ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 8.839— 2013/ OIML D 31:2008

Государственная система обеспечения единства измерений

ОБЩИЕ ТРЕБОВАНИЯ К ИЗМЕРИТЕЛЬНЫМ ПРИБОРАМ С ПРОГРАММНЫМ УПРАВЛЕНИЕМ

OIML D 31:2008
General requirements for software controlled measuring instruments
(IDT)

Издание официальное

Москва
Стандартинформ
2014

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным унитарным предприятием «Уральский научно-исследовательский институт метрологии» (ФГУП «УНИИМ») на основе собственного аутентичного перевода на русский язык международного документа, указанного в пункте 4

2 ВНЕСЕН Управлением метрологии Федерального агентства по техническому регулированию метрологии, Техническим комитетом по стандартизации ТК 53 «Основные нормы и правила в области обеспечения единства измерений»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 17 октября 2013 г. № 1164-ст

4 Настоящий стандарт идентичен международному документу OIML D 31:2008 «Общие требования к измерительным приборам с программным управлением» (OIML D 31:2008 «General requirements for software controlled measuring instruments»).

Наименование настоящего стандарта изменено относительно наименования указанного международного документа для приведения в соответствие с ГОСТ Р 1.5 (подраздел 3.5).

В настоящий стандарт внесены следующие редакционные изменения: введение, раздел «Термины и определения» и «Библиография» приведены в соответствие с требованиями ГОСТ Р 1.7—2007.

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

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (gost.ru)

© Стандартинформ, 2014

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

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
3.1 Общая терминология 2
3.2 Сокращения 6
4 Правила применения настоящего стандарта 7
5 Требования к измерительным приборам в части практического применения программного обеспечения 7
5.1 Общие требования 7
5.2 Требования для конкретных вариантов конфигурации 11
6 Утверждение типа 21
6.1 Документация, которая должна представляться при утверждении типа 21
6.2 Требования к процедуре утверждения 22
6.3 Методы аттестации (экспертиза программного обеспечения) 23
6.4 Процедура аттестации 28
6.5 Тестируемое оборудование 30
7 Верификация 30
8 Оценка уровней жесткости требований 30
Приложение А (справочное) Библиография 32
Приложение В (справочное) Пример отчета по оценке программного обеспечения 33
Приложение С (справочное) Предметный указатель 39
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации 41

Введение

Международная Организация по законодательной метрологии (МОЗМ) представляет собой всемирную межправительственную организацию, первостепенной задачей которой является гармонизация правил и средств метрологического контроля, используемых на практике национальными метрологическими службами или родственными организациями в странах — членах этой организации.

Документ МОЗМ Д 31 «Общие требования к измерительным приборам с программным управлением» (OIML D 31:2008 «General requirements for software controlled measuring instruments»), на основе которого подготовлен настоящий стандарт, разработан Техническим подкомитетом OIML TC 5/SC 2 «Программное обеспечение» и был утвержден для окончательной публикации Международным Комитетом по законодательной метрологии в 2008 году.

При подготовке настоящего стандарта добавлено справочное приложение ДА, содержащее сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации. Исправлены обнаруженные опечатки в тексте применяемого международного документа. В необходимых случаях добавлены примечания разработчика, поясняющие с учетом действующих нормативных документов некоторые положения применяемого международного документа (см., например, примечания к термину 3.1.57 «верификация»).

Настоящий стандарт содержит рекомендации МОЗМ, которые позволяют гармонизировать требования национальных стандартов стран — членов МОЗМ в области законодательной метрологии к измерительным приборам с программным управлением.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Государственная система обеспечения единства измерений

ОБЩИЕ ТРЕБОВАНИЯ К ИЗМЕРИТЕЛЬНЫМ ПРИБОРАМ С ПРОГРАММНЫМ УПРАВЛЕНИЕМ

State system for ensuring the uniformity of measurements.
General requirements for software controlled measuring instruments

Дата введения — 2015—01—01

1 Область применения

1.1 Настоящий стандарт устанавливает общие требования к функциональным возможностям измерительных приборов, связанным с программным обеспечением, и предлагает правила подтверждения соответствия измерительных приборов этим требованиям.

1.2 Настоящий стандарт может учитываться национальными органами по стандартизации стран — членов МОЗМ ТК и ПК МОЗМ в качестве основы для разработки конкретных требований к программному обеспечению и конкретных процедур, имеющих отношение к отдельным категориям измерительных приборов.

1.3 Правила настоящего стандарта применимы только к тем измерительным приборам или электронным устройствам, которые имеют программное управление.

Примечания

1 Настоящий стандарт не распространяется на технические требования, которые относятся к конкретным измерительным приборам с программным управлением; эти требования должны указываться в соответствующих национальных нормативных документах и Рекомендациях МОЗМ, например, для взвешивающих измерительных приборов, счетчиков воды и т. д.

2 Настоящий стандарт рассматривает некоторые вопросы, касающиеся защиты данных. Помимо этого необходимо учитывать национальные нормативные акты в этой области.

3 Поскольку устройства с программным управлением всегда являются электронными устройствами, необходимо также учитывать требования документа [3].

2 Нормативные ссылки

Нижеследующие документы, на которые приводятся ссылки, являются обязательными для применения настоящего стандарта. В отношении датированных ссылок действительно только указанное издание. В отношении недатированных ссылок действительно последнее издание публикации (включая любые изменения), на которую дается ссылка:

Международный словарь по метрологии. Основные и общие понятия и соответствующие термины (VIM), подготовленный Рабочей группой 2 Объединенного комитета по руководствам в области метрологии , в состав которого входят представители МБМВ, МЭК, МФКХ, ИСО, ИЮПАК, ИЮПАП, МОЗМ, ИЛАК

ИСО/МЭК 9594-8 Информационные технологии. Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации

Издание официальное

3 Термины и определения

В настоящем стандарте приведены термины по [1], [3], [8], а также следующие термины с соответствующими определениями:

Примечание — В необходимых случаях приводимые в документе определения уточняются с учетом действующих российских и международных документов.

3.1 Общая терминология

3.1.1 **приемлемое решение** (acceptable solution): Конструкция или принцип действия программного модуля или аппаратного блока, либо конструкция или принцип действия какой-либо функции, которые считаются соответствующими конкретному требованию. Приемлемое решение дает пример того, как может быть удовлетворено конкретное требование. Оно не исключает возможности любого другого решения, которое также удовлетворяет данному требованию.

3.1.2 **контрольный журнал** (audit trail): Непрерывно ведущийся файл данных, в который заносят информационные записи о событиях с отметками времени события, например, об изменениях значений параметров устройства или об обновлениях программного обеспечения либо о других действиях, которые законодательно контролируемы и могут оказывать влияние на метрологические характеристики.

3.1.3 **аутентификация** (authentication): Проверка декларированной или предполагаемой подлинности пользователя, процесса или устройства (например, проверка того, что загружаемое программное обеспечение исходит от владельца свидетельства об утверждения типа прибора).

3.1.4 **аутентичность** (authenticity): Результат процесса аутентификации (прошел проверку или не прошел).

3.1.5 **контрольное устройство** (checking facility [3]): Устройство, которое встроено в измерительный прибор и позволяет обнаруживать существенные сбои и выполнять последующие действия.

Примечание — «Выполнять последующие действия» относится к любой адекватной реакции со стороны измерительного прибора (например, световой сигнал, акустический сигнал, блокировка процесса измерения).

3.1.6 **закрытая сеть** (closed network): Сеть из фиксированного числа участников с известными адресами, функциями и пунктами их местонахождения (см. также 3.1.35 «открытая сеть»).

3.1.7 **команды** (commands): Команды могут представлять собой некую последовательность электрических (оптических, электромагнитных и т. д.) сигналов на входных интерфейсах или кодов в протоколах передачи данных. Они могут формироваться программой измерительного прибора/электронного устройства/компоновочного узла (программируемые команды) или формироваться пользователем посредством интерфейса пользователя измерительного прибора (команды пользователя).

3.1.8 **связь** (communication): Обмен информацией между двумя или несколькими блоками (например, программными модулями, электронными устройствами, компоновочными узлами) согласно установленным правилам.

3.1.9 **интерфейс связи** (communication interface): Электронное, оптическое, радио- или иное техническое устройство сопряжения, которое позволяет обмениваться информацией между компонентами измерительного прибора (например, электронными устройствами) или компоновочными узлами.

3.1.10 **криптографический сертификат** (cryptographic certificate): Набор данных, включающий в себя открытый криптографический ключ, принадлежащий какому-нибудь измерительному прибору или какому-нибудь лицу, и идентификационный номер данного объекта, например, заводской номер измерительного прибора, имя или персональный идентификационный код (ПИН-код) данного лица. Этот набор данных заверяет аккредитованная в установленном порядке организация с помощью электронной подписи. Принадлежность открытого криптографического ключа какому-либо объекту можно верифицировать использованием открытого криптографического ключа указанной заслуживающей доверие организации и расшифровки подписи на данном сертификате.

3.1.11 **криптографические средства** (cryptographic means): Кодирование данных отправителем (программой передачи или запоминания данных) и декодирование данных получателем (программой считывания) для сокрытия информации от лиц, не имеющих права доступа к ней.

Подтверждение достоверности данных электронной подписью для того, чтобы получатель или пользователь мог проверить источник этих данных, то есть подтвердить их аутентичность.

Примечание — Для формирования электронной подписи, как правило, применяют криптографическую систему с открытым ключом, алгоритм функционирования которой основан на применении пары ключей, из которых только один ключ должен держаться в секрете, а другой может быть открытым.

Отправитель (программа передачи или запоминания данных) формирует хеш-код (см. 3.1.25 «хеш-функция») данных и зашифровывает его с помощью *секретного ключа*. Результатом оказывается электронная подпись. Получатель (программа получения или считывания данных) расшифровывает электронную подпись с помощью *открытого криптографического ключа* отправителя и сравнивает результат с фактическим хеш-кодом данных. В случае совпадения результатов данные признаются аутентичными.

Получатель может требовать криптографический сертификат отправителя (см. 2.1.10 «Криптографический сертификат») для того, чтобы быть уверенным в аутентичности данного открытого криптографического ключа.

3.1.12 **область данных** (data domain): Область памяти, которая требуется каждой программе для обработки данных. Эта область памяти в зависимости от типа применяемого языка программирования определяется с помощью аппаратных адресов или символических наименований (наименований переменных). Размер наименьшей адресуемой области обычно оказывается равным одному байту, но этот размер может быть почти неограниченным: он колеблется в пределах от 1 бита (например, флаг какого-нибудь регистра) до произвольных структур данных, которые могут быть настолько большими, насколько это нужно программисту.

Области данных могут принадлежать одному *программному модулю* или нескольким модулям. При использовании языков высокого уровня (например, JAVA, C/C++) легко отделить область данных одного программного модуля для предотвращения доступа к ней любых других программных модулей.

3.1.13 **значимый параметр устройства** (device-specific parameter): Законодательно контролируемый параметр, значение которого определяется характеристиками конкретного устройства. Значимые параметры устройства включают в себя параметры настройки (например, настройки диапазона, другие виды настройки или корректировки) и параметры конфигурации (например, максимальное значение, минимальное значение, единицы измерения и т. д.).

3.1.14 **работоспособность** (durability [3]): Способность измерительного прибора сохранять свои функциональные характеристики в течение периода применения.

3.1.15 **электронный измерительный прибор** (electronic measuring instrument [3]): Измерительный прибор, предназначенный для измерения электрической или неэлектрической величины с применением электронных средств или оборудованный электронными средствами.

Примечание — В рамках настоящего стандарта любое вспомогательное оборудование, подлежащее законодательному метрологическому контролю, считается частью данного измерительного прибора.

3.1.16 **электронное устройство** (electronic device [3]): Устройство, содержащее электронные компоновочные узлы и предназначенное для выполнения конкретной функции. Электронное устройство изготавливается обычно в виде отдельного блока и может подвергаться независимому тестированию.

Примечание — Электронное устройство может представлять собой измерительный прибор (например, счетчик электрической энергии) или часть измерительного прибора (например, принтер, индикатор).

Электронное устройство может быть неким модулем в том смысле, в каком этот термин применяется [2].

3.1.17 **погрешность (показания)** (error (of indication) [3]): Разность между измеренным значением величины и опорным значением величины.

Примечание — Приведенное определение соответствует определению статьи 2.16 Международного словаря по метрологии VIM (см. таблицу ДА.1 приложения ДА).

3.1.18 **файл регистрации ошибок** (error log): Непрерывно ведущийся файл данных, в который заносят информационные записи об отказах и неисправностях, оказывающих влияние на метрологические характеристики. Этот файл особенно полезен для обнаружения неустойчивых отказов, которые нельзя распознать впоследствии после проведения измерений.

3.1.19 **испытания (типа прибора)** (evaluation (type) [8]): Обязательные испытания одного или нескольких образцов измерительного прибора, предназначенного для применения в сфере государственного регулирования обеспечения единства измерений, с целью утверждения типа прибора.

3.1.20 **событие** (event): Действие, при котором проводят изменение какого-либо параметра измерительного прибора, введение поправочного коэффициента или обновление программного модуля.

3.1.21 **счетчик событий** (event counter): Не сбрасываемый на ноль счетчик с энергонезависимой памятью, показания которого увеличиваются на единицу каждый раз, когда происходит какое-либо событие.

3.1.22 **исполняемый код** (executable code): Файл, загруженный в вычислительную систему конкретного измерительного прибора, электронного устройства или компоновочного узла (программируемое запоминающее устройство, жесткий диск и т. д.). Этот исполняемый код интерпретируется микропроцессором и преобразуется в определенные логические и арифметические операции, операции декодирования или передачи данных.

3.1.23 **неисправность** (fault [3]): Дефект, который имеет определенные негативные последствия для свойств или функций измерительного прибора или обуславливает погрешность показания, превышающую предел допускаемой погрешности.

3.1.24 **постоянная часть**[1] **законодательно контролируемого программного обеспечения** (fixed legally relevant software part): Часть законодательно контролируемого программного обеспечения, являющаяся и остающаяся идентичной по исполняемому коду программному обеспечению измерительного прибора утвержденного типа.

3.1.25 **хеш-функция** (hash function [4]): Функция (математическая), отображающая значения из бóльшей (возможно, очень большой) области в меньшую область значений. Результаты применения «хорошей» хеш-функции к большому набору значений области данных распределены равномерно (и, очевидно, случайно) по диапазону.

3.1.26 **целостность программ, данных или параметров** (integrity of programs, data, or parameters): Гарантии того, что программы, данные или параметры в процессе применения, переноса, хранения, ремонта или технического обслуживания прибора не подверглись несанкционированным или случайным изменениям.

3.1.27 **интерфейс** (interface [5]): Общая граница между двумя функциональными блоками, которые различаются характеристиками функционирования, взаимосвязи, характеристиками обмена сигналами и другим характеристикам этих блоков.

Примечание — Приведенное определение соответствует определению статьи 10.7 РМГ 29—99.

3.1.28 **основная погрешность** (intrinsic error [3]): Погрешность измерительного прибора, применяемого в нормальных условиях.

3.1.29 **законодательно контролируемое** (legally relevant): Программное обеспечение/аппаратное обеспечение/данные или часть программного обеспечения/аппаратного обеспечения/данных измерительного прибора, относящиеся к характеристикам, регулируемым законодательной метрологией, например, точность измерения или правильное функционирование измерительного прибора.

3.1.30 **законодательно контролируемый параметр** (legally relevant parameter): Параметр измерительного прибора, электронного устройства или компоновочного узла, подлежащий законодательному контролю. Различают следующие типы законодательно контролируемых параметров: *значимые параметры типа прибора* и *значимые параметры конкретного устройства*.

3.1.31 **законодательно контролируемая часть программного обеспечения** (legally relevant software part): Та часть *программных модулей* измерительного прибора, электронного устройства или компоновочного узла, которая является законодательно контролируемой.

3.1.32 **предел допускаемой погрешности (измерительного прибора)** (maximum permissible error (of a measuring instrument [3]): Предельное значение погрешности, устанавливаемое нормативным документом для измерительного прибора данного типа.

3.1.33 **измерительный прибор** (measuring instrument [1]): Устройство, предназначенное для проведения измерений в индивидуальном порядке или совместно с дополнительным устройством(ами) и получения значений измеряемой величины в установленном диапазоне.

Примечание — Измерительные приборы по принципу действия разделяют на интегрирующие и суммирующие. Различают также приборы прямого действия и приборы сравнения, аналоговые и цифровые приборы, самопишущие и печатающие приборы.

3.1.34 **непрерываемое/прерываемое измерение** (non-interruptible/interruptible measurement): Непрерываемое измерение представляет собой измерительный процесс с непрерывным накоплением результатов без определенного окончания. Такой измерительный процесс не может быть остановлен и продолжен вновь без недопустимого нарушения процесса или результата измерения (например, при измерении расхода товара или энергии).

---

[1] Эта часть программного обеспечения контролирует обновление программного обеспечения (загрузку программ, аутентификацию, проверку целостности, установку и активацию).

Если процесс измерения может быть легко остановлен в нормальном режиме работы, а не только в случае аварийной ситуации без искажения результатов, то такой процесс измерения называют прерываемым.

3.1.35 **открытая сеть** (open network): Сеть из произвольного числа участников (электронных устройств с произвольными функциями). Число участников, идентификационные данные и местонахождение участников сети могут динамично изменяться и оставаться неизвестными для других участников (см. также 3.1.6 «закрытая сеть»).

3.1.36 **функциональная характеристика** (performance [3]): Способность измерительного прибора выполнять функции, для которых он предназначается.

3.1.37 **программный код** (program code): *Исходный или исполняемый код.*

3.1.38 **пломбирование** (sealing): Способ защиты измерительного прибора от любого несанкционированного изменения, регулирования, демонтажа деталей, удаления программ. Способ может реализовываться с помощью аппаратных средств, программ или их комбинации.

