ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ БЕЛАРУСЬ **СТБ/ПР_1/ХХХ**

Система обеспечения единства измерений Республики Беларусь
ОБЩИЕ ТРЕБОВАНИЯ К ПРОГРАММНО-УПРАВЛЯЕМЫМ СРЕДСТВАМ ИЗМЕРЕНИЙ

Сістэма забеспячэння адзінства вымярэнняў Рэспублікі Беларусь
АГУЛЬНЫЯ ПАТРАБАВАННІ ДА ПРАГРАММНА-КІРУЕМЫХ СРОДКАЎ ВЫМЯРЭННЯЎ

(OIML D 31:2008, IDT)

Настоящий проект стандарта не подлежит применению до его утверждения

Госстандарт
Минск

УДК МКС 17.020 КП 06

Ключевые слова: программно-управляемые средства измерений, электронные технические устройства, программное обеспечение, критерии испытаний, контрольная сумма, обработка измерительной информации

Предисловие

Цели, основные принципы, положения по государственному регулированию и управлению в области технического нормирования и стандартизации установлены Законом Республики Беларусь «О техническом нормировании и стандартизации»

1 РАЗРАБОТАН республиканским унитарным предприятием «Белорусский государственный институт метрологии» (БелГИМ)

ВНЕСЕН ТК 6 «Стандартизация в области метрологии»

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ постановлением Госстандарта Республики Беларусь от 2016 г. №

3 Настоящий стандарт разработан на основе документа Международной организации по законодательной метрологии (МОЗМ) OIML D 31 «General requirements for software controlled measuring instruments» («Общие требования к программно-управляемым средствам измерений») с учетом требований руководства WELMEC Guide 7.2 «Software Guide» (май 2008, 3 издание, является руководством к реализации требований Директивы ЕС «Measuring Instruments Directive 2004/22/EC» («Директива 2004/22/ЕС Европейского парламента и Совета от 31 марта 2004 года, касающаяся средств измерений»)).

ВВЕДЕН ВПЕРВЫЕ

Издан на русском языке

Содержание

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ БЕЛАРУСЬ

Система обеспечения единства измерений Республики Беларусь ОБЩИЕ ТРЕБОВАНИЯ К ПРОГРАММНО-УПРАВЛЯЕМЫМ СРЕДСТВАМ ИЗМЕРЕНИЙ

Сістэма забеспячэння адзінства вымярэнняў Рэспублікі Беларусь АГУЛЬНЫЯ ПАТРАБАВАННІ ДА ПРАГРАММНА-КІРУЕМЫХ СРОДКАЎ ВЫМЯРЭННЯЎ

System for ensuring the uniformity of measurements of the Republic of Belarus
General requirements for software controlled measuring instruments

Дата введения ____-__-__

1 Введение

Настоящий стандарт устанавливает общие требования к программно-управляемым средствам измерений и распространяется на средства измерений, предназначенные для применения либо применяемые в сфере законодательной метрологии.

2 Область применения

2.1 Требования настоящего стандарта должны учитываться разработчиками СИ при проектировании электронных средств измерений и иных программно-управляемых технических устройств с измерительными функциями.

2.2 Указанные требования также должны учитываться разработчиками технических нормативных правовых актов в области технического нормирования и стандартизации (далее – ТНПА) на конкретные виды средств измерений. Настоящий стандарт также является руководством по проверке соответствия указанной категории СИ требованиям настоящего стандарта и распространяющихся на них ТНПА, в том числе при проведении метрологического контроля и инспекции.

2.3 Требования и методы, изложенные в настоящем стандарте применимы только к электронным программно-управляемым средствам измерений и иным программно-управляемым техническим устройствам с измерительными функциями.

Примечания:
1 Настоящий стандарт может не содержать требований, которые индивидуальны для конкретного вида средств измерений. Такие требования должны быть изложены в соответствующих ТНПА, например, на весы, счетчики воды и т.п.
2 В стандарте рассмотрены отдельные вопросы безопасности данных. Дополнительно необходимо учитывать требования национального законодательства в данной области.
3 Поскольку средства измерений, работающие под управлением программного обеспечения (далее – ПО), всегда электронные, необходимо принимать во внимание требования распространяющихся на них ТНПА (например, [3]).

