.58; 3.1.60; 3.1.62; 4.3; 5.1; 6.1; 6.1.1; 6.1.2; 6.1.3.1; 6.1.3.2.1; 6.1.3.2.3; 6.1.3.2.4; 6.1.4.2; 6.1.5; 6.2.1; 6.2.2; 6.2.2.1.1; 6.2.2.2.1; 6.2.2.2.4; 6.2.3; 6.2.4.2; 6.2.4.3; 6.2.5.1; 6.2.5.2; 6.2.6.1; 6.2.6.7.1; 6.2.8.1; 6.2.8.2; 6.2.8.3; 6.2.8.4.1; 6.2.8.4.2; 6.2.8.4.3; 6.2.8.4.4; 6.2.8.4.6; 6.2.8.4.7; 6.2.8.4.8; 6.2.8.5; 7.1.1; 7.1.2;7.2.1; 7.3.2.1; 7.3.2.2; 7.5; 8.1.

Прерываемое/непрерывное измерение: 3.1.23; 3.1.42; 6.1.4.1.

Операционная система: 3.1.4; 3.1.59; 6.1.3.2.1; 6.2.2.2.3; 6.2.2.2.4; 6.2.3; 6.2.6.1; 6.2.6.2; 6.2.6.3.5; 6.2.6.4; 6.2.6.5.2; 6.2.6.6; 6.2.6.7.1; 6.2.6.7.2; 6.2.6.8; 6.2.6.9; 7.1.2.

Работа: 3.1.11; 7.2.1.

Программный код:3.1.49; 6.1.4.1; 6.2.2.2.2; 6.2.4.3; 6.2.5.2; 8.2.2.ь

Защитный интерфейс: 3.1.43; 6.2.6.1; 6.2.6.6.

Опечатывание 3.1.44; 5.2; 6.1.3.2.1; 6.1.3.2.4; 7.1.2.

Обеспечение: 3.1.13; 3.1.45; 6.2.2.1.1; 6.2.2.1.2; 6.2.3; 6.2.8.3; 6.2.8.4.2; 7.2.2; 8.1.

Экспертиза программного обеспечения: 3.1.47; 6.1.2; 7.2.1.

Идентификация программного обеспечения: 3.1.48; 6.1.1; 6.2.8.4.6; 7.1.2; 7.2.2; 7.3.1; 7.3.2.3; 8.1.

Интерфейс программного обеспечения:3.1.49; 3.1.52; 6.2.2.2.2; 6.2.2.2.3; 6.2.6.2; 6.2.6.6; 7.1.1 7.1.2; 7.3.1 7.3.2.4.

Программный модуль: 3.1.9; 3.1.16; 3.1.27; 3.1.43; 3.1.48; 3.1.49; 3.1.50; 3.1.60; 6.1.3.2.2; 6.2.2.2.1; 6.2.4.3; 6.2.5.2; 6.2.6.6; 7.1.2; 7.2.2; 7.3.1; 7.3.2.6; 7.5.

Защита программного обеспечения: 3.1.51; 6.1.3; 6.1.3.2.4; 7.3.1.

Разделение программного обеспечения: 3.1.52; 6.2.2.22; 6.2.2.24; 7.3.1; 7.3.2.4.

Исходный код: 3.1.53; 7.1.2;7.3.1; 7.3.2.2; 7.3.2.4; 7.3.2.5; 7.3.2.6.

Устройство хранения: 3.1.54; 6.2.4.4.1; 6.2.8.4.6.

Тестирование:3.2; 5.1; 6.1.2; 6.1.5; 6.2.8.4.8; 7.2.1; 7.3.1; 7.3.2.1; 7.3.2.2; 7.3.2.3; 7.3.2.6; 7.4; 7.5; 8.2.

Метка времени: 3.1.1; 3.1.55; 6.1.5; 6.2.2.1.2; 6.2.4.2; 6.2.5.1; 6.2.6.7.2; 6.2.8.4.6; 7.3.1; 7.4.

Передача данных измерения: 3.1.56; 6.1.3.2.1; 6.2.2.1.1; 6.2.5; 6.2.5.1; 6.2.5.2; 6.2.5.3; 7.3.1.

Параметр, зависящий от типа: 3.1.26; 3.1.58; 6.1.3.23.

Универсальное устройство: 3.1.59; 5.2; 6.1.3.2.1; 6.2.2.1.1; 6.2.2.2.3; 6.2.2.2.4; 6.2.6.9.

Пользовательский интерфейс: 3.1.60; 6.1.1; 6.1.3.2.2; 6.2.3; 7.1.2; 7.3.2.3.

Поверка: 3.1.61; 3.1.62; 6.1.3.2.3; 6.2.8.1; 6.2.8.2; 6.2.8.3; 6.2.8.4.16.2.8.4; 6.2.8.4.6; 6.2.8.4.8; 7.2.1;7.3.1; 7.3.2.2; 7.3.2.3; 7.3.2.6; 7.4; 8.1; 8.2; 8.2.1; 8.2.31.