3.1.39 **защита** (securing): Совокупность технических решений и процедур для предотвращения несанкционированного доступа к аппаратной или программной части устройства.

3.1.40 **программное обеспечение** (software): Общий термин, охватывающий программный код, данные и параметры.

3.1.41 **проверка программного обеспечения** (software examination): Техническая операция, которая заключается в определении одной или нескольких характеристик программного обеспечения согласно конкретной заданной процедуре (например, экспертиза технической документации или прогон программы при контролируемых условиях).

3.1.42 **идентификация программного обеспечения** (software identification): Последовательность читаемых символов (например, номер версии, контрольная сумма), которая неразрывно связана с рассматриваемым программным обеспечением или *программным модулем*. Ее можно проверить на конкретном приборе в процессе его применения.

3.1.43 **программный интерфейс** (software interface): Этот интерфейс состоит из управляющей программы и специально выделенной области данных; он обеспечивает получение, фильтрацию или передачу данных между *программными модулями,* которые могут не относиться к законодательно контролируемым.

3.1.44 **программный модуль** (software module [6]): Логические элементы, такие как программы, подпрограммы, библиотеки и объекты, включая их *области данных*, которые могут быть взаимосвязаны с другими элементами. Программное обеспечение измерительного прибора, электронного устройства или компоновочного блока состоит из одного или нескольких программных модулей.

3.1.45 **защита программного обеспечения** (software protection): Обеспечение защиты программного обеспечения или области данных измерительного прибора с помощью «пломбирования», осуществляемого аппаратными или программными средствами. Такая «пломба» должна быть снята, сломана или нарушена для того, чтобы можно было получить доступ к программному обеспечению с целью его изменения.

3.1.46 **разделение программного обеспечения** (software separation): Программное обеспечение в измерительных приборах/электронных устройствах/ компоновочных блоках можно разделить на *законодательно контролируемую* и *законодательно неконтролируемую* части. Связь между этими частями осуществляется через *программный интерфейс*.

3.1.47 **исходный код** (source code): Компьютерная программа, написанная в такой форме (на языке программирования), что она становится удобочитаемой и редактируемой. Исходный код компилируется или интерпретируется в *исполняемый код*.

3.1.48 **запоминающее устройство** (storage device): Устройство хранения, применяемое для сохранения данных измерений в состоянии готовности после завершения измерения для последующих законодательно контролируемых целей (например, для заключения какой-либо коммерческой сделки).

3.1.49 **компоновочный блок (узел)** (sub-assembly [3]): Часть электронного устройства, в которой применяют электронные детали или узлы и которая выполняет свою собственную распознаваемую функцию.

Пример — Усилители, компараторы, силовые преобразователи и т. д.

3.1.50 **тестирование** (test [3]): Серия операций, предназначенных для проверки соответствия подвергаемого испытанию оборудования установленным требованиям.

3.1.51 **отметка времени** (time stamp): Однозначный отсчет монотонно возрастающего времени, например, в секундах, или строка из даты и времени, обозначающая дату и/или время некоторого события или сбоя. Эта отметка времени сохраняется в согласованном формате, который позволяет легко сравнивать две разные записи и следить за развитием событий во времени.

3.1.52 **передача данных измерений** (transmission of measurement data): Передача результатов измерений с помощью сетей связи или иных средств удаленному электронному устройству для дальнейшей обработки и/или применения в регулируемых законодательством целях.

3.1.53 **значимый параметр типа прибора** (type-specific parameter): *Законодательно контролируемый параметр,* значение которого зависит только от типа прибора. Значимые параметры типа прибора являются частью законодательно контролируемого программного обеспечения.

Пример — Если рассматривать систему измерения расхода жидкостей отличных от воды, то диапазон значений кинематической вязкости перекачиваемой жидкости является значимым параметром типа прибора, фиксируемым при утверждении типа турбины. Для всех турбин этого типа регламентирован один и тот же диапазон вязкости перекачиваемой жидкости.

3.1.54 **универсальный компьютер** (universal computer): ПЭВМ, которая не предназначена для выполнения специальных целей, но может быть приспособлена для выполнения метрологических задач с помощью программного обеспечения. Обычно такое программное обеспечение базируется на операционной системе, которая позволяет загружать и применять программное обеспечение, предназначенное для конкретных целей.

3.1.55 **интерфейс пользователя** (user interface): Интерфейс, обеспечивающий возможность обмена информацией между человеком и конкретным измерительным прибором или его аппаратной или программной частью, например, выключатели, клавиатура, мышка, дисплей, монитор, принтер, сенсорный экран, окно программного обеспечения на экране дисплея, включая ту программу, которая его формирует.

3.1.56 **аттестация, оценка пригодности** (validation): Подтверждение путем проверки и предоставления объективных доказательств (т. е. информации, истинность которой может быть показана на основании фактов, полученных из наблюдений, измерений, тестирования) того, что специальные требования для применения прибора по назначению выполняются. В данном случае такими требованиями являются требования, содержащиеся в настоящем стандарте.

3.1.57 **верификация** (verification [8]): Процедура (отличная от процедуры утверждения типа), которая включает в себя экспертизу, изучение и маркировку и/или выдачу документального подтверждения, в котором утверждается и подтверждается, что данный измерительный прибор отвечает установленным законом требованиям[1)].

Примечания

1 В международном словаре по метрологии VIM, указанном в приложении ДА, два последних термина определены следующим образом:

- **верификация** (статья 3.44) — предоставление объективных свидетельств того, что данный объект полностью удовлетворяет установленным требованиям, а

- **валидация** (статья 3.45) — верификация, при которой установленные требования соответствуют (адекватны) предполагаемому применению.

2 Объектом верификации может быть, например, процесс, методика измерений, материал или измерительная система.

3 Установленными требованиями, например, могут быть те, что удовлетворяют спецификации изготовителя.

4 Термины «верификация» и «поверка» применительно к средству измерений, являются синонимами.

3.2 Сокращения

В настоящем стандарте применены следующие сокращения:

МЭК — Международная электротехническая комиссия;

ИСО — Международная организация по стандартизации;

МОЗМ — Международная организация законодательной метрологии;

PIN — Персональный идентификационный номер (ПИН-код);

ТК — Технический комитет МОЗМ;

ПК — подкомитет МОЗМ.

[1)] Это определение отличается от определений, приведенных в других стандартах, например в стандарте ИСО/МЭК 14598 или стандарте МЭК 61508-4.

4 Правила применения настоящего стандарта

4.1 Положения настоящего стандарта применимы к новым нормативным документам и документам, находящимся в стадии пересмотра. Национальные органы по стандартизации стран — членов МОЗМ, ТК и ПК МОЗМ должны применять настоящий стандарт для разработки требований к программному обеспечению в дополнение к прочим техническим и метрологическим требованиям соответствующих нормативных документов.

4.2 Все нормативные документы подлежат пересмотру, и пользователям настоящего стандарта рекомендуется применять в своей практической работе самые последние редакции нормативных документов.

4.3 Цель создания настоящего стандарта состоит в том, чтобы обеспечить национальные органы по стандартизации стран — членов МОЗМ, ТК и ПК МОЗМ, ответственные за разработку документов законодательной метрологии, совокупностью требований — частично разного уровня жесткости — рассчитанных на то, чтобы охватить все виды измерительных приборов и все сферы применения. Национальные органы по стандартизации стран—членов МОЗМ, ТК и ПК должны решать, какой уровень требований приемлем для решения вопросов защиты, соответствия требованиям или аттестации. Некоторые полезные советы по выполнению этой задачи приведены в разделе 8.

5 Требования к измерительным приборам в части практического применения программного обеспечения

5.1 Общие требования

На момент публикации настоящего стандарта настоящие общие требования отражают состояние развития информационных технологий. Они в принципе применимы ко всем видам измерительных приборов, электронных устройств и компоновочных блоков с программным управлением и должны приниматься в расчет во всех нормативных документах. В отличие от этих общих требований специальные требования для конкретной конфигурации (5.2) имеют отношение к техническим особенностям, которые не являются общими для приборов некоторых видов или в некоторых сферах практического применения.

В приводимых ниже примерах приводятся требования как нормального, так и повышенного уровня жесткости. В настоящем стандарте применяют следующую систему обозначений:

(I) приемлемое техническое решение для нормального уровня жесткости требований;

(II) приемлемое техническое решение для повышенного уровня жесткости требований (см. раздел 8).

5.1.1 Идентификация программного обеспечения

Законодательно контролируемое программное обеспечение измерительного прибора/электронного устройства/компоновочного блока должно быть однозначно идентифицировано указанием версии программного обеспечения или иным способом. Такое идентификационное обозначение может состоять более чем из одной части, но при этом по меньшей мере одна его часть должна быть посвящена законодательно контролируемым целям.

Идентификационное обозначение должно быть неразрывно связано с самим программным обеспечением и должно выводиться на печать или на дисплей во время работы или при включении измерительного прибора. Если компоновочный блок или электронное устройство не имеет ни дисплея, ни принтера, то идентификационное обозначение должно отсылаться через интерфейс связи для воспроизведения на дисплее или печати на другом компоновочном блоке или электронном устройстве.

В особых случаях приемлемым решением следует считать маркировку идентификации программного обеспечения на соответствующем измерительном приборе или электронном устройстве при выполнении следующих условий:

1) Интерфейс пользователя не имеет функции индикации идентификационного обозначения программного обеспечения на экране дисплея или дисплей не имеет технической возможности отображения идентификационного обозначения программного обеспечения (аналоговое индикаторное устройство или электромеханический счетчик).

2) Измерительный прибор или электронное устройство не имеет интерфейса для передачи идентификационного обозначения программного обеспечения.

3) После изготовления измерительного прибора или электронного устройства изменение программного обеспечения невозможно или же возможно только в случае, когда проводят изменения аппаратного обеспечения данного прибора или его компонента.

Изготовитель аппаратного обеспечения или значимого компонента аппаратного обеспечения несет ответственность за обеспечение гарантий того, что на соответствующем измерительном приборе или электронном устройстве обеспечена правильная маркировка идентификационного обозначения его программного обеспечения.

Идентификационное обозначение программного обеспечения и способы идентификации должны быть указаны в свидетельстве об утверждении типа прибора.

Это исключение из правил допускается или не допускается в соответствующих нормативных документах национальных органов по стандартизации стран — членов МОЗМ и документах МОЗМ.

Примечание — Каждый применяемый измерительный прибор должен соответствовать утвержденному типу такого прибора. Идентификационное обозначение программного обеспечения позволяет персоналу, осуществляющему надзор, или лицам, которых непосредственно касаются данные измерения, определять, соответствует ли требованиям применяемый прибор.

Примеры идентификации

(I) Программное обеспечение содержит текстовую строку или номер, позволяющий однозначно идентифицировать версию установленного программного обеспечения. Эта строка выводится на дисплей прибора при нажатии соответствующей кнопки, когда прибор включен, или периодически контролируется с помощью таймера.

Номер версии может иметь следующую структуру: A.Y.Z. Если мы рассматриваем вычислитель расхода, то буква A представляет версию резидентной программы, которая обеспечивает счет импульсов, буква Y представляет версию функции преобразования (преобразование отсутствует, преобразование при температуре 15 °C, преобразование при температуре 20 °C), а буква Z представляет язык интерфейса пользователя.

(II) Программное обеспечение вычисляет контрольную сумму исполняемого кода и представляет идентификационное обозначение исполняемого кода в виде строки, указанной в подпункте (I), или же в дополнение к этой строке. Алгоритм вычисления контрольной суммы должен быть неким стандартным алгоритмом, например можно применять алгоритм циклического кодирования CRC16, предназначенный для проверки целостности блока данных.

Пример решения (II) применим в случае, когда требуется повышенная степень соответствия (см. 5.2.5, перечисление d) и раздел 8).

5.1.2 Корректность алгоритмов и функций

Измерительные алгоритмы и функции электронного устройства должны быть соответствующими и функционально корректными для конкретной области применения и конкретного типа устройства (точность этих алгоритмов, погрешность вычислений согласно определенным правилам, алгоритмы округления и т. д.).

Результат измерения и сопроводительная информация, которая требуется согласно конкретной рекомендации МОЗМ или национальному законодательству, должны правильно воспроизводиться на экране дисплея или распечатываться.

Должна быть обеспечена возможность проверки алгоритмов и функций с помощью метрологического тестирования, тестирования или проверки программного обеспечения (как это описано в 6.3).

5.1.3 Защита программного обеспечения

5.1.3.1 Предотвращение неправильного использования

Измерительный прибор должен конструироваться таким образом, чтобы минимизировать возможности неумышленного, случайного или несанкционированного использования. В рамках настоящего стандарта это особенно касается программного обеспечения. Представление результатов измерений должно быть четким и однозначным для всех заинтересованных в этом сторон.

Примечание — Измерительные приборы с программным управлением часто функционально сложны. Пользователю необходимо хорошее руководство по правильному применению прибора и способам получения корректных результатов измерений.

Пример защиты — Пользователь руководствуется в работе меню. Законодательно контролируемые функции объединяют в отдельную ветвь этого меню. Если какие-либо измеренные значения могут быть утеряны вследствие некоторого действия, то пользователь должен быть предупрежден об этом вместе с просьбой выполнить другое действие до выполнения данного действия (см. также 5.2.2).

5.1.3.2 Защита от мошенничества

5.1.3.2a Законодательно контролируемое программное обеспечение должно быть защищено от несанкционированных изменений, загрузки или изменений путем дозагрузки в запоминающее устройство. В дополнение к механическому пломбированию могут потребоваться технические средства для защиты измерительных приборов, имеющих операционную систему или опцию загрузки программного обеспечения.

Примечание — Если программное обеспечение хранится в постоянной памяти прибора (в которой данные защищены, например, опцией «Память только для чтения»), то потребность в технических средствах соответственно снижается.

Примеры защиты

(I)/(II) Корпус, в котором находится запоминающее устройство, опломбирован, или запоминающее устройство опломбировано на печатной плате.

(II) Если применяют устройство многократной записи, то входной сигнал разрешения записи блокируют с помощью выключателя, который может быть опломбирован. Электрическая цепь должна быть построена таким образом, чтобы функцию защиты записи нельзя было отменить с помощью короткого замыкания контактов.

(I) Измерительная система состоит из двух компоновочных блоков, один из которых, выполняющий функции измерения, размещен в корпусе, который может быть опломбирован. Другим компоновочным блоком является универсальный компьютер, работающий под управлением операционной системы. Некоторые функции типа индикации включены в программное обеспечение этого компьютера. Благодаря относительно легкой манипуляции — особенно если для связи между обеими частями программного обеспечения применяют стандартный протокол — может происходить дозагрузка посторонней информации в программное обеспечение универсального компьютера. Такую манипуляцию можно предотвратить с помощью простых криптографических средств, например кодированием передачи данных между компоновочным блоком и универсальным компьютером. Ключ декодирования размещают в законодательно контролируемой программе универсального компьютера. Только эта программа знает ключ и способна считывать, декодировать и применять измеренные значения. Другие программы не могут применяться для этой цели, потому что они не могут расшифровывать измеренные значения (см., например, 5.2.1.2, перечисление d)).

5.1.3.2b Только однозначно документированные функции (см. 6.1) могут активироваться с помощью интерфейса пользователя, реализация которого не должна способствовать мошенническому применению. Вывод данных должен соответствовать требованиям 5.2.2.

Примечание — Эксперт, проводящий проверку, должен решить, все ли документированные команды являются допустимыми.

Пример защиты — (I)/(II) Все входные сигналы интерфейса пользователя переправляются программе, которая фильтрует поступающие команды. Только эта программа может пропустить документально подтвержденные команды и не пропустить все прочие. Эта программа или программный модуль представляет собой часть законодательно контролируемого программного обеспечения.

5.1.3.2c Значимые параметры, которые определяют законодательно контролируемые характеристики измерительного прибора, должны быть защищены от неразрешенных изменений. Если это необходимо для целей верификации, то должна быть возможность воспроизведения на экране дисплея или распечатки текущих параметров настройки.

Примечание — Значимые параметры устройства могут регулироваться или выбираться только в особом режиме работы прибора. Их можно разделить на параметры, которые должны быть защищены (фиксированные параметры), и параметры, к которым возможен доступ (устанавливаемые параметры) конкретного лица, например, владельца прибора или его продавца. Значимые параметры типа прибора имеют одинаковые значения для всех образцов данного типа. Они определяются при утверждении типа прибора.

Пример защиты — (I)/(II) Значимые параметры конкретного устройства, подлежащие защите, сохраняются в энергонезависимой памяти. Сигнал разрешения записи в этой памяти блокируется с помощью выключателя, который может быть опломбирован.

См. примеры (1)—(3) в 5.1.3.2d настоящего раздела.

5.1.3.2d Защита программного обеспечения осуществляется с помощью пломбирования механическими, электронными (программными) и/или криптографическими методами, благодаря которым неразрешенное вмешательство становится невозможным или же очевидным.

Примеры защиты

1 (I) Электронное пломбирование. Метрологические параметры прибора могут вводиться и регулироваться с помощью элемента меню. В этом случае программное обеспечение распознает каждое изменение и увеличивает показания счетчика событий на единицу при каждом событии такого рода. Значение счетчика событий может отображаться на индикаторе. Начальное значение счетчика событий должно быть зарегистрировано. Если отображаемое на индикаторе значение отличается от зарегистрированного значения, то такой прибор оказывается в «неверифицированном» состоянии (эквивалент сломанной пломбы).

2 (I)/(II) Программное обеспечение измерительного прибора построено так (см. пример 5.1.3.2a), что нет иного способа изменить параметры и законодательно контролируемую конфигурацию, кроме как с помощью ключа защиты меню. Этот ключ механически пломбируется в неактивном положении, делая тем самым изменение параметров и законодательно контролируемой конфигурации невозможным.