3 Термины и определения

Термины, используемые в настоящем стандарте, соответствуют приведенным в Международном словаре по метрологии (VIM3:2012) [1], а также в Международном словаре законодательной метрологии (OIML V 1:2013) [8] и общим требованиям к электронным средствам измерений (OIML D 11:2004) [3].

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 Основные термины

3.1.1 приемлемое решение (acceptable solution): Структура или принцип работы программного модуля или аппаратного модуля или структура и организация определенной функции, которая считается соответствующей определенному требованию. Приемлемое решение является примером того, как необходимо выполнять конкретное требование. Оно ни в коем случае не исключает иные решения, которые также обеспечивают выполнение соответствующего требования.

3.1.2 журнал аудита (audit trail): Непрерывный файл данных, содержащий привязанную к определенному времени информационную запись или событие, например, изменение значений параметров устройства, обновление программного обеспечения или иные законодательно контролируемые изменения, которые могут влиять на метрологические характеристики.

Проект, первая редакция

3.1.3 аутентификация (authentication): Проверка заявленной или предполагаемой идентификации пользователя, процесса или устройства (например, проверка того, что программное обеспечение разработано именно владельцем сертификата утверждения типа).

3.1.4 аутентичность (authenticity): Результат процесса аутентификации (соответствует или не соответствует).

3.1.5 контрольное устройство (checking facility): Устройство, которое входит в состав средства измерений и обеспечивает обнаружение и реагирование на значительные сбои в работе [OIML D 11:2004, 3.18].

Примечание – «Реагирование» включает в себя любую подходящую реакцию средства измерений на сбой (световой, акустический сигналы, блокирование выполнения измерений и т.д.).

3.1.6 закрытая сеть (closed network): Сеть из ограниченного числа участников с известной идентификацией, функциями и местоположением (см. «открытая сеть»).

3.1.7 команды (commands): Команды могут являться последовательностью электрических (оптических, электромагнитных и т.п.) сигналов с интерфейса ввода или кодами протоколов обмена информацией. Они могут генерироваться программным обеспечением средства измерений, электронного устройства, функционального узла (командами ПО) или генерироваться оператором через интерфейс пользователя средства измерений (команды оператора).

3.1.8 связь (communication): Обмен информацией между двумя или более функциональными единицами (например, программные модули, электронные устройства, функциональные узлы и т.д.) в соответствии с установленными правилами.

3.1.9 интерфейс связи (communication interface): Электронный, оптический, радио или иной технически реализованный интерфейс, который обеспечивает прохождение информации между функциональными единицами средства измерений (например, электронными устройствами) или функциональными узлами.

3.1.10 криптографический сертификат (cryptographic certificate): Набор данных, содержащих открытый ключ, принадлежащий средству измерений или лицу, и уникальную идентификацию объекта, например, серийный номер прибора или название или Личный идентификационный номер (PIN) лица. Набор данных подписывается авторитетной организацией электронной подписью. Присвоение открытого ключа объекту проверяется с использованием открытого ключа авторитетной организации и дешифрования электронной подписи сертификата.

3.1.11 криптографические средства (cryptographic means): Шифрование данных их отправителем (записывающая или передающая программа) и дешифрование этих данных их получателем (считывающая программа) с целью сокрытия передаваемой информации от посторонних лиц.

Электронная подпись данных с целью возможности проверки их происхождения получателем или пользователем, т.е. для подтверждения их аутентичности.

Примечание – Для электронной подписи обычно используется система открытых ключей, т.е. процедура требует пары ключей, один из которых должен храниться в секрете, другой может быть открытым. Отправитель (посылающая или записывающая программа) генерирует хэш-код (см.3.1.25) для данных и шифрует их с использованием секретного ключа. В результате получают цифровую подпись. Получатель (принимающая или считывающая программа) дешифрует электронную подпись с использованием открытого ключа отправителя и сравнивает результат с оригинальным хэш-кодом переданных данных. В случае совпадения хэш-кода данные считаются аутентичными. Получатель может потребовать предоставить криптографический сертификат отправителя (см. 3.1.10) с тем, что бы убедиться в аутентичности открытого ключа.