Чтобы изменить параметры и конфигурацию, ключ должен быть включен, что неизбежно приводит к «срыву пломбы» в такой защите.

3 (II) Программное обеспечение измерительного прибора построено таким образом (см. пример 5.1.3.2a), что нет иного способа изменить параметры и законодательно контролируемую конфигурацию, кроме как с помощью уполномоченного лица. Если какое-либо лицо хочет ввести конкретный элемент в меню параметров, то оно должно использовать свою смарт-карту, которая содержит ПИН-код как часть криптографического сертификата. Программное обеспечение прибора проверяет аутентичность данного ПИН-кода указанному сертификату и дает разрешение на ввод данного элемента в меню параметров. Такой доступ должен регистрироваться в контрольном журнале с указанием личных данных этого лица (или по меньшей мере номера применяемой смарт-карты).

Уровень (II) из числа примеров приемлемых технических решений, подходящих в случае, когда необходима повышенная защита от обмана и мошенничества (см. раздел 8).

5.1.4 Поддержка аппаратных функций

5.1.4.1 Поддержка обнаружения неисправностей

Нормативный документ национального органа по стандартизации или рекомендация МОЗМ может требовать обнаружения определенных видов неисправностей измерительных приборов (см. [3], 5.1.2(b) и 5.3). В этом случае изготовитель измерительного прибора обязан включать в программную или аппаратную часть такого прибора соответствующие контрольные устройства или предложить способ, благодаря которому аппаратные части могут быть поддержаны программными частями прибора.

Если программное обеспечение прибора участвует в обнаружении неисправностей, то должна быть реализована соответствующая реакция прибора. Нормативный документ национального органа по стандартизации или рекомендация МОЗМ может потребовать, чтобы при обнаружении неисправности измерительный прибор или электронное устройство дезактивировалось или формировался сигнал тревоги или соответствующая запись в файле регистрации ошибок.

В документации, представляемой при утверждении типа прибора, должен содержаться перечень неисправностей, которые могут быть обнаружены с помощью программного обеспечения, и ожидаемых реакций программного обеспечения и, если это необходимо для понимания, описание алгоритма обнаружения.

Пример обнаружения — (I)/(II) При каждом запуске законодательно контролируемая программа вычисляет контрольную сумму программного кода и законодательно контролируемых параметров. Номинальные значения этих контрольных сумм вычисляют заранее и сохраняют в памяти прибора. Если вычисленные и сохраненные в памяти значения не совпадают между собой, то исполнение программы прекращается.

Если процесс измерения непрерываемый, то контрольная сумма вычисляется периодически и контролируется с помощью программного таймера. В случае обнаружения отказа программное обеспечение обеспечивает вывод на экран дисплея сообщения об отказе или включает индикатор отказов и записывает время возникновения неисправности в файле регистрации ошибок (если таковой существует).

Приемлемым алгоритмом для проверки контрольных сумм является алгоритм CRC16.

5.1.4.2 Поддержка функции защиты работоспособности прибора

Изготовитель вправе реализовать средства защиты работоспособности прибора, о которых говорится в документе [3] (5.1.3(b) и 5.4), на основе программного обеспечения или аппаратными средствами или же обеспечить возможность поддержки аппаратных средств защиты программным

обеспечением. Соответствующие решения должны содержаться в нормативных документах национального органа по стандартизации и/или рекомендациях МОЗМ.

Если программное обеспечение задействовано в защите работоспособности прибора, то должна быть обеспечена соответствующая реакция прибора. Соответствующий нормативный документ может требовать, чтобы измерительный прибор в случае обнаружения угрозы его работоспособности прекращал работу или формировал сигнал тревоги или соответствующее сообщение.

Пример защиты — (I)/(II) Некоторые виды измерительных приборов необходимо настраивать после заданного интервала времени для того, чтобы гарантировать длительный период измерений. Программное обеспечение по истечении интервала между циклами технического обслуживания выдает сигнал предупреждения и даже останавливает процесс измерений, если период измерения превысил установленный требованиями интервал времени.

5.2 Требования для конкретных вариантов конфигурации

Требования настоящего раздела базируются на типовых технических решениях в области информационных технологий и могут не подходить для всех областей законодательного применения. При соблюдении этих требований возможны технические решения, гарантирующие такую же степень безопасности и соответствия типу, как и измерительные приборы, не имеющие программного управления.

Нижеследующие специальные требования нужны в случаях, когда в измерительных системах применяют определенные технологии. Эти требования должны учитываться в дополнение к требованиям, приведенным в 5.1.

В приводимых примерах демонстрируют как нормальный, так и повышенный уровень жесткости. В настоящем стандарте применяют следующую систему обозначений (см. 5.1):

(I) Технические решения, которые приемлемы в случае нормального уровня жесткости требований.

(II) Технические решения, которые приемлемы в случае повышенного уровня жесткости требований (см. раздел 8).

5.2.1 Определение и разделение значимых частей и определение интерфейсов между частями

Критически важные с метрологической точки зрения части измерительной системы — программная или аппаратная часть — не должны подвергаться недопустимому влиянию со стороны других частей измерительной системы.

Это требование применяется в случае, когда измерительный прибор (электронное устройство, или компоновочный блок) имеет интерфейсы для передачи данных другим электронным устройствам, пользователям или другим частям программного обеспечения помимо критически важных с метрологической точки зрения частей внутри измерительного прибора (электронного устройства, или компоновочного блока).

5.2.1.1 Разделение электронных устройств и компоновочных блоков

5.2.1.1a Компоновочные блоки или электронные устройства измерительной системы, которые выполняют законодательно контролируемые функции, должны быть надлежащим образом идентифицированы, однозначно определены и документально оформлены. Из них формируется законодательно контролируемая часть данной измерительной системы.

Примечание — Инспектирующий специалист решает вопрос о том, является ли эта часть полной и можно ли исключить из дальнейшего рассмотрения другие части измерительной системы.

Примеры законодательно контролируемых устройств

1 (I)/(II) Счетчик электрической энергии оборудован оптическим интерфейсом для подключения электронного устройства, обеспечивающего считывание измеренных значений. В памяти счетчика сохраняются все значимые параметры, их значения и результаты измерений, которые могут считываться в течение достаточно продолжительного интервала времени. В такой системе только счетчик электрической энергии является законодательно контролируемым устройством. Другие устройства, не являющиеся законодательно контролируемыми, могут быть подсоединены к интерфейсу этого прибора при условии выполнения требования 5.2.1.1b. Защита самой передачи данных (см. 5.2.3) не требуется.

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

- цифрового датчика, обеспечивающего вычисление объема или массы;

- универсального компьютера, вычисляющего цену;

- принтера, обеспечивающего распечатку измеренного значения и цены, которую нужно заплатить.

Все компоновочные блоки связаны между собой с помощью локальной сети. В этом случае цифровой датчик, универсальный компьютер и принтер являются законодательно контролируемыми компоновочными блоками и могут по желанию пользователя подключаться к какой-нибудь коммерческой системе, которая не является законодательно контролируемой. Законодательно контролируемые компоновочные блоки должны удовлетворять требованиям 5.2.1.1 b, а также — ввиду того, что передача данных осуществляется через упомянутую сеть — должны удовлетворять требованиям 5.2.3. Никаких требований к коммерческой системе управления не предъявляется.

5.2.1.1b При проведении тестирования в целях утверждения типа должно быть показано, что значимые функции и данные компоновочных блоков и электронных устройств не могут подвергаться недопустимому влиянию со стороны команд, поступающих через интерфейс.

Это значит, что назначение каждой команды должно быть однозначным для всех инициируемых функций или изменений данных в конкретном компоновочном блоке или электронном устройстве.

Примечание — Если «законодательно контролируемые» компоновочные блоки или электронные устройства взаимодействуют с другими компоновочными блоками или электронными устройствами, которые являются «законодательно контролируемыми», то следует обратиться к 5.2.3.

Примеры защиты программного обеспечения

1 (I)/(II) Программное обеспечение счетчика электрической энергии (см. пример 1 в 5.2.1.1a) способно принимать команды для вывода требующихся измеряемых величин. Оно обеспечивает объединение измеренного значения с дополнительной информацией — например, с отметкой времени, единицей изменения — и передачу этого набора данных устройству, от которого поступил запрос. Данное программное обеспечение должно осуществлять прием только тех команд, которые относятся к выводу разрешенных величин, и отвергать любую иную команду, возвращая назад только сообщение об ошибке. Могут быть средства защиты указанного набора данных, но они не являются необходимыми, поскольку передаваемый набор данных не подпадает под законодательный контроль.

2 (I)/(II) Внутри корпуса устройства, который может быть опломбирован, есть выключатель, который определяет режим работы счетчика электрической энергии: одно положение этого выключателя означает верифицированный режим, а другое положение означает неверифицированный режим (возможно применение средств защиты, кроме механического пломбирования; см. примеры в 5.1.3.2a и 5.1.3.2d). При интерпретировании получаемых команд программа должна проверять положение выключателя: в неверифицированном режиме набор команд, которые принимаются программным обеспечением, оказывается расширенным по сравнению с вышеописанным режимом; например, может оказаться возможным регулирование калибровочного коэффициента с помощью команды, которая отвергается в верифицированном режиме.

5.2.1.2 Разделение программного обеспечения на части

ТК и ПК МОЗМ в своих рекомендациях могут определять, какую часть программного обеспечения, аппаратного обеспечения или данных следует отнести к законодательно контролируемым.

Национальные нормативные акты с учетом рекомендаций МОЗМ должны определять, какое программное обеспечение, аппаратные средства, данные или части программного обеспечения, аппаратного обеспечения и данных следует считать законодательно контролируемыми.

5.2.1.2a Все программные модули (программы, подпрограммы, объекты и т. д.), которые выполняют законодательно контролируемые функции или включают в себя законодательно контролируемые области данных составляют часть законодательно контролируемого программного обеспечения измерительного прибора (электронного устройства или компоновочного блока). Требование о соответствии применяется именно к этой части (см. 5.2.5), и она должна быть идентифицирована так, как это описано в 5.1.1.

Если разделение программного обеспечения оказывается невозможным или не нужным, то такое программное обеспечение считают законодательно контролируемым в целом.

Пример выделения законодательно контролируемой части программного обеспечения — (I) Измерительная система состоит из нескольких цифровых датчиков, подключенных к персональной ЭВМ, которая выводит измеренные значения на экран монитора. Законодательно контролируемое программное обеспечение на этой ПЭВМ отделяется от не являющихся законодательно контролируемыми частей программного обеспечения путем объединения всех процедур, реализующих законодательно контролируемые функции, в некую динамически компонуемую библиотеку. Одна или несколько прикладных программ, не являющихся законодательно контролируемыми, могут выполнять выборку соответствующих процедур из этой библиотеки. Благодаря этим процедурам обеспечивается получение измеренных данных от цифровых датчиков, вычисление результатов измерений и их воспроизведение в каком-нибудь программном окне. Когда выполнение законодательно контролируемых функций завершается, контроль возвращается к прикладной программе, не являющейся законодательно контролируемой.

5.2.1.2b Если законодательно контролируемая часть программного обеспечения может устанавливать связь с другими частями программного обеспечения, то должен быть определен программный интерфейс. Вся связь должна осуществляться исключительно через этот интерфейс. Законодательно контролируемая часть программного обеспечения и упомянутый интерфейс должны быть четко документированы. Должны быть описаны все законодательно контролируемые функции и области данных такого программного обеспечения для того, чтобы иметь возможность при утверждении типа прибора решить вопрос о корректности разделения программного обеспечения.

Такой интерфейс состоит из программного кода и выделенных областей данных. Обмен определенными зашифрованными командами или данными между частями программного обеспечения обеспечивается благодаря сохранению упомянутой специально выделенной области данных в памяти одной части программного обеспечения и считыванию данных из нее другой частью программного обеспечения. Управляющая программа записи и считывания данных является частью такого программного интерфейса. Область данных, формирующая данный программный интерфейс, включая управляющую программу, обеспечивающую экспорт данных из законодательно контролируемой части программного обеспечения в область данных интерфейса, и управляющую программу, обеспечивающую импорт данных из интерфейса в законодательно контролируемую часть программного обеспечения, должна быть четко определена и документирована. Операции в обход такого декларированного программного интерфейса не должны допускаться.

Изготовитель прибора несет ответственность за соблюдение этих ограничений. Технические средства (типа пломбирования) для защиты от работы программы в обход упомянутого интерфейса или для предотвращения программирования скрытых команд оказываются невозможными. Программист законодательно контролируемой части программного обеспечения так же, как программист части программного обеспечения, не являющейся законодательно контролируемой, должны получить от изготовителя прибора соответствующие инструкции, касающиеся выполнения этих требований.

5.2.1.2c Должно быть обеспечено однозначное назначение каждой команды для всех инициируемых функций или изменений данных в законодательно контролируемой части программного обеспечения. Команды, с помощью которых осуществляется связь через программный интерфейс, должны декларироваться и документально оформляться. Через программный интерфейс должна допускаться работа только документально оформленных команд. Изготовитель прибора должен заявить полноту документального оформления команд.

Пример реализации программного интерфейса — (I) В примере, описанном в 5.2.1.2a, реализован программный интерфейс с параметрами и возвращаемыми значениями процедур динамически компонуемой библиотеки. Никакие указатели областей данных внутри этой библиотеки не должны возвращаться. Описание этого интерфейса определено в указанной законодательно контролируемой библиотеке, скомпилированной ранее, и не может быть изменено никакой прикладной программой. Устанавливать связь в обход программного интерфейса и адресоваться к областям данных в указанной библиотеке напрямую в принципе возможно, но это плохая практика программирования, которую следует классифицировать как «хакерство».

5.2.1.2d В случаях, когда законодательно контролируемая и не являющееся законодательно контролируемой части программного обеспечения разделены, законодательно контролируемое программное обеспечение должно иметь приоритет в применении ресурсов по отношению к не являющемуся законодательно контролируемым программному обеспечению. Выполнение измерений (реализуемое законодательно контролируемой частью программного обеспечения) не должно задерживаться или блокироваться из-за выполнения других задач.

Изготовитель несет ответственность за соблюдение этого ограничения. Должны быть обеспечены технические средства для предотвращения влияния на законодательно контролируемые функции какой-либо не являющейся законодательно контролируемой программой. Программист законодательно контролируемой части программного обеспечения так же, как программист не являющейся законодательно контролируемой части программного обеспечения, должны получить от изготовителя прибора соответствующие инструкции, касающиеся выполнения этих требований.

Примеры приоритета законодательно контролируемого программного обеспечения

1 (I) В примерах, приводимых в 5.2.1.2a/c, не являющаяся законодательно контролируемой прикладная программа осуществляет запуск законодательно контролируемых процедур указанной библиотеки. Пропуск вызова этих процедур может стать источником задержки выполнения законодательно контролируемой функции системы. Поэтому для удовлетворения требований 5.2.1.2d применяют сле-

дующие меры в рассматриваемом примере: цифровые датчики посылают данные измерений в зашифрованном виде. Ключ для их расшифровки скрыт в упомянутой библиотеке. Только процедуры библиотеки знают этот ключ и могут считывать, расшифровывать и выводить на экран дисплея измеренные значения. Если программист, занимающийся прикладными программами, хочет обеспечить считывание и обработку измеренных значений, то он должен использовать те законодательно контролируемые процедуры указанной библиотеки, которые в случае их вызова выполняют все законодательно контролируемые функции в качестве побочного эффекта. Данная библиотека включает в себя те процедуры, которые обеспечивают экспорт расшифрованных измеренных значений, позволяя занимающемуся прикладными программами программисту использовать их для своих собственных нужд после того, как завершена законодательно контролируемая обработка информации.

2 (I)/(II) Программное обеспечение электронного счетчика электрической энергии считывает необработанные измеренные значения аналого-цифрового преобразователя. Для правильного вычисления измеренных значений критически важное значение имеет задержка между сигналом аналого-цифрового преобразователя «Данные готовы» и моментом окончания буферизации измеренных значений. Необработанные значения считывают с помощью подпрограммы обработки прерываний, инициируемой сигналом «Данные готовы». Измерительный прибор может устанавливать связь через интерфейс с другими электронными устройствами, параллельно обслуживаемыми другой программой обработки прерываний (не являющаяся законодательно контролируемой связь). Если рассмотреть требование 5.2.1.2 для такого варианта конфигурации, то получается, что приоритет программы обработки прерываний для обработки измеренных значений должен быть выше, чем у коммуникационной подпрограммы связи.

Примеры, приводимые в 5.2.1.2a—5.2.1.2c и в 5.2.1.2d (1), являются приемлемыми в качестве технического решения только для нормального уровня жесткости требований (I). Если необходима повышенная защита от мошенничества или повышенная степень соответствия установленным требованиям (см. раздел 8), то разделение программного обеспечения на части оказывается недостаточным, и потребуются дополнительные средства, или все программное обеспечение в целом следует считать подлежащим законодательно контролируемому контролю.

5.2.2 Совместная индикация

Для представления информации, поступающей от законодательно контролируемой части программного обеспечения, и прочей информации можно применять экран дисплея или распечатку данных. Содержание и общая схема размещения данных носят конкретный характер для типа прибора и области его применения и должны быть определены в нормативных документах национального органа по стандартизации и/или соответствующих рекомендациях МОЗМ. Однако если для индикации информации применяют интерфейс пользователя со множеством окон, то действует следующее требование:

Программное обеспечение, осуществляющее индикацию измеряемых значений и другой законодательно контролируемой информации, относится к законодательно контролируемой части программного обеспечения. Окно, в котором находятся эти данные, должно иметь наивысший приоритет, то есть оно не должно удаляться другими программами или подвергаться наложению других окон, формируемых другими программами, либо минимизироваться в размерах или закрываться, пока идет процесс измерения и пока представляемые в этом окне результаты нужны в законодательно контролируемых целях.

Пример совместной индикации — (I) В случае с системой, описывавшейся в 5.2.1.2a—5.2.1.2d, измеряемые значения воспроизводят в отдельном программном окне. Способ, описывавшийся в 5.2.1.2d, гарантирует, что измеряемые значения могут считываться только законодательно контролируемой частью программы. При применении операционной системы с интерфейсом пользователя со множеством окон для удовлетворения требования 5.2.2 применяют дополнительный технический способ: окно, в котором воспроизводятся законодательно контролируемые данные, формируют и контролируют процедурами, находящимися в законодательно контролируемой динамически компонуемой библиотеке (см. 5.2.1.2). В процессе измерений эти процедуры обеспечивают периодическую проверку того, что соответствующее окно попрежнему находится поверх всех прочих открытых окон; если это не так, то благодаря этим процедурам это окно выносится наверх.

Если необходима повышенная степень защиты от мошенничества (II), то распечатки данных в качестве единственного способа индикации может быть недостаточно. Должен иметься некий компоновочный блок с устройствами повышенной безопасности, который может воспроизводить на экране дисплея измеряемые значения.

Применение универсального компьютера как части измерительной системы не является подходящим решением, если необходима повышенная степень защиты от мошенничества (уровень II). В этом

случае следует предусмотреть дополнительные меры предосторожности для предотвращения или минимизации риска мошенничества в форме аппаратных средств или же программных средств, как это обеспечивается при использовании универсального компьютера типа ПЭВМ.

5.2.3 Сохранение данных, передача через системы связи

Если измеряемые значения применяют в ином месте, нежели место измерений, или в более позднее время, нежели время измерений, то они, возможно, должны покидать измерительный прибор (электронное устройство, компоновочный блок) и запоминаться или передаваться через незащищенную среду перед тем, как они будут применяться для законодательно контролируемых целей. В этом случае применяются следующие требования:

5.2.3.1 Запоминаемые или передаваемые измеряемые значения должны сопровождаться всей соответствующей информацией, необходимой для будущего законодательно контролируемого использования.

Пример — (I)/(II) Набор данных может включать в себя следующие элементы:

- измеряемое значение, включая единицу измерения;

- отметку времени измерения (см. 5.2.3.7);

- место измерения или идентификационное обозначение измерительного прибора, который применяют для измерения;

- однозначные идентификационные обозначения измерения, например, порядковые номера, позволяющие присваивать их распечатываемым значениям.

5.2.3.2 Данные должны быть защищены с помощью программных средств, чтобы гарантировать аутентичность, целостность и, если необходимо, корректность информации, касающейся времени измерения. Программа, обеспечивающая воспроизведение на дисплее или дальнейшую обработку измеряемых значений и сопровождающих данных, должна выполнять проверку времени измерения, аутентичности и целостности данных после их считывания из незащищенной памяти или после получения их из незащищенного канала передачи данных. Если обнаруживается искажение, то такие данные следует отбрасывать или маркировать как непригодные для применения.

Программные модули, выполняющие подготовку сохранения или передачи данных, или выполняющие проверку данных после их считывания или получения, относят к законодательно контролируемой части программного обеспечения.

Примечание — При применении открытой сети, разумно требовать более высокого уровня жесткости требований.

Пример программной защиты — (I) Программа устройства, осуществляющего передачу данных, обеспечивает вычисление контрольной суммы конкретного набора данных (с помощью алгоритма типа BCC, CRC16, CRC32 и т. д.) и дополняет ею набор данных. Она применяет некое секретное первоначальное значение для выполнения данного вычисления вместо значения, указанного в стандарте. Это первоначальное значение применяют в качестве ключа и запоминается в качестве некой постоянной в управляющей команде. Программа приема или считывания данных также сохраняет это первоначальное значение в своей управляющей программе. Прежде чем применять полученный набор данных, программа приема данных вычисляет контрольную сумму и сравнивает ее с той, что заложена в данном наборе данных. Если оба эти значения совпадают между собой, то данный набор данных считается не фальсифицированным. В противном случае данная программа считает данные фальсифицированными и удаляет данный набор данных.

5.2.3.3 В случаях с высоким уровнем защиты необходимо применять криптографические методы. Конфиденциальные ключи, применяемые для этой цели, должны быть в секрете, и должна обеспечиваться защита их безопасности в применяемых измерительных приборах, электронных устройствах или компоновочных блоках. Должны быть средства, благодаря которым эти ключи могут только вводиться или считываться, если защита оказывается взломанной.

Пример программной защиты — (II) Программа запоминания или передачи данных формирует «электронную подпись» путем первоначального вычисления хеш-значения[1)] и последующего шифрования этого хеш-значения с помощью секретного ключа криптографической системы с открытым ключом[2)]. В результате получается электронная подпись. Она добавляется в конце сохраненного в памяти

[1)] Приемлемые алгоритмы: SHA-1, MD5, RipeMD160 или их эквиваленты.

[2)] Приемлемые алгоритмы: RSA (ключ длиной 1024 бита), Elliptic Curves (ключ длиной 160 бит) или их эквиваленты.

или переданного набора данных. Принимающая программа также вычисляет хеш-значение этого набора данных и расшифровывает с помощью открытого ключа подпись, добавленную к данному набору данных. Вычисленное и расшифрованное хеш-значения сравниваются между собой. Если они оказываются одинаковыми, то набор данных считается нефальсифицированным (его целостность считается доказанной). Чтобы проверить происхождение набора данных, принимающая программа должна знать, действительно ли данный открытый ключ принадлежит «отправителю», то есть устройству, передающему данные. Поэтому открытый ключ воспроизводится на дисплее измерительного устройства и может быть однократно зарегистрирован, например, вместе с заводским номером данного устройства при законодательно контролируемой верификации на месте эксплуатации. Если принимающая программа уверена в том, что ею применен правильный открытый ключ для расшифровки упомянутой подписи, то аутентичность набора данных считается доказанной.

5.2.3.4 Автоматическое сохранение

5.2.3.4a В случаях, когда с учетом прикладной задачи требуется сохранение данных в памяти, результаты измерений должны сохраняться в памяти автоматически после завершения процесса измерения, то есть когда получено окончательное значение, применяемое для законодательно контролируемых целей.

Запоминающее устройство должно быть достаточно надежным для того, чтобы гарантировать, что при нормальных условиях хранения данные не окажутся разрушенными. Емкость памяти должна быть достаточной для любого практического применения.

В случаях, когда конечное значение, применяемое для законодательно контролируемых целей, получается в результате вычислений, все данные, необходимые для выполнения вычислений, должны автоматически сохраняться в памяти вместе с конечным значением.

Примечание — Интегральные измеряемые значения, например, электроэнергия или объем газа, должны постоянно обновляться. Поскольку при этом всегда применяется одна и та же область данных (программная переменная), требование по емкости памяти в отношении интегральных измерений не применяют.

5.2.3.4b Сохраняемые в памяти данные могут удаляться в том случае, если:

- операция завершена;
- данные распечатаны печатающим устройством, которое подлежит законодательно контролируемому контролю.

Примечание — Национальные нормативные документы (например, налоговые документы) могут содержать строгие ограничения на удаление сохраняемых в памяти данных измерений.

5.2.3.4c При выполнении требований 5.2.3.4b и в тех случаях, когда память оказывается полностью занятой, разрешается удалять сохраненные в памяти данные, когда удовлетворяются оба приведенных ниже условия:

- данные удаляются в той же последовательности, в какой они записывались, при соблюдении правил, установленных для конкретной сферы применения;
- удаление данных осуществляется либо автоматически, либо после специальной ручной операции.

Примечания

1 При применении специальной ручной операции, которая предписывается во втором случае, следует рассмотреть вопрос о дополнительных правах доступа к информации.

2 Национальные нормативные документы (например, налоговые документы) могут содержать перечень пользователей, с которыми следует согласовать удаление данных.

5.2.3.5 Задержка передачи

Не должно быть недопустимого влияния задержки передачи данных на процесс измерения.

5.2.3.6 Прерывание передачи

Если сетевые услуги становятся недоступными, то данные измерений не должны теряться. Во избежание потерь данных процесс измерения должен быть остановлен.

Примечание — Следует рассмотреть вопрос об установлении различия между статическими и динамическими измерениями.

Пример организации передачи данных — (I)/(II) Устройство, отправляющее данные, ждет до того момента, когда принимающее устройство пришлет подтверждение правильного приема набора данных. При этом набор данных сохраняется в буфере устройства до тех пор, пока такое подтверждение

не будет получено. Буфер может иметь емкость, превышающую один набор данных, и может быть организован по принципу простой очереди (принцип FIFO[1)]).

5.2.3.7 Отметка времени

Отметка времени должна считываться с часов устройства. В зависимости от типа измерительного прибора или сферы его применения установка часов может быть законодательно контролируемой операцией, и должны быть приняты соответствующие меры защиты в соответствии с уровнем жесткости применяемых требований (см. 5.1.3.2c).

Внутренние часы автономного измерительного прибора могут иметь довольно большую погрешность, если отсутствуют способы для их синхронизации с астрономическим временем. Но если информация о времени измерения необходима для конкретного применения, то точность внутренних часов измерительного прибора должна быть повышена с помощью специальных средств.

Пример повышения точности внутренних кварцевых часов — (II) Надежность внутренних кварцевых часов измерительного прибора повышается с использованием принципа избыточности: таймер подсчитывает тактовые сигналы часов микроконтроллера, синхронизируемые от другого кварцевого кристалла. Когда таймер досчитает до заданного значения, например до 1 секунды, устанавливается специальный флаг микроконтроллера, и подпрограмма прерываний данной программы формирует приращение показаний второго счетчика. В конце, например, одного дня программное обеспечение считывает показания контролируемых кварцем часов прибора и вычисляет разницу в секундах, с программным счетчиком. Если разница находится в заданных пределах, то программный счетчик сбрасывается до нуля, и данная процедура повторяется; но если указанная разница во времени превышает установленные пределы, то данная программа инициирует соответствующую реакцию исправления ошибок.

5.2.4 Совместимость операционных систем и аппаратного обеспечения, портативность

5.2.4.1 Изготовитель измерительного прибора должен определить минимальные требования к аппаратному и программному обеспечению. Изготовителем должны быть декларированы и указаны в свидетельстве об утверждении типа прибора минимальные ресурсы и подходящая конфигурация (например, процессор, оперативная память, жесткий диск, требования к связи, версия операционной системы и т. д.), которые необходимы для правильного функционирования прибора.

5.2.4.2 В законодательно контролируемом программном обеспечении должны быть предусмотрены технические средства для предотвращения работы в случае, когда не удовлетворяются минимальные требования к конфигурации. Система должна эксплуатироваться только в тех условиях, которые указаны изготовителем для ее правильного функционирования.

Например, если для правильного функционирования системы определены некие неизменные условия, то должны быть предусмотрены средства для сохранения этих условий эксплуатации. Это особенно касается универсального компьютера, выполняющего законодательно контролируемые функции.

Требования к аппаратному обеспечению, операционной системе и общей конфигурации системы универсального компьютера должны учитываться в следующих случаях:

- если требуется высокая степень соответствия требованиям (см. 5.2.5(d));
- если требуется конкретное программное обеспечение (см., например, 5.2.6.3b по вопросу прослеживаемого обновления программного обеспечения);
- если применены криптографические алгоритмы или ключи (см. 5.2.3).

5.2.5 Соответствие изготавливаемого устройства утвержденному типу

Изготовитель должен обеспечивать производство таких устройств и такого законодательно контролируемого программного обеспечения, которые соответствуют утвержденному типу и представленной документации. Существуют разные уровни требований соответствия:

(a) идентичность *законодательно контролируемых функций,* описываемых в документации (см. 6.1), каждого устройства утвержденному типу (исполняемый код может отличаться);

(b) идентичность *частей законодательно контролируемого исходного кода* и соответствие остальных частей законодательно контролируемого программного обеспечения подпункту (a);

(c) идентичность *всего законодательно контролируемого исходного кода в целом*; и

(d) идентичность *всего исполняемого кода в целом.*

В нормативных документах национального органа по стандартизации и/или соответствующих рекомендациях МОЗМ должно указываться, какая степень соответствия является приемлемой. В этих рекомендациях может быть определена подгруппа таких степеней соответствия.

[1)] FIFO: «Первый на входе — первый на выходе».

За исключением случая подпункта (d) в составе программного обеспечения может быть часть программного обеспечения без всяких требований в отношении соответствия, при условии, что эта часть программного обеспечения разделена с законодательно контролируемой частью программного обеспечения согласно 5.2.1.2.

Для того, чтобы сделать соответствие требованиям очевидным, следует применять способы, описываемые в 5.1.1 и 5.2.1.

Примечание — Требования перечислений (a) и (b) должны применяться в случае с нормальным уровнем жесткости требований, а требования перечислений (c) и (d) — в случае с повышенным уровнем жесткости требований.

5.2.6 Техническое обслуживание и реконфигурация

Обновление законодательно контролируемого программного обеспечения измерительного прибора на месте эксплуатации следует рассматривать как:

- модификацию измерительного прибора, когда имеющееся программное обеспечение заменяется программным обеспечением другой утвержденной версии;
- ремонт измерительного прибора, когда повторно устанавливается программное обеспечение той же самой версии.

Для любого измерительного прибора, подвергшегося модификации или ремонту в процессе его эксплуатации, может потребоваться первоначальная или последующая верификация в зависимости от национальных правил.

Программное обеспечение, которое не является необходимым для правильного функционирования измерительного прибора, не требует верификации после его обновления.

5.2.6.1 Разрешается применять только те версии законодательно контролируемого программного обеспечения, которые соответствуют утвержденному типу прибора (см. 5.2.5). Применимость нижеследующих требований зависит от вида измерительного прибора, и этот вопрос должен быть проработан в нормативных документах национального органа по стандартизации и/или соответствующих рекомендациях МОЗМ. Эти требования также могут различаться в зависимости от типа рассматриваемого прибора. Нижеследующие варианты выбора (опции), описываемые в 5.2.6.2 и 5.2.6.3, являются эквивалентными альтернативами. Этот вопрос касается верификации на месте эксплуатации. Дополнительные ограничения приведены в разделе 7.

5.2.6.2 Верифицируемое обновление

Применяемое для обновления программное обеспечение можно загружать на месте, то есть непосредственно в измерительное устройство, либо дистанционно через какую-нибудь сеть. Загрузка и установка программ могут быть выполнены в два разных этапа (как показано на рисунке 1) или могут быть объединены в рамках одного этапа в зависимости от требований конкретного технического решения. На месте установки измерительного прибора должно быть лицо, ответственное за проверку эффективности обновления программного обеспечения. После обновления законодательно контролируемого программного обеспечения измерительного прибора (замены на другую утвержденную версию программного обеспечения или повторной установки старой версии) данный измерительный прибор не разрешается применять в законодательно контролируемых (установленных законодательством) целях, пока не будет выполнена верификация данного прибора согласно процедуре, описываемой в разделе 7, и пока не будут обновлены средства защиты (если только нет иных указаний в нормативных документах национального органа по стандартизации или в свидетельстве об утверждении типа прибора).

5.2.6.3 Прослеживаемое обновление

Программное обеспечение устанавливают в измерительном приборе согласно требованиям к процедуре «Прослеживаемое обновление» (см. 5.2.6.3a—5.2.6.3g) в случае, когда оно допускается нормативными документами национального органа по стандартизации и/или соответствующими рекомендациями МОЗМ. Прослеживаемое обновление является конкретной процедурой изменения программного обеспечения в верифицированном приборе или устройстве, после которой последующая верификация на месте эксплуатации ответственным лицом не является необходимой. Подлежащее обновлению программное обеспечение можно загружать непосредственно в измерительное устройство, либо дистанционно через какую-нибудь сеть. Обновление программного обеспечения регистрируют в контрольном журнале (см. 3.1.2). Процедура «Прослеживаемое обновление» включает в себя несколько этапов: загрузка, проверка целостности, проверка источника (аутентификации), установка, регистрация и активация.

5.2.6.3a Прослеживаемое обновление программного обеспечения должно проводиться автоматически. По завершении процедуры обновления условия защиты программного обеспечения должны быть на том уровне, который требуется для утвержденного типа прибора.

5.2.6.3b Специализированный измерительный прибор (электронное устройство, компоновочный блок) должен иметь постоянную часть законодательно контролируемого программного обеспечения, которая не может быть изменена и в которой есть все функции проверки, необходимые для выполнения прослеживаемого обновления.

5.2.6.3c Должны применяться соответствующие технические средства для того, чтобы гарантировать аутентичность загружаемого программного обеспечения, то есть то, что оно исходит от владельца свидетельства об утверждения типа прибора. Если загружаемое программное обеспечение не может пройти проверку на аутентичность, то оно должно быть забраковано и следует применять предшествующую версию программного обеспечения или переключиться в нерабочий режим.

Пример проверки на аутентичность — (II) Проверку на аутентичность осуществляют с помощью криптографических средств, таких как криптографическая система с открытым ключом. Владелец свидетельства об утверждении типа прибора (каковым обычно является изготовитель данного измерительного прибора) формирует электронную подпись загружаемой версии программного обеспечения с применением секретного ключа. Открытый ключ сохраняют в памяти измерительного прибора в постоянной части его программного обеспечения. Электронная подпись проверяется в автоматическом режиме с помощью открытого ключа при загрузке программного обеспечения в измерительный прибор. Если проверка электронной подписи загружаемого программного обеспечения дает положительный результат, то программное обеспечение устанавливают и активируют; если проверка дает отрицательный результат, то постоянное программное обеспечение бракует это программное обеспечение и использует предшествующую версию программного обеспечения или переключается в нерабочий режим.

5.2.6.3d Должны применяться соответствующие технические средства для того, чтобы гарантировать целостность загружаемого программного обеспечения, то есть того, что оно не подвергалось недопустимым изменениям перед загрузкой. Эта задача может решаться добавлением контрольной суммы или хеш-кода загружаемого программного обеспечения и его тестирования во время процедуры загрузки. В случае, если загружаемое программное обеспечение не проходит такое тестирование, измерительный прибор должен браковать это программное обеспечения и применять предшествующую версию программного обеспечения или переключиться в нерабочий режим. В этом режиме функции измерения должны быть заблокированы. Можно только возобновить процедуру загрузки без пропуска любого этапа из числа указанных на блок-схеме «Прослеживаемое обновление».

5.2.6.3e Чтобы гарантировать, что этапы процедуры «Прослеживаемое обновление» законодательно контролируемого программного обеспечения адекватно отслеживаются внутри данного измерительного прибора, следует применять соответствующие технические средства, например, контрольный журнал, для обеспечения последующей верификации и надзора или инспекции.

В контрольном журнале должна содержаться как минимум следующая информация: успешные или неудачные результаты процедуры обновления программного обеспечения, идентификационное обозначение установленной версии программного обеспечения, идентификационное обозначение предшествующей установленной версии программного обеспечения, отметка времени данного события, идентификационное обозначение партии загрузки. Соответствующую запись делают в этом файле при каждой попытке обновления независимо от того, оказалась она успешной или нет.

Запоминающее устройство, обеспечивающее выполнение процедуры «Прослеживаемое обновление», должно иметь достаточную емкость для того, чтобы обеспечивать гарантии прослеживаемости процедуры «Прослеживаемое обновление» законодательно контролируемого программного обеспечения по меньшей мере между двумя последовательными циклами верификации прибора на месте эксплуатации или при проведении инспекционной проверки. После достижения предельного объема сохраняемых данных контрольного журнала технические средства прибора должны гарантировать, что дальнейшие циклы загрузки программного обеспечения будут невозможны без взлома защиты.

Примечание — Это требование позволяет органам исполнительной власти, осуществляющим функции государственного метрологического надзора за измерительными приборами, используемыми в сфере государственного регулирования обеспечения единства измерений, осуществлять обратное прослеживание процедуры «Прослеживаемое обновление» законодательно контролируемого программного обеспечения таких приборов, за вполне достаточный период времени (зависящий от национального законодательства).

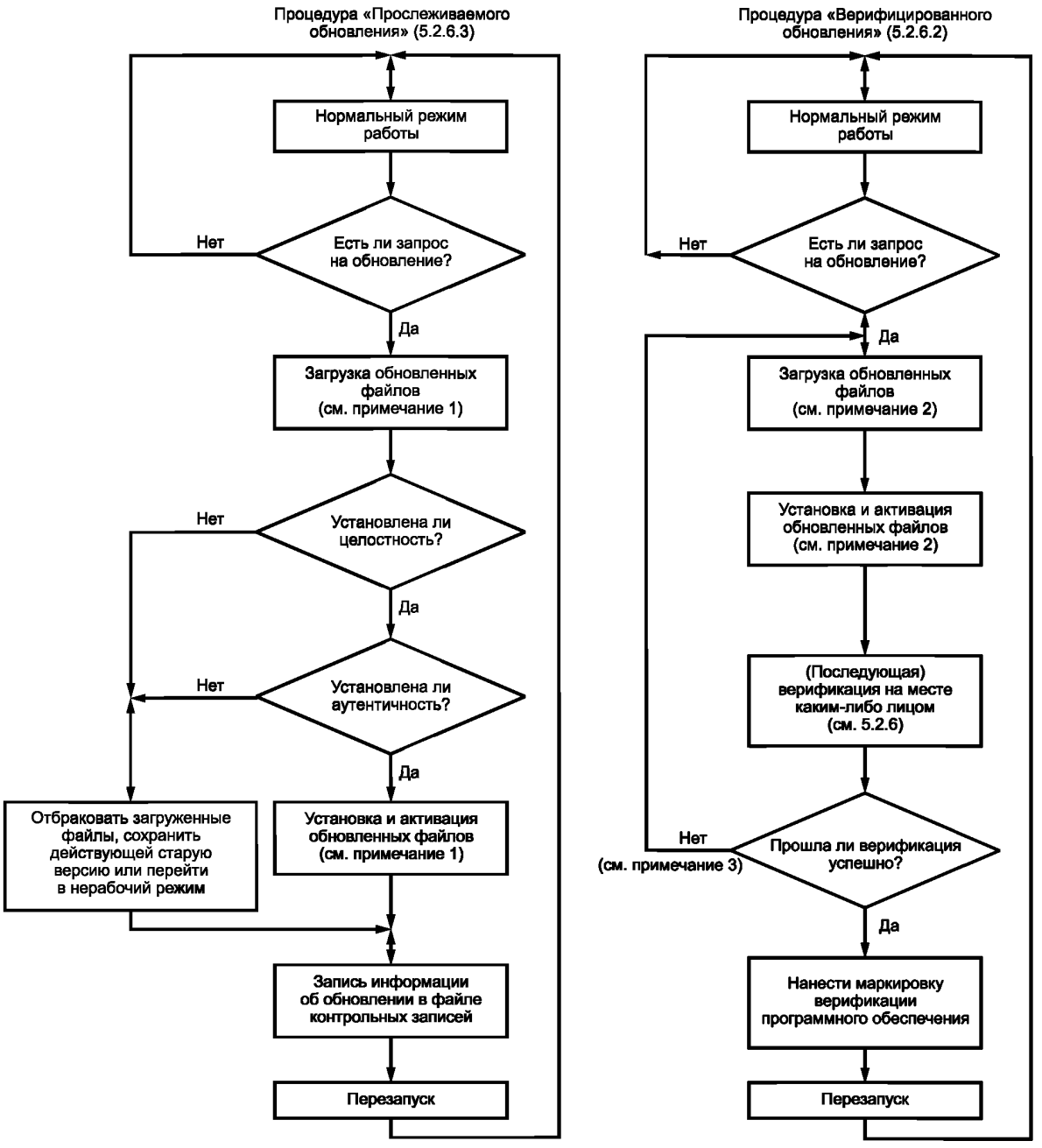


Рисунок 1 — Процедуры обновления программного обеспечения

5.2.6.3f Национальное законодательство может требовать, чтобы пользователь или владелец конкретного измерительного прибора давал свое согласие на загрузку программного обеспечения. В таком случае в измерительном приборе должен быть компоновочный блок или электронное устройство для того, чтобы пользователь или владелец прибора мог выразить свое согласие, например, командная кнопка, нажимаемая перед загрузкой программного обеспечения. Должна быть возможность для включения или отключения данного компоновочного блока или электронного устройства, например, с помощью пломбируемого выключателя, или с помощью какого-нибудь параметра. Если такой компоновочный блок или электронное устройство включено, то каждый цикл загрузки должен инициироваться пользователем или владельцем прибора. Если же этот компоновочный блок или электронное устройство отключено, то для выполнения загрузки программного обеспечения никаких действий со стороны пользователя или владельца прибора не требуется.

5.2.6.3g Если требования 5.2.6.3a—5.2.6.3f не могут быть выполнены, то обновление не являющегося законодательно контролируемым программного обеспечения все же возможно. В этом случае должны выполняться следующие требования:

- имеется четкое разделение между законодательно контролируемым программным обеспечением и не являющимся законодательно контролируемым программным обеспечением согласно 5.2.1;
- законодательно контролируемое программное обеспечение в целом не может быть обновлено без взлома защиты;
- в свидетельстве об утверждении типа прибора указывается, что обновление не являющейся законодательно контролируемой части программного обеспечения является допустимым.

Примечания

1 Процедуру «Прослеживаемое обновление» разделяют на два этапа: «Загрузка» и «Установка/Активация». Это означает, что загружаемое программное обеспечение временно сохраняется после загрузки без активации, потому что должна иметься возможность для отбраковки загруженного программного обеспечения и возврата к старой версии, если проверка принесет отрицательный результат.

2 В случае с процедурой верифицированного обновления программное обеспечение также может загружаться и временно сохраняться в памяти перед его установкой, но в зависимости от принимаемого технического решения установка и активация могут также осуществляться за один этап.

3 Здесь рассматривается только неудачный исход процедуры верификации при обновлении программного обеспечения. В случае неудачного исхода верификации по иным причинам повторная загрузка и повторная установка программного обеспечения, символизируемые ветвью «Нет», не требуются.

5.2.6.4 Нормативные документы национального органа по стандартизации и/или рекомендация МОЗМ могут требовать от пользователя установки определенных значимых параметров устройства. В таком случае измерительный прибор должен быть оборудован устройством для автоматической и нестираемой регистрации любого изменения значимого параметра устройства, например, в контрольном журнале. Конструкцией измерительного прибора должна быть предусмотрена возможность просмотра записанных в контрольный журнал записей.

Примечание — Счетчик событий не является приемлемым решением в этом случае.

5.2.6.5 Средства прослеживания и записи событий относятся к законодательно контролируемому программному обеспечению и должны быть защищены как таковые. Программа, которую применяют для воспроизведения записей контрольного журнала на экране дисплея (см. 5.2.6.2, 5.2.6.3), относится к постоянной части законодательно контролируемого программного обеспечения.

6 Утверждение типа

6.1 Документация, которая должна предоставляться при утверждении типа

При утверждении типа измерительного прибора изготовитель должен декларировать и документировать все программные функции, соответствующие структуры данных и программные интерфейсы законодательно контролируемой части программного обеспечения, которые реализуются в приборе. Никаких скрытых недокументированных функций не должно существовать.

В программной документации, которая должна представляться при утверждении типа прибора, должно быть приведено полное описание команд и результатов их действия. Изготовитель должен констатировать полноту описания команд в документации. Если команды вводят с помощью интерфейса пользователя, то они должны быть полностью описаны в документации по программному обеспечению, которая должна представляться для утверждения типа прибора.

Кроме того, заявка на проведение испытаний в целях утверждения типа прибора должна сопровождаться документом или иным свидетельством того, что принципы разработки и характеристики программного обеспечения измерительного прибора соответствуют требованиям действующих национальных нормативных документов.

6.1.1 Типовая документация (по каждому измерительному прибору, электронному устройству или компоновочному блоку), как правило, включает в себя:

- описание конкретного законодательно контролируемого программного обеспечения и того, как удовлетворяются действующие требования;
- перечень программных модулей, которые относятся к законодательно контролируемой части программного обеспечения (см. приложение В), включая декларацию о том, что в этот перечень включены все законодательно контролируемые функции;

- описание программных интерфейсов законодательно контролируемой части программного обеспечения, имеющихся команд и данных, проходящих через такой интерфейс, включая декларацию о полноте представленного описания (см. приложение В);

- описание принципа формирования идентификационного обозначения программного обеспечения;

- в зависимости от метода аттестации, который выбран в соответствии с 6.3 и 6.4, исходная программа может быть предоставлена в распоряжение испытательной организации в случае, если в нормативных документах национального органа по стандартизации и/или соответствующих рекомендациях МОЗМ требуется высокая степень соответствия требованиям или мощная защита;

- перечень параметров, подлежащих защите и описание средств защиты;

- описание соответствующей конфигурации системы и минимальных требующихся ресурсов (см. 5.2.4);

- описание средств защиты имеющейся операционной системы (пароль и т. п., если требуется);

- описание (программных) методов пломбирования;

- общий обзор аппаратного обеспечения системы, например, топологическая блок-схема, тип компьютера (компьютеров), сети и т. д. В случаях, когда элемент аппаратного обеспечения является законодательно контролируемым или когда он выполняет законодательно контролируемые функции, это должно быть указано;

- описание точности алгоритмов (например, фильтрации результатов аналого-цифрового преобразования, расчета погрешности, алгоритмов округления и т. д.);

- описание интерфейса пользователя, меню и диалогов;

- идентификационное обозначение программного обеспечения и инструкции по его определению в применяемом приборе;

- перечень команд каждого аппаратного интерфейса измерительного прибора, электронного устройства, компоновочного блока, включая декларацию полноты перечня;

- список ошибок, связанных с работоспособностью прибора, которые обнаруживаются с помощью программного обеспечения, и, если это необходимо для понимания, описание алгоритмов обнаружения ошибок;

- описание сохраняемых в памяти или передаваемых наборов данных;

- если в данном программном обеспечении реализуется функция обнаружения неисправностей, то перечень неисправностей, которые могут обнаруживаться, и описание алгоритма обнаружения;

- руководство по эксплуатации.

Примечание — Состав документации, представляемой при утверждении типа прибора, должен быть определен в национальных нормативных документах, действующих в стране.

6.2 Требования к процедуре утверждения

Процедуры тестирования в рамках процедуры утверждения типа, например, те, что описываются в документе [3], базируются на применении четко определяемых режимов и условий тестирования и могут основываться на точных сравнительных измерениях. «Тестирование» и «аттестация» программного обеспечения являются разными процедурами. Правильность или корректность программного обеспечения вообще нельзя измерить в метрологическом смысле, хотя есть стандарты, в которых указывается, как следует «измерять» качество программного обеспечения (например, серия стандартов [7]). В описываемых в указанных документах процедурах учитываются как нужды законодательной метрологии, так и хорошо известные в технике программирования методы аттестации и тестирования, которые, однако, имеют неодинаковые цели (например, в случае с разработчиком программ, который осуществляет поиск погрешностей, но также стремится оптимизировать функциональные характеристики). Как показано в 6.4, каждое требование к программному обеспечению вызывает необходимость индивидуальной адаптации соответствующих процедур аттестации. Усилия, прикладываемые для реализации данных процедур, должны отражать важное значение данных требований в смысле точности, надежности и защиты от неправильного применения.

Цель аттестации заключается в том, чтобы подтвердить, что данный измерительный прибор, подлежащий утверждению типа, соответствует требованиям нормативных документов национального органа по стандартизации и/или соответствующим рекомендациям МОЗМ. В случаях с измерительными приборами с программным управлением процедура аттестации включает в себя проверку, экспертизу и тестирование, и соответствующие рекомендации МОЗМ должны включать в себя набор подходящих методов, описываемых ниже.

Описываемые ниже методы ориентированы на тестирование типа прибора. Верификация каждого отдельно взятого измерительного прибора в условиях эксплуатации не охватывается данными методами аттестации. Дополнительная информация приведена в разделе 7.

Методы, предназначаемые специально для аттестации программного обеспечения, приведены в 6.3. Комбинированные сочетания этих методов, формирующих полную процедуру аттестации, адаптированную под все требования, которые определены в разделе 5, указываются в 6.4.

Примечание — Требования к процедурам утверждения типа должны быть регламентированы национальными стандартами.

6.3 Методы аттестации (экспертиза программного обеспечения)

6.3.1 Обзор методов и их практическое применение

Выбор и последовательность применения описанных в таблице 1 методов не являются строго предписанными и могут быть разными в рамках отдельно взятой процедуры аттестации.

Таблица 1 — Обзор отдельных предлагаемых методов аттестации

Аббревиатура метода	Описание	Применение	Предусловия, инструменты для применения	Специальные навыки для выполнения
AD	Экспертиза документации и аттестация конструкции (6.3.2.1)	Во всех случаях	Документация	
VFTM	Аттестация путем функционального тестирования измерительных функций (6.3.2.2)	Корректность алгоритмов, неопределенность, алгоритмы компенсации и корректировки, правила расчета погрешности	Документация	
VFTSw	Аттестация путем функционального тестирования программного обеспечения (6.3.2.3)	Правильное функционирование связи, средств индикации, защита от мошенничества, от операционных погрешностей, защита параметров, обнаружение неисправностей	Документация, инструменты стандартного программного обеспечения	
DFA	Анализ потока результатов измерений (6.3.2.4)	Разделение программного обеспечения на части, оценка влияния команд на функции измерительного прибора	Исходный код, инструменты стандартного программного обеспечения (простая процедура), специальные инструменты (сложная процедура)	Знание языков программирования. Необходимые инструкции по конкретному методу
CIWT	Проверка и сквозной контроль программ (6.3.2.5)	Для всех целей	Исходный код, инструменты стандартного программного обеспечения	Знание языков программирования, протоколов и других аспектов информационных технологий
SMT	Тестирование программных модулей (6.3.2.6)	Для всех целей, когда могут быть четко определены входные и выходные сигналы	Исходный код, условия проведения испытаний, специальные программные инструменты	Знание языков программирования, протоколов и других аспектов информационных технологий. Инструкции по использованию необходимых инструментов
Примечание — Текстовые редакторы, редакторы шестнадцатиричных кодов и т. д. рассматриваются как «Инструменты стандартного программного обеспечения».				

6.3.2 Описание выбранных методов аттестации

6.3.2.1 Экспертиза документации и аттестация конструкции (AD)

Применение:

Данная процедура является базовой процедурой, которая должна применяться в любом случае.

Предварительные условия:

Данная процедура базируется на документации изготовителя по измерительному прибору. В зависимости от требований документация должна включать в себя:

(1) спецификацию внешних доступных функций измерительного прибора в общем виде (подходит для простых измерительных приборов без всяких интерфейсов за исключением дисплея, возможность верификации всех функций с помощью функционального тестирования, низкий риск мошенничества);

(2) спецификацию программных функций и интерфейсов (необходима для приборов с интерфейсами и для функций приборов, которые невозможно подвергнуть функциональному тестированию, и в случае повышенного риска мошенничества). Описание должно быть понятным и объяснять все программные функции, которые могут влиять на метрологические характеристики;

(3) в части интерфейсов документация должна включать в себя полный перечень команд или сигналов, которые программное обеспечение способно воспринимать. Должна быть детально описана работа каждой команды. Должно быть дано описание того, как измерительный прибор реагирует на не документированные команды;

(4) должна быть предоставлена дополнительная документация по программному обеспечению в случаях наличия сложных алгоритмов измерения, криптографических функций или критически важных ограничений по времени, если это необходимо для понимания и оценки функций программного обеспечения;

(5) в случаях, когда не ясно, как проводить аттестацию какой-либо функции программного обеспечения, на изготовителя должна быть возложена обязанность разработки соответствующего метода тестирования. Кроме того, проводящему обследование эксперту должны быть предоставлены услуги программиста для ответов на его вопросы.

Общим предварительным условием для проверки является полнота документации и четкая идентификация испытуемого оборудования, например, пакетов программ, которые вносят свой вклад в реализацию измерительных функций (см. 6.1.1).

Описание:

Проводящий проверку эксперт оценивает функции и технические особенности измерительного прибора с применением их вербального описания и графических форм представления информации и решает вопрос о том, соответствуют ли они требованиям нормативных документов национального органа по стандартизации и/или соответствующим рекомендациям МОЗМ. Необходимо учесть и оценить метрологические требования, а также функциональные требования к программному обеспечению, определяемые в разделе 5 (например, защита от мошенничества, защита параметров настройки, отказ от выполнения неразрешенных функций, связь с другими устройствами, функция обновления программного обеспечения, функция обнаружения неисправностей и т. д.). Выполнение этой задачи может быть облегчено применением формы «Отчета по оценке программного обеспечения» (см. приложение В).

Результат:

Процедура обеспечивает получение результата для всех характеристик рассматриваемого измерительного прибора при условии, что изготовителем предоставлена соответствующая документация. Этот результат должен быть документально оформлен в разделе, который касается программного обеспечения, в «Отчете по оценке программного обеспечения» (см. приложение В), представленном в виде «Отчета о результатах оценки», приводимого в нормативных документах национального органа по стандартизации и/или соответствующих рекомендациях МОЗМ.

Дополнительные процедуры:

Если при изучении документации не могут быть получены обоснованные результаты аттестации, то следует применять дополнительные процедуры. В большинстве случаев такой процедурой является процедура «Аттестация путем функционального тестирования измерительных функций» (см. 6.3.2.2).

Справочные документы:

Документы [9], [10].

6.3.2.2 Аттестация путем функционального тестирования измерительных функций (метод VFTM)

Применение:

Проверка правильности алгоритмов для вычисления измеренных значений на основе исходных данных, для линеаризации какой-нибудь характеристики, компенсации факторов влияния окружающей среды, округления при расчете погрешности и т. д.

Предварительные условия:

Руководство по эксплуатации, модель функционирования, метрологические справочные материалы и оборудование для тестирования.

Описание:

Большинство методов, применяемых при утверждении типа и тестировании, описываемых в рекомендациях МОЗМ, базируется на выполнении контрольных измерений при различных условиях. Их применение не ограничено рамками определенной технологии создания измерительного прибора. Хотя эти методы не нацелены в первую очередь на аттестацию программного обеспечения, результаты тестирования можно рассматривать как аттестацию некоторых частей программного обеспечения, обычно даже наиболее важных в метрологическом отношении. Если тесты, описанные в соответствующих рекомендациях МОЗМ, охватывают все значимые в метрологическом отношении функции измерительного прибора, то соответствующие части программного обеспечения могут считаться прошедшими аттестацию. Вообще в этом случае для аттестации метрологических особенностей измерительного прибора никакой дополнительной экспертизы или тестирования программного обеспечения проводить не нужно.

Результат:

Алгоритмы корректны или нет, если соответственно они прошли или не прошли аттестацию. Измеряемые значения, получаемые при всех условиях, либо находятся в рамках пределов допускаемой погрешности, либо нет.

Дополнительные процедуры:

Метод, как правило, используют в качестве дополнительного по отношению к методу, описанному в 6.3.2.1. В некоторых случаях более легким и более эффективным способом может быть объединение данного метода с проверками исходного кода (см. 6.3.2.5) или путем моделирования входных сигналов (см. 6.3.2.6), например, для динамических измерений.

Справочные документы:

Конкретные Рекомендации МОЗМ.

6.3.2.3 Аттестация путем функционального тестирования программного обеспечения (метод VFTSw)

Применение:

Аттестация, например, защиты параметров, индикации идентификационного обозначения программного обеспечения, поддерживаемой программным обеспечением функции обнаружения неисправностей, конфигурации конкретной системы (особенно программных средств и т. д.).

Предварительные условия:

Руководство по эксплуатации, документация по программному обеспечению, модель функционирования, оборудование для тестирования.

Описание:

Функциональные особенности, описываемые в руководстве по эксплуатации, документации по измерительному прибору или по программному обеспечению проверяются практически. Если они определяются программным обеспечением, то их следует считать прошедшими аттестацию без дальнейшей экспертизы программного обеспечения, если они функционируют правильно. Адресуемыми в данном случае функциональными особенностями являются, например:

- нормальная работа измерительного прибора в том случае, если его работа контролируется программным обеспечением. Следует проверить все ключи и клавиши и их описанные комбинации и оценить реакцию измерительного прибора на это. В графических интерфейсах пользователя следует активировать и проверить все меню и прочие графические элементы;

- эффективность защиты параметров может проверяться путем активации средств защиты и совершением попытки изменить какой-нибудь параметр;

- эффективность защиты сохраняемых в памяти данных может проверяться путем изменения некоторых данных в конкретном файле и последующей проверки, обнаруживается ли это изменение программой;

- формирование и индикация идентификационного обозначения программного обеспечения могут подвергаться аттестации путем практической проверки данных функций;

- если функция обнаружения неисправностей поддерживается программным обеспечением, то соответствующие части программного обеспечения могут подвергаться аттестации путем провоцирования, реализации или моделирования какой-нибудь неисправности и проверки правильности реакции данного измерительного прибора;

- если конфигурация или программная среда законодательно контролируемого программного обеспечения не должны изменяться, то средства защиты можно проверить путем внесения неразрешенных изменений. Программное обеспечение должно препятствовать этим изменениям или должно прекратить свое функционирование.

Результат:

Рассматриваемая функция, контролируемая программным обеспечением, работает правильно или не работает.

Дополнительные процедуры:

Некоторые особенности или функции измерительного прибора с программным управлением не могут быть практически подвергнуты аттестации так, как это описано. Если прибор имеет интерфейсы, то вообще говоря невозможно обнаружить неразрешенные команды только путем перебора случайных команд. Кроме того, необходимо средство генерации этих команд. Для нормального уровня аттестации метод, описанный в 6.3.2.1, включая декларацию изготовителя, может соответствовать этим требованиям. Для повышенного уровня проверки необходима экспертиза программного обеспечения, аналогичная описанной в 6.3.2.4 или 6.3.2.5.

Справочные документы:

Документы [11], [12], [13].

6.3.2.4 Анализ потока результатов измерений (метод DFA)

Применение:

Создание потока измеряемых значений через области данных, которые подпадают под законодательно контролируемый контроль. Проверка разделения программного обеспечения на части.

Предварительные условия:

Документация по программному обеспечению, исходный код, программа-редактор, программа текстового поиска или специальные инструменты. Знание языков программирования.

Описание:

Цель настоящего метода заключается в выявлении всех частей программного обеспечения, которые связаны с вычислением измеряемого значения или могут оказывать влияние на него. Начиная с аппаратного порта, на который поступают необработанные данные от датчика, проводят поиск подпрограммы чтения данных. Эта подпрограмма будет запоминать данные в какой-нибудь переменной после возможного выполнения некоторых вычислений. Из этой переменной с помощью другой подпрограммы считывают промежуточное значение и так далее до тех пор, пока на дисплей не будет выведено законченное измеренное значение. Все переменные, которые используются в качестве средства сохранения промежуточных измеряемых значений, и все подпрограммы, обеспечивающие передачу этих значений, можно просто найти в исходном коде с помощью текстового редактора и программы текстового поиска для выявления имен этой переменной или подпрограмм в другой программе, нежели та, что на текущий момент времени открыта в упомянутом текстовом редакторе.

С помощью этого метода можно найти другие потоки данных, например, потоки данных от интерфейсов к программе-интерпретатору получаемых команд. Кроме того, можно обнаружить потоки данных в обход программного интерфейса (см. 5.2.1.2).

Результат:

Результат аттестации — правильно осуществлено разделение программного обеспечения согласно 5.2.1.2 или нет.

Дополнительные процедуры:

Настоящий метод рекомендуется в том случае, если реализуется разделение программного обеспечения на части и если требуется высокая степень соответствия требованиям или сильная защита от манипуляций. Этот метод является усилением для методов, описываемых в 6.3.2.1—6.3.2.3 и в 6.3.2.5.

Справочные документы:

Стандарт МЭК 61131-3:2003 «Программируемые контроллеры. Часть 3. Языки программирования (IEC 61131-3:2003 «Programmable controllers — Part 3: Programming languages»).

6.3.2.5 Проверка и сквозной контроль программы (метод CIWT)

Применение:

С помощью настоящего метода можно аттестовать любую особенность программного обеспечения, если необходима усиленная проверка.

Предварительные условия:

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

Описание:

Проводящий проверку эксперт последовательно просматривает исходный код по каждому функциональному назначению, чтобы определить, удовлетворяются ли соответствующие требования и соответствуют ли функции и особенности построения программы имеющейся документации.

Кроме того, эксперт может также сконцентрировать свое внимание на тех алгоритмах или функциях, которые он идентифицировал как сложные, чреватые ошибками, недостаточно документированные и т. д. и может обследовать соответствующую часть этого исходного кода посредством ее экспертизы и проверки в работе.

Перед выполнением этапов этих проверок эксперт должен идентифицировать законодательно контролируемую часть программного обеспечения, например, путем анализа потока результатов измерений (см. 6.3.2.4). Вообще говоря, проверка и сквозной контроль программ ограничивается именно этой частью программного обеспечения. Благодаря объединению этих двух методов объем работы при экспертизе программ становится минимальным по сравнению с практическим применением этих методов в обычном программировании с целью создания безошибочных программ или оптимизации функциональных характеристик.

Результат:

Реализация программного обеспечения совместима с документацией на него и соответствует требованиям или нет.

Дополнительные процедуры:

Настоящий метод является расширенным и дополнительным по отношению к методам, описываемым в 6.3.2.1 и 6.3.2.4. Как правило, настоящий метод применяется только при выборочных проверках.

Справочные документы:

Стандарт [9].

6.3.2.6 Тестирование программных модулей (метод SMT)

Применение:

Только в тех случаях, когда требуется высокая степень соответствия требованиям и защиты от мошенничества. Настоящий метод применяется тогда, когда функции какой-либо программы невозможно проверить исключительно на основе письменной информации. Он подходит и оказывается экономически выгодным при аттестации алгоритмов динамических измерений.

Предварительные условия:

Исходный код, инструментальные средства разработки (по меньшей мере компилятор), среда функционирования для программного обеспечения испытуемого модуля при тестировании, набор входных данных и соответствующий набор точных справочных выходных данных или инструментальные программные средства автоматизации. Навыки в области информационных технологий, знание языков программирования. Рекомендуется сотрудничество с программистом тестируемого программного модуля.

Описание:

Испытуемый программный модуль при тестировании помещается в среду функционирования, представляющую собой специальный программный модуль для проведения тестирования, который связывается с испытуемым программным модулем и снабжает его всеми необходимыми входными данными. Программа тестирования получает выходные данные от испытуемого программного модуля и сравнивает их с ожидаемыми контрольными значениями.

Результат:

Алгоритм измерения или другие тестируемые функции работают либо правильно, либо нет.

Дополнительные процедуры:

Это метод усиленной проверки, применяемый в дополнение к методу, описываемому в 6.3.2.2 или 6.3.2.5. Он применяется только в исключительных случаях.

Справочные документы:

Стандарт [9].

6.4 Процедура аттестации

Процедура аттестации состоит из комбинации методов экспертизы и тестирования. В нормативных документах национального органа по стандартизации и/или соответствующих рекомендациях МОЗМ могут устанавливаться некоторые детали, касающиеся процедуры аттестации, включая следующие:

(a) какой из описанных в 6.3 методов аттестации следует применять;

(b) как оценивать результаты тестирования;

(c) как документировать результаты тестирования (см. приложение В).

В таблице 2 определены два альтернативных уровня требований А и В для процедур аттестации. Уровень В подразумевает расширенную проверку по сравнению с уровнем А. Выбор между процедурами аттестации типов А и типа В может определяться согласно нормативным документам национального органа по стандартизации и/или соответствующей рекомендации МОЗМ — с разным предпочтением или одинаковым предпочтением — в зависимости от ожидаемых:

- риска мошенничества;
- области применения;
- требуемого соответствия утвержденному типу прибора;
- степени риска получения ошибочных результатов измерения из-за погрешностей эксплуатации.

Таблица 2 — Рекомендации по комбинированным сочетаниям методов экспертизы и тестирования для проверки соблюдения разных требований к программному обеспечению (сокращенные названия методов определены в таблице 1)

Требования		Процедура аттестации А (нормальный уровень проверки)	Процедура аттестации В (повышенный уровень проверки)	Замечания
5.1.1	Идентификационное обозначение программы	AD + VFTSw	AD + VFTSw + CIWT	Выбрать «В», если требуется высокая степень соответствия требованиям
5.1.2	Корректность алгоритмов и функций	AD + VFTM	AD + VFTM + CIWT/SMT	
Защита программного обеспечения				
5.1.3.1	Предотвращение неправильного применения	AD + VFTSw	AD + VFTSw	
5.1.3.2	Защита от мошенничества	AD + VFTSw	AD + VFTSw + + DFA/CIWT/SMT	Выбрать «В» в случае высокой степени риска мошенничества
Поддержка аппаратных функций				
5.1.4.1	Поддержка функции обнаружения неисправностей	AD + VFTSw	AD + VFTSw + CIWT + + SMT	Выбрать «В», если требуется высокая степень надежности
5.1.4.2	Поддержка функции защиты работоспособности прибора	AD + VFTSw	AD + VFTSw + CIWT + + SMT	Выбрать «В», если требуется высокая степень надежности
Определение и разделение метрологически значимой и метрологически незначимой частей программного обеспечения, определение интерфейсов между разными частями программного обеспечения				
5.2.1.1	Разделение электронных устройств и компоновочных блоков	AD	AD	
5.2.1.2	Разделение программного обеспечения на части	AD	AD + DFA/CIWT	

Продолжение таблицы 2

Требования		Процедура аттестации А (нормальный уровень проверки)	Процедура аттестации В (повышенный уровень проверки)	Замечания
5.2.2	Совместная функция индикации	AD + VFTM/VFTSw	AD + VFTM/ VFTSw + + DFA/CIWT	
5.2.3	Сохранение данных в памяти, передача данных через коммуникационные системы	AD + VFTSw	AD + VFTSw + + CIWT/SMT	Выбрать «В», если планируется передача данных измерений в открытой системе
5.2.3.1	Сохраняемое в памяти или передаваемое измеренное значение должно сопровождаться всей необходимой информацией для законодательно контролируемого использования в будущем	AD + VFTSw	AD + VFTSw + + CIWT/SMT	Выбрать «В» в случае высокой степени риска мошенничества
5.2.3.2	Данные должны быть защищены с помощью программных средств, чтобы гарантировать аутентичность, целостность и, если необходимо, точность информации о времени измерения	AD + VFTSw		
5.2.3.3	Для высокого уровня защиты необходимо применять криптографические методы	AD + VFTSw	AD + VFTSw + + CIWT/SMT	
5.2.3.4	Автоматическое запоминание	AD + VFTSw	AD + VFTSw + SMT	
5.2.3.5	Задержка передачи данных	AD + VFTSw	AD + VFTSw + SMT	Выбрать «В» в случае высокой степени риска мошенничества, например, в открытых системах
5.2.3.6	Прерывание передачи данных	AD + VFTSw	AD + VFTSw + SMT	Выбрать «В» в случае высокой степени риска мошенничества, например, в открытых системах
5.2.3.7	Отметка времени	AD + VFTSw	AD + VFTSw + SMT	
5.2.4	Совместимость операционных систем и аппаратного обеспечения, портативность	AD + VFTSw	AD + VFTSw + SMT	
Техническое обслуживание и реконфигурирование				
5.2.6.2	«Верифицированное обновление»	AD	AD	
5.2.6.3	«Прослеживаемое обновление»	AD + VFTSw	AD + VFTSw + + CIWT/SMT	Выбрать «В» в случае высокой степени риска мошенничества

6.5 Тестируемое оборудование

Обычно тестирование проводят на полностью укомплектованном измерительном приборе (функциональное тестирование). Если размеры или конфигурация измерительного прибора не позволяют тестировать его в полностью укомплектованном виде или если рассматривается только отдельно взятое устройство (модуль) измерительного прибора, то в нормативных документах национального органа по стандартизации и/или соответствующих рекомендациях МОЗМ может указываться, что все тестирование или отдельные его этапы следует проводить на отдельных электронных устройствах или программных модулях при условии, что в процессе тестирования эти устройства включаются в состав моделирующей схемы, в достаточной мере отображающей нормальный режим работы устройства. Заявитель, представляющий заявку на утверждение типа прибора, несет ответственность за предоставление всего необходимо оборудования и компонентов.

7 Верификация

Если в стране существует метрологический контроль измерительных приборов, то должны быть средства для проверки на месте эксплуатации прибора идентичности программного обеспечения, аттестации настройки и степени соответствия утвержденному типу прибора.

Нормативный документ национального органа по стандартизации и/или соответствующая рекомендация МОЗМ может требовать проведения верификации программного обеспечения за один или большее число шагов согласно характеру рассматриваемого измерительного прибора.

Верификация программного обеспечения должна включать в себя:

- проверку соответствия данного программного обеспечения его утвержденной версии (например, верификация номера версии и контрольной суммы);
- проверку того, что данная конфигурация совместима с декларированной минимальной конфигурацией, если она указана в сертификате утверждения типа;
- проверку того, что параметры входов и выходов измерительного прибора правильно описаны в программном обеспечении в тех случаях, когда эти параметры являются значимыми параметрами устройства;
- проверку того, что значимые параметры устройства (особенно параметры настройки) определены правильно.

Процедуры обновления программного обеспечения описываются в 5.2.6.2 и 5.2.6.3.

8 Оценка уровней жесткости требований

8.1 Настоящий раздел является руководством для определения совокупности уровней жесткости требований, которые должны применяться при тестировании электронных измерительных приборов. Этот раздел не рассчитан на то, чтобы дать некую систему классификации со строгими границами, ведущую к предъявлению особых требований, как это имеет место в случае с системой классификации по точности.

Более того, настоящий стандарт не ограничивает право Технических Комитетов и Подкомитетов в определении таких уровней жесткости требований, которые отличаются от приводимых в настоящем стандарте. В соответствии со специальными ограничениями, предписываемыми нормативными документами национального органа по стандартизации и/или соответствующей рекомендацией МОЗМ, можно применять разные уровни жесткости требований.

8.2 Уровень жесткости требования должен выбираться независимо от того или иного требования.

8.3 При выборе уровней жесткости требований для конкретной категории измерительных приборов и области применения (торговля, прямая продажа населению, здравоохранение, правоприменение и т. д.) могут быть приняты во внимание:

(а) риск мошенничества:

- последствия и социальный и общественный эффект от неправильного выполнения функций;
- стоимость измеряемых товаров;
- применяемая платформа (специально построенная или универсальный компьютер);
- открытость для источников потенциального мошенничества (не контролируемые людьми устройства самообслуживания);

(b) требующееся соответствие утвержденному типу:

- практические возможности промышленности в обеспечении соответствия предписанному уровню жесткости;

(c) требующаяся надежность:

- окружающие условия;
- последствия и социальный и общественный эффект от погрешностей;

(d) интерес для мошенников:

- простая возможность совершить мошенничество может быть достаточным мотивационным фактором;

(e) возможность повторения измерения или его прерывания.

В рамках раздела о требованиях (см. раздел 5) приводятся разные примеры приемлемых технических решений, иллюстрирующие базовый уровень защиты от мошенничества, соответствия утвержденному типу, надежности и типу измерения (отмеченные символом (I)). В соответствующих случаях представляются также примеры усиленных мер противодействия для повышенного уровня жесткости требований по вышеописанным аспектам (отмеченные символом (II)).

Процедура аттестации прибора и уровень жесткости требований неразрывно связаны между собой. В случаях, когда требуется повышенный уровень жесткости требований, следует выполнять подробную экспертизу программного обеспечения, чтобы обнаружить недостатки программного обеспечения или слабости в защите. С другой стороны, при выборе процедуры аттестации следует учитывать механические средства защиты (например, пломбирование коммуникационного порта или корпуса).

Приложение А
(справочное)

Библиография

[1] Международный словарь основных и общих понятий в метрологии (VIM),1993 (International Vocabulary of Basic and General Terms in Metrology (VIM),1993)

[2] МОЗМ В 3:2003 Система сертификации МОЗМ для измерительных приборов (OIML B 3:2003, The OIML Certificate System for Measuring Instruments)

[3] МОЗМ D 11:2004 Общие требования к электронным измерительным приборам (OIML D 11:2004, General requirements for electronic measuring instruments)

[4] ИСО/МЭК 9594-8:2001 Информационные технологии. Взаимодействие открытых систем. Открытый ключ и структуры сертификации атрибутов (ISO/IEC 9594-8:2001 Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks

[5] ИСО 2382-9:1995 Информационные технологии. Словарь. Часть 9. Передача данных (ISO 2382-9:1995, Information technology — Vocabulary — Part 9: Data communication)

[6] МЭК 61508-4:1998 Функциональная безопасность систем электрических/электронных/программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения (IEC 61508-4:1998, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations)

[7] ИСО/МЭК 14598 Стандарты информационных технологий. Развитие программного обеспечения (ISO/IEC 14598 series, Information technology — Software product evaluation)

[8] V 1:2000 Международный словарь терминов в законодательной метрологии (VIML)
(V 1:2000 International vocabulary of terms in legal metrology (VIML))

[9] МЭК 61508-5:1998 Функциональная безопасность электрических/электронных/программируемых электронных систем безопасности. Часть 5. Примеры методов определения уровней полноты безопасности (IEC 61508-5:1998, Functional safety of electrical/electronic/programmable electronic safety related systems — Part 5: Examples of methods for the determination of safety integrity levels)

Примечание — В 2008 году Объединенный комитет по руководствам в области метрологии (JCGM) опубликовал 3-е издание словаря VIM, которое заменяет цитируемое в [1] издание словаря VIM (1993) и представлено в документе JCGM 200:2008 «International vocabulary of metrology — Basic and general concepts and associated Terms (VIM)». Ссылка на официальный перевод указанного документа на русский язык приведена в таблице ДА.1 приложения ДА.

Приложение В
(справочное)

Пример отчета по оценке программного обеспечения

Примечание — Вопрос о том, какую информацию следует включать в «Отчет о тестировании» и в подтверждающий документ, должен решаться в нормативных документах национального органа по стандартизации и/или соответствующих рекомендациях МОЗМ. Например, в «Отчет о тестировании» нижеследующего примера включены наименование, версия и контрольная сумма исполняемого файла.

Отчет о тестировании № XYZ122344
Аттестация программного обеспечения расходомера компании «Tournesol Metering» модели TT100

Программное обеспечение измерительного прибора аттестовалось для того, чтобы продемонстрировать его соответствие требованиям нормативного документа национального органа по стандартизации (рекомендации МОЗМ) № R-xyz.

Аттестация проводилась на основе отчета, содержащегося в Рекомендации МОЗМ D 31:2008, в котором интерпретируются и объясняются важнейшие требования к программному обеспечению. В настоящем отчете описывается проверка программного обеспечения для оценки его соответствия требованиям документа R-xyz.

Изготовитель:	Заявитель:
«Tournesol Metering»	Новая Компания
п/я 1120333	Нова Стрит 123
100 Клоу	1000 Лас Допикос
Силдави	Сан Теодород
Контакт: мистер Трифон Турнесол	Контакт: Арчибальд Хэддок

Объект тестирования

Расходомер TT100 компании «Tournesol Metering» является измерительным прибором, предназначенным для измерения скоростей потока жидкости. Заявленный диапазон измерения скорости потока: от 1 вплоть до 2000 л/с включительно. Измерительный прибор имеет следующие основные функции:

- измерение скорости потока жидкостей;
- индикация измеряемого объема;
- интерфейс с преобразователем.

Расходомер представляет собой специально сконструированный измерительный прибор (измерительную систему) с запоминающим устройством, в котором содержатся законодательно контролируемые данные.

Расходомер TT100 является независимым измерительным прибором, который укомплектован преобразователем. Преобразователь имеет встроенную функцию температурной компенсации. Регулировка скорости потока возможна с помощью калибровочных параметров, хранящихся в энергонезависимой памяти преобразователя. Преобразователь крепится к измерительному прибору и не может отсоединяться от него. Индикация измеряемого объема обеспечивается на экране дисплея. Никакая связь с другими устройствами не является возможной.

Встроенное программное обеспечение измерительного прибора разработано компанией:

«Tournesol Metering», п/я 1120333, 100 Клоу, Силдави.

Наименование исполняемого файла: **«tt100_12.exe»**.

Прошедшая аттестацию версия программного обеспечения: **V1.2c**. Номер версии программного обеспечения выводится на экран дисплея при запуске устройства и нажатии кнопки «УРОВЕНЬ» в течение 4 секунд.

Исходная программа состоит из следующих законодательно контролируемых файлов:

- main.c	12301 байт	23 ноября 2003 года;
- int.c	6509 байтов	23 ноября 2003 года;
- filter.c	10897 байтов	20 октября 2003 года;
- input.c	2004 байта	20 октября 2003 года;
- display.c	32000 байтов	23 ноября 2003 года;
- ethernet.c	23455 байтов	15 июня 2002 года;
- driver.c	11670 байтов	15 июня 2002 года;
- calculate.c	6788 байтов	23 ноября 2003 года.

Исполняемый файл **«tt100_12.exe»** защищен от изменений с помощью контрольной суммы. Значение контрольной суммы согласно алгоритму **XYZ** равно **1A2B3C**.

Аттестация основывалась на следующих документах изготовителя:

- Руководство пользователя прибора TT 100, выпуск 1.6;
- Руководство по техническому обслуживанию прибора TT 100, выпуск 1.1;

- Описание программного обеспечения к прибору ТТ 100 (внутренний проектный документ от 22 ноября 2003 года);

- Электронная схема прибора ТТ 100 (чертеж № 222-31 от 15 октября 2003 года).

Окончательная версия объекта тестирования была передана в Национальную испытательную и Измерительную лабораторию 25 ноября 2003 года.

Выполнение аттестации

Аттестация выполнялась в соответствии с Рекомендацией МОЗМ D 31:2008. Аттестация выполнялась в период с 1 ноября по 23 декабря 2003 года. Обсуждение результатов аттестации было проведено 3 декабря доктором К.Фелером (K.Fehler) в штаб-квартире компании «Tournesol Metering» в Клоу. Прочие работы по аттестации прибора проводились в Национальной Испытательной и Измерительной Лаборатории доктором К.Фелером и мистером С.Проблюмом (S.Problume).

Требования, соблюдение которых проверялось при аттестации:

- идентификация программного обеспечения;
- корректность алгоритмов и функций;
- защита программного обеспечения;
- защита от случайного нарушения правил применения;
- защита от мошенничества;
- поддержка аппаратных функций;
- сохранение данных в памяти, передача данных через коммуникационные системы.

Применялись следующие методы аттестации:

- экспертиза документации и аттестация конструкции;
- аттестация измерительных функций с помощью функционального тестирования;
- сквозной контроль, проверка программы;
- тестирование программного модуля calculate.c с помощью SDK XXX.

Результат

В результате аттестации не выявлено нарушения требований следующих пунктов Рекомендации МОЗМ D 31:2008:

5.1.1; 5.1.2; 5.1.3.2; 5.2.1; 5.2.2.1; 5.2.2.2; 5.2.2.3.

Было обнаружено, что в «Руководстве оператора» не были первоначально описаны две команды. Эти две команды были включены в «Руководство оператора», которое датировано 10 декабря 2003 года.

В пакете программ V1.2b была обнаружена ошибка программного обеспечения, из-за которого февраль месяц ограничивался только 28 днями даже в високосный год. Эта ошибка исправлена в пакете программ версии V1.2c.

Приведенные результаты действительны только для тестировавшегося прибора с заводским номером 1188093-B-2004.

Заключение

Программное обеспечение прибора модели **ТТ 100** компании **«Tournesol Metering»**, версия V1.2c, отвечает требованиям нормативного документа национального органа по стандартизации (рекомендации МОЗМ) R-xyz.

Национальная испытательная и измерительная лаборатория,

Отдел программного обеспечения,

Д-р К.Э.И.Н.Фелер — м-р С.А.Н.С.Проблюм

Технический директор — Технический специалист

Перечень проверок

Пункт	Требование	Годен	Не годен	Примечания
5.1 **5.1.1**	**Общие требования** **Идентификация программного обеспечения** Законодательно контролируемое программное обеспечение должно быть четко идентифицировано			
5.1.2	**Корректность алгоритмов и функций** Алгоритмы измерения и функции измерительного прибора должны быть корректными			
5.1.3 **5.1.3.1**	**Защита программного обеспечения** **Предотвращение неправильного применения** Измерительный прибор — особенно его программное обеспечение — должен быть сконструирован таким образом, чтобы возможности непреднамеренного случайного неправильного применения были минимальными			

Пункт	Требование	Годен	Не годен	Примечания
5.1.3.2 a) b) c) d)	**Защита от мошенничества** Законодательно контролируемое программное обеспечение должно быть защищено от неразрешенных изменений, загрузки или изменений посредством дозагрузки памяти прибора. Помимо механического пломбирования могут оказаться необходимыми другие технические средства защиты измерительного прибора, имеющего операционную систему или опцию для загрузки программного обеспечения. С помощью интерфейса пользователя разрешается активировать только четко документированные функции (см. 6.1). Интерфейс пользователя должен быть реализован таким образом, чтобы он не способствовал мошенническому использованию. Форма представления информации должна отвечать требованиям 5.2.2. Параметры, определяющие законодательно контролируемые характеристики измерительного прибора, должны быть защищены от несанкционированных изменений. Если это необходимо в целях верификации прибора, то должна быть возможность воспроизведения на дисплее или распечатки текущих значений параметров настройки. Защита программного обеспечения включает соответствующую защиту с помощью механических, электронных и/или криптографических средств, делающих невозможным или очевидным любое несанкционированное вмешательство			
5.1.4 5.1.4.1	**Поддержка аппаратных функций** **Поддержка функции обнаружения неисправностей** От изготовителя измерительного прибора следует требовать включения средств проверки или контроля в программную или аппаратную части прибора или требовать создания средств, с помощью которых отдельные части аппаратного обеспечения могли бы поддерживаться отдельными частями программного обеспечения данного прибора			
5.1.4.2	**Поддержка функции защиты работоспособности прибора** По своему выбору изготовитель может реализовать средства защиты работоспособности прибора в программном или аппаратном обеспечении прибора либо обеспечить поддержку аппаратных средств защиты со стороны программного обеспечения			
5.2 5.2.1	**Требования для конкретных вариантов конфигурации** **Выделение и разделение законодательно контролируемых и не являющихся законодательно контролируемыми частей и определение интерфейса между ними** Критически важные с метрологической точки зрения части измерительной системы не должны подвергаться недопустимому влиянию со стороны других частей данной измерительной системы			
5.2.1.1 a) b)	**Разделение электронных устройств и компоновочных блоков** Компоновочные блоки или электронные устройства измерительной системы, которые выполняют законодательно контролируемые функции, должны быть идентифицированы, четко определены и документированы. При тестировании в целях утверждения типа прибора необходимо продемонстрировать, что значимые функции и данные компоновочных блоков и электронных устройств не могут подвергаться влиянию команд, получаемых через интерфейс			
5.2.1.2 a)	**Разделение программного обеспечения на части** Требование о соответствии типу действует в отношении законодательно контролируемой части программного обеспечения измерительного прибора (см. 5.2.5), и эта часть должна быть идентифицируемой, как это описывается в 5.1.1.			

Пункт	Требование	Годен	Не годен	Примечания
b)	Если законодательно контролируемая часть программного обеспечения имеет связь с другими частями программного обеспечения, то должен быть определен интерфейс для программного обеспечения. Вся связь должна осуществляться исключительно через данный интерфейс. Законодательно контролируемая часть программного обеспечения и интерфейс должны быть четко документированы. Должно быть дано описание всех законодательно контролируемых функций и областей данных программного обеспечения для того, чтобы организация, утверждающая тип прибора, могла решить вопрос о правильности разделения программного обеспечения.			
c)	Каждая команда должна быть однозначно определена для всех инициируемых функций или данных в законодательно контролируемой части программного обеспечения. Команды, которые передаются через интерфейс программного обеспечения, должны быть задекларированы и документированы. Только документированные команды разрешается активировать через указанный интерфейс. Изготовитель должен констатировать полноту документации по командам.			
d)	В тех случаях, когда законодательно контролируемое программное обеспечение разделено с не являющимся законодательно контролируемым программным обеспечением, законодательно контролируемое программное обеспечение должно иметь приоритет в применении ресурсов перед не являющимся законодательно контролируемым программным обеспечением			
5.2.2	**Совместная индикация** Если индикация результатов осуществляется с помощью интерфейса пользователя со множеством окон, то тогда действует следующее требование: - Программное обеспечение, которое реализует задачу индикации измеряемых значений и прочей законодательно контролируемой информации, относится к законодательно контролируемой части программного обеспечения. Окно, в котором содержатся эти данные, должно иметь самый высокий приоритет			
5.2.3 5.2.3.1	**Сохранение данных, передача через коммуникационную систему** Сохраняемое или передаваемое измеренное значение должно сопровождаться соответствующей информацией, необходимой для законодательно контролируемого применения в будущем			
5.2.3.2	Данные должны быть защищены с помощью программных средств для того, чтобы гарантировать аутентичность, целостность и, если необходимо, точность информации о времени измерения. Программа, которая обеспечивает вывод на дисплей или дальнейшую обработку измеренных значений и сопроводительных данных, должна проверять время измерения, аутентичность и целостность данных после их считывания из незащищенной памяти или после их получения из незащищенного канала передачи данных. Если обнаруживается искажение данных, то такие данные должны быть забракованы или помечены как непригодные для применения			
5.2.3.3	Для обеспечения высокого уровня защиты необходимо применять криптографические методы			
5.2.3.4 a)	**Автоматическое сохранение** Когда процесс измерения завершается, данные измерений должны сохраняться в памяти автоматически. Запоминающее устройство должно обладать достаточной стойкостью для того, чтобы гарантировать, что данные не будут нарушаться при нормальных условиях хранения в памяти. Емкость памяти должна быть достаточной для любой конкретной цели применения. Когда окончательное значение, применяемое для законодательно контролируемых целей, получается в результате вычислений, вместе с окончательным значением должны сохраняться в памяти автоматически все данные, необходимые для вычислений.			

Пункт	Требование	Годен	Не годен	Примечания
b) c)	Сохраняемые в памяти данные могут удаляться: - если операция полностью завершена; - если эти данные распечатываются принтером, подпадающим под законодательный контроль. После того, как требования 5.2.3.4b оказываются выполненными, и когда память оказывается заполненной полностью, разрешается удалять сохраненные в памяти данные в тех случаях, когда удовлетворяются следующие условия: - данные удаляются в той же последовательности, в какой они записывались, и соблюдаются правила, установленные для конкретной цели применения; - удаление данных осуществляется либо автоматически, либо после специальной операции, выполняемой вручную			
5.2.3.5	**Задержка передачи** Любая задержка передачи данных не должна оказывать недопустимого влияния на процесс измерения			
5.2.3.6	**Прерывание передачи** Если сетевые услуги становятся недоступными, то не должно происходить никаких потерь данных. Процесс измерения может быть остановлен для того, чтобы избежать потерь данных измерений			
5.2.3.7	**Отметка времени** Отметка времени должна считываться с часового механизма конкретного устройства. Должны быть предприняты меры защиты, соответствующие применяемому уровню жесткости требований (см. 5.1.3.2.c). Если необходима информация о времени измерения, то с помощью специальных средств следует повысить надежность внутреннего часового устройства данного измерительного прибора			
5.2.4 5.2.4.1	**Совместимость операционных систем и аппаратного обеспечения, портативность** Изготовитель должен идентифицировать приемлемые аппаратные средства и программное обеспечение. Изготовитель должен декларировать минимальные ресурсы и конфигурацию, которые необходимы для правильного функционирования измерительного прибора			
5.2.4.2	Должны быть предусмотрены соответствующие технические средства для предотвращения работы прибора в том случае, если не соблюдаются минимальные требования в отношении конфигурации.			
5.2.6 5.2.6.1	**Техническое обслуживание и реконфигурация** Разрешается применять только те версии законодательно контролируемого программного обеспечения, которые соответствуют программному обеспечению утвержденного типа прибора			
5.2.6.2	**Верифицируемое обновление** После обновления законодательно контролируемого программного обеспечения измерительного прибора (замена на другую утвержденную версию или повторная установка старой версии) данный измерительный прибор нельзя использовать для законодательных целей до того, как будет выполнена верификация данного прибора и будут обновлены средства обеспечения безопасности			
5.2.6.3 a)	**Прослеживаемое обновление** Процедура «Прослеживаемое обновление» программного обеспечения должна выполняться автоматически. После завершения процедуры обновления программного обеспечения условия защиты программного обеспечения должны быть на том уровне, какой требуется согласно утвержденному типу измерительного прибора.			

Пункт	Требование	Годен	Не годен	Примечания
b)	Специализированный измерительный прибор должен иметь постоянную часть законодательно контролируемого программного обеспечения.			
c)	Соответствующие технические средства следует применять для того, чтобы гарантировать аутентичность загруженного программного обеспечения. Если загруженное программное обеспечение не проходит проверку на аутентичность, измерительный прибор должен браковать его и использовать прежнюю версию программного обеспечения или переключиться в нерабочий режим.			
d)	Соответствующие технические средства следует применять для того, чтобы гарантировать целостность загруженного программного обеспечения, то есть то, что оно не подверглось недопустимым изменениям перед его загрузкой.			
e)	Соответствующие технические средства следует применять, чтобы гарантировать, что процедуры «Прослеживаемое обновление» могут быть адекватно отслеживаемыми внутри данного измерительного прибора.			
f)	Измерительный прибор должен иметь компоновочный блок или электронное устройство для того, чтобы пользователь или владелец прибора мог выразить свое согласие. Должна быть возможность для включения и выключения такого компоновочного блока или электронного устройства, например, с помощью выключателя, который может пломбироваться, или с помощью какого-нибудь параметра. Если данный компоновочный блок или электронное устройство оказывается включенным, то каждая загрузка программного обеспечения должна инициироваться пользователем или владельцем данного измерительного прибора. Если же данный компоновочный блок или электронное устройство заблокировано, то никакая деятельность пользователя или владельца данного измерительного прибора не требуется.			
g)	Если требования 5.2.6.3(a)—5.2.6.3(f) не могут быть выполнены, то все же остается возможность для обновления той части программного обеспечения, которая не является законодательно контролируемой. В этом случае должны быть выполнены следующие требования: - существует четкое разделение между законодательно контролируемой частью программного обеспечения и не являющейся законодательно контролируемой частью программного обеспечения в соответствии с 5.2.1; - обновление всей законодательно контролируемой части программного обеспечения является невозможным без взлома защиты; - в свидетельстве об утверждении типа указывается, что обновление не являющейся законодательно контролируемой части программного обеспечения является допустимым			
5.2.6.4	Измерительный прибор должен быть оснащен устройством для выполнения автоматической нестираемой записи любого случая регулирования значимого параметра конкретного устройства, например контрольным журналом. Измерительный прибор должен быть способен представлять записываемые в контрольный журнал данные			
5.2.6.5	Средства отслеживания и записи являются частью законодательно контролируемого программного обеспечения и должны быть защищены как таковые			

Приложение С
(справочное)

Предметный указатель

Аттестация: 3.1.56; 4.3; 6.1.1; 6.2; 6.3; 6.3.1; 6.3.2; 6.3.2.1; 6.3.2.2; 6.3.2.3; 6.3.2.4; 6.3; 6.3.2; 6.4; 8.3; Приложение В.
Аутентификация: 3.1.3; 3.1.4; 5.2.6.3, Библиография, Приложение ДА.
Аутентичность: 3.1.4; 3.1.11; 5.1.3.2d; 5.2.3.2; 5.2.3.3; 5.2.6.3c, 6.4; Приложение В.
Верификация: 3.1.57; 5.1.3.2c; 5.2.3.3; 5.2.6; 5.2.6.1; 5.2.6.2; 5.2.6.3; 5.2.6.3e; 6.2; 6.3.2.1; 7; Приложение В.
Законодательно контролируемый: 3.1.2; 3.1.29; 3.1.43; 3.1.46; 3.1.48; 5.1.3.1; 5.1.3.2a; 5.1.3.2c; 5.1.3.2d; 5.1.4.1; 5.2.1.1a; 5.2.1.1b; 5.2.1.2; 5.2.1.2a; 5.2.1.2b; 5.2.1.2c; 5.2.1.2d; 5.2.2; 5.2.3; 5.2.3.1; 5.2.3.2; 5.2.3.3, 5.2.3.4a: 5.2.3.4в; 5.2.3.7; 5.2.4.2; 5.2.5; 6.1.1; 6.4; Приложение В.
Законодательно контролируемый параметр: 3.1.13; 3.1.30; 3.1.53.
Законодательно контролируемая часть программного обеспечения: 3.1.24; 3.1.31; 3.1.53; 5.1.1; 5.1.3.2a; 5.1.3.2b; 5.2.1.2a—5.2.1.2d; 5.2.3.2; 5.2.4.2; 5.2.5; 5.2.6; 5.2.6.1; 5.2.6.2; 5.2.6.3b; 5.2.6.3e; 5.2.6.3g; 5.2.6.5; 6.1; 6.1.1; 6.3.2.3; 6.3.2.5.
Закрытая сеть: 3.1.6; 3.1.35.
Запоминающее устройство: 3.1.22; 3.1.48; 5.1.3.2a; 5.2.3.4a; 5.2.6.3e; Приложение В.
Защита: 3.1.39; 3.1.45; 5.1.3; 5.1.3.2; 5.1.3.2d; 5.2.1.1a; 5.2.1.1b; 5.2.2; 5.2.6.2; 6.1.1: 6.3.1; 6.3.2.1; 6.3.2.4; Приложение В.
Защита программного обеспечения: 2.1.45; 5.1.3; 5.1.3.2d; 5.2.6.3a; 6.4; Приложение В.
Значимый параметр типа прибора: 3.1.30; 2.1.53; 5.1.3.2c.
Значимый параметр устройства: 3.1.13; 2.1.30; 5.1.3.2c; 5.2.6.4; 7, Приложение В.
Идентификация программного обеспечения: 3.1.42; 5.1.1; 5.2.6.3e; 6.1.1; 6.3.2.3; 6.4; Приложение В.
Измерительный прибор: Введение; 1.1; 1.2; 1.3; 3.1.5; 2.1.7; 3.1.9; 3.1.10; 3.1.14; 3.1.15; 3.1.16; 3.1.19; 3.1.20; 3.1.22; 3.1.23; 3.1.24; 3.1.28; 3.1.29; 3.1.30; 3.1.31; 3.1.32; 3.1.33; 3.1.36; 3.1.38; 3.1.44; 3.1.45; 3.1.46; 3.1.55; 3.1.57; 4.3; 5.1; 5.1.1; 5.1.3.1; 5.1.3.2a; 5.1.3.2c; 5.1.3.2d; 5.1.4.1; 5.1.4.2; 5.2; 5.2.1; 5.2.1.1a; 5.2.1.2.a; 5.2.1.2d; 5.2.3; 5.2.3.1; 5.2.3.3; 5.2.3.7; 5.2.4.1; 5.2.6; 5.2.6.1; 5.2.6.2; 5.2.6.3; 5.2.6.3b; 5.2.6.3c; 5.2.6.3d; 5.2.6.3e; 5.2.6.3f; 5.2.6.4; 6.1; 6.1.1; 6.2; 6.3.1; 6.3.2.1; 6.3.2.2; 6.3.2.3; 6.5; 7; 8.1; Приложение В.
Интерфейс: 3.1.7; 3.1.9; 3.1.27; 3.1.43; 3.1.46; 3.1.55; 5.1.1; 5.1.2; 5.1.3.2b; 5.2.1; 5.2.1.1.a; 5.2.1.1.b; 5.2.1.2.b; 5.2.1.2.c; 5.2.1.2.d; 5.2.2; 6.1; 6.1.1; 6.3.2.1; 6.3.2.3; 6.3.2.4; 6.4; Приложение В.
Интерфейс пользователя: 3.1.7; 3.1.55; 5.1.1; 5.1.3.2.b; 5.2.2; 6.1; 6.1.1; 6.3.2.3, Приложение В.
Интерфейс связи: 3.1.9; 5.1.1.
Исполняемый код: 3.1.22; 3.1.24; 3.1.37; 3.1.47; 5.1.1; 5.2.5; Приложение В.
Испытания (типа прибора): 3.1.19; 6.1; 6.3.1.
Исходный код: 3.1.37; 3.1.47; 5.2.5; 6.3.1; 6.3.2.2; 6.3.2.4; 6.3.2.5; 6.3.2.6.
Команды: 3.1.7; 5.1.3.2.b; 5.2.1.1.b; 5.2.1.2.b; 5.2.1.2.c; 5.2.3.2; 6.1; 6.1.1; 6.3.1; 6.3.2.1; 6.3.2.3; 6.3.2.4; Приложение В.
Компоновочный блок (узел): 3.1.7; 3.1.8; 3.1.9; 3.1.16; 2.1.22; 3.1.30; 3.1.31; 3.1.44; 3.1.46; 3.1.49; 5.1; 5.1.1; 5.1.3.2a; 5.2.1; 5.2.1.1; 5.2.1.1a; 5.2.1.1b; 5.2.1.2a; 5.2.2; 5.2.3; 5.2.3.3; 5.2.6.3b; 5.2.6.3f; 6.1.1.
Контрольный журнал: 3.1.2; 5.1.3.2.d; 5.2.6.3; 5.2.6.3.e; 5.2.6.4; 5.2.6.5, Приложение В.
Контрольное устройство: 3.1.5; 5.1.4.1.
Криптографический сертификат: 3.1.10; 3.1.11; 5.1.3.2d.
Криптографические средства: 3.1.11; 5.1.3.2a; 5.1.3.2d; 5.2.6.3c.
Неисправность: 3.1.18; 3.1.23; 5.1.4.1; 6.1.1; 6.3.1; 6.3.2.1; 6.3.2.3; 6.4; Приложение В.
Непрерываемое/прерываемое измерение: 3.1.34; 5.1.4.1.
Область данных: 3.1.12; 3.1.43; 3.1.44; 3.1.45; 5.2.1.2.a; 5.2.1.2.b; 5.2.1.2.c; 5.2.3.4.a; 6.3.2.4.
Основная погрешность: 3.1.28.
Открытая сеть: 3.1.6; 3.1.35; 5.2.3.2.
Отметка времени: 3.1.2; 3.1.51; 5.2.1.1.b; 5.2.3.1; 5.2.3.7; 5.2.6.3e; 6.4.
Передача данных измерений: 3.1.7; 3.1.52; 5.2.1; 5.2.11a; 5.2.3; 5.2.3.2; 5.2.3.5; 5.2.3.6; 6.4; Приложение В.
Пломбирование: 3.1.38; 3.1.45, 5.1.3.2a; 5.1.3.2d; 5.2.1.2b; 6.1.1; 8.3.
Погрешность (показания): 3.1.17; 3.1.23; 3.1.32; 5.2.3.7; 6.1.1; 6.2; 6.3.1; 6.3.2.5; 6.4; 8.3.
Постоянная часть законодательно контролируемого программного обеспечения: 3.1.24; 5.2.6.3b; 5.2.6.3c; 5.2.6.5.
Предел допускаемой погрешности (измерительного прибора): 3.1.23; 3.1.32; 6.3.2.2.
Приемлемое решение: 3.1.1; 5.1; 5.1.1; 5.1.3.2d; 5.2; 5.2.1.2d; 5.2.6.4; 8.3.
Проверка программного обеспечения: 3.1.41; 5.1.2; Приложение В.
Программный интерфейс: 3.1.43; 3.1.46; 5.2.1.2b; 5.2.1.2c; 6.1; 6.1.1; 6.3.2.4.

Программный модуль: 3.1.1; 3.1.8; 3.1.12; 3.1.20; 3.1.31; 3.1.42; 3.1.43; 3.1.44; 5.1.3.2.b; 5.2.1.2a; 5.2.3.2; 6.1.1; 6.3.1; 6.3.2.6; 6.5; Приложение В.
Работоспособность: 3.1.14; 5.1.4.2; 6.1.1; 6.4, Приложение В.
Разделение программного обеспечения: 3.1.46; 5.2.1.2b; 5.2.1.2d; 6.3.1; 6.3.2.4.
Связь: 3.1.8; 2.1.46; 3.1.52; 5.1.3.2a; 5.2.1.2b; 5.2.1.2d; 5.2.3; 5.2.4.1; 6.3.1; 6.3.2.1; 6.4; 8.3; Приложение В.
Событие: 3.1.2; 3.1.20; 3.1.21; 3.1.51; 5.1.3.2.d; 5.2.6.3.e; 5.2.6.4.
Счетчик событий: 3.1.21; 5.1.3.2d; 5.2.6.4.
Тестирование: 3.1.16; 3.1.50; 3.1.56; 5.1.2; 5.2.1.1b; 5.2.6.3d; 6.2; 6.3.1; 6.3.2.1; 6.3.2.2; 6.3.2.3; 6.3.2.6; 6.4; 6.5; 8.1; Приложение В.
Универсальный компьютер: 3.1.54; 5.1.3.2.a; 5.2.1.1.a; 5.2.2; 5.2.4.2; 8.3.
Файл регистрации ошибок: 3.1.18; 5.1.4.1.
Функциональная характеристика: 3.1.14; 3.1.36; 6.2; 6.3.2.5.
Хеш-функция: 3.1.11; 3.1.25; 5.2.3.3; 5.2.6.3.d.
Целостность программ, данных или параметров: 3.1.26; 5.2.3.2; 5.2.3.3; 5.2.6.3; 5.2.6.3d; 6.4.
Электронный измерительный прибор: 3.1.15; 8.1.
Электронное устройство: 1.3; 3.1.7; 3.1.8; 3.1.9; 3.1.15; 3.1.16; 3.1.22; 3.1.30; 3.1.31; 3.1.35; 3.1.44; 3.1.46; 3.1.49; 3.1.52; 5.1; 5.1.1; 5.1.2; 5.1.4.1; 5.1.4.2; 5.2.1; 5.2.1.1.a; 5.2.1.2.b; 5.2.1.2.d; 5.2.3; 5.2.3.3; 5.2.6.3.b; 5.2.6.3.f; 6.1.1; 6.4; 6.5.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО/МЭК 9594-8:2001	IDT	ГОСТ Р ИСО/МЭК 9594-8—98[1)] «Информационные технологии. Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации»
МЭК 61508-4:1998	IDT	ГОСТ Р МЭК 61508-4—2007 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения»
МЭК 61508-5:1998	IDT	ГОСТ Р МЭК 61508-5—2007 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности»
МОЗМ Б 3:2003	—	*
МОЗМ Д 11:2004	—	*
ИСО/МЭК 2382-9:1995	—	*
ИСО/МЭК 4598-1:1999	—	Заменен ИСО/МЭК 25040:2011* «Проектирование систем и разработка программного обеспечения. Требования к качеству систем и программного обеспечения и их оценка (SQuaRE). Процесс оценки»
ИСО/МЭК 4598-2:2000	—	Заменен ИСО/МЭК 25001:2007* «Программирование. Требования к качеству программного продукта и его оценка. Планирование и менеджмент»
ИСО МЭК 45983-3:2000 ИСО/МЭК 4:1999	—	Заменен ИСО/МЭК 25041:2012* «Разработка систем и программ. Требования и оценивание качества систем и программ. Руководство по оцениванию для разработчиков, покупателей и независимых оценщиков»
ИСО/МЭК 5:1998	—	*
ИСО/МЭК 6:2001	—	*
V 1:2000	—	*
МЭК 61131-3:2003	—	*

[1)] Национальный стандарт идентичен предыдущей версии цитируемого стандарта ISO/IEC 9594-8:1994, Information technology — Open Systems Interconnection — The Directory. Part 8: Authentication framework.

* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

- IDT — идентичные стандарты.

УДК 389.14:006.354 ОКС 17.020 Т80

Ключевые слова: измерительный прибор, аутентификация, контрольный журнал, программное обеспечение, разделение программного обеспечения, законодательно контролируемое программное обеспечение

Редактор *М.В. Глушкова*
Технический редактор *Е.В. Беспрозванная*
Корректор *Р.А, Ментова*
Компьютерная верстка *В.И. Грищенко*

Сдано в набор 10.11.2014. Подписано в печать 21.11.2014. Формат 60x84 1/8. Гарнитура Ариал. Усл. печ. л. 5,12. Уч.-изд. л. 5,05. Тираж 85 экз. Зак. 4698.

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.

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

gost.e-ecolog.ru