3.1.12 домен данных (data domain): Область памяти, которая используется каждой программой для обработки данных. В зависимости от используемого языка программирования данная область определяется адресами аппаратной конфигурации или символьными именами (идентификатор, имена переменных). Размер наименьшего рабочего домена обычно равен 1 байту, однако на практике этот размер практически неограничен: он может варьировать от 1 бита (например, признак или регистр) до произвольной структуры данных, отвечающей задачам программирования. Домены данных могут принадлежать одному или нескольким программным модулям. Для языков программирования высокого уровня (таких как JAVA, C/C++ и др.) наиболее просто разделить домены данных, используемые разными программными модулями с использованием возможностей языка программирования.

3.1.13 устройство-определяющий (опорный) параметр (device-specific parameter): Законодательно контролируемый параметр, имеющий значение, которое зависит от конкретного средства измерений. Устройство-определяющие параметры включают параметры настройки (например, установка диапазона измерений и иные настроечные характеристики и поправочные коэффициенты), а также параметры конфигурации (например, максимальное и минимальное значения, единицы измерений и т.д.).

3.1.14 долговечность (durability): Свойство средства измерений, обуславливающее его способность сохранять рабочие характеристики в течение периода эксплуатации [OIML D 11:2004, 3.17].

3.1.15 электронное средство измерений (electronic measuring instrument): Средство измерения, предназначенное для измерения электрической или неэлектрической величины, используя электронные средства и/или оборудованное электронными устройствами [OIML D 11:2004, 3.1].

Примечание – В настоящем стандарте, вспомогательное оборудование, если оно выполняет законодательно-контролируемые функции, рассматривается как неотъемлемая часть средства измерений.

3.1.16 электронное устройство (electronic device): Устройство, включающее функциональные блоки и выполняющее определенную функцию. Электронные устройства обычно изготавливаются как самостоятельные единицы и могут быть испытаны индивидуально [OIML D 11:2004, 3.2].

Примечание - Электронное устройство может быть как единым средством измерения (например, счётчик электроэнергии), так и составной частью средства измерения (например, принтер, индикатор).

Электронное устройство может быть модулем (измерительный модуль давления и т.п.).

3.1.17 погрешность (measurement error): Измеренное значение величины минус опорное значение величины [VIM3:2012, 2.16; OIML D 11:2004, 3.5]

Примечания
1 Понятие «погрешность измерения» может использоваться в следующих случаях:
a) когда имеется единственное опорное значение величины для ссылки, как в случае калибровки по эталону, у которого измеренное значение величины имеет пренебрежимо малую неопределенность измерения, или если дано принятое значение величины. В этом случае погрешность измерения известна;
b) если предполагается, что измеряемая величина представлена единственным истинным значением величины или совокупностью истинных значений величины в малом диапазоне. В этом случае погрешность измерения неизвестна.
2 Погрешность измерения не следует путать с погрешностью производства или с ошибкой.

3.1.18 протокол ошибок (error log): Непрерывный файл данных, содержащий информационную запись об отказах/сбоях, которые имеют влияние на метрологические характеристики. Это, в частности, относиться к случайно возникающим отказам, которые не могут быть в последствии выявлены при использовании результатов измерений.

3.1.19 оценка типа (evaluation (type)): Систематическое обследование и испытание функционирования одного или более образцов определенного типа средства измерений (pattern) на соответствие документированным требованиям, результаты которых сводятся в отчет испытаний для принятия решения об утверждении типа [OIML V1:2013, 2.5].

3.1.20 событие (event): Действие, в результате которого происходит изменение параметра средства измерений, поправочного коэффициента или обновление программного модуля.

3.1.21 счетчик событий (event counter): Необнуляемый счетчик, который принимает новое значение каждый раз при появлении события.

3.1.22 исполняемый код (executable code): Файл, установленный в вычислительной системе средства измерений, электронном устройстве, или функциональном блоке (EPROM, жесткий диск и др.). Данный код интерпретируется микропроцессором и передается для выполнения определенных логических и арифметических операций, а также дешифрования или передачи данных.

3.1.23 сбой (fault): Дефект, который имеет влияние на свойства или функции средства измерений, или который приводит к ошибке показаний на значение, превышающее максимально допустимую погрешность (МДП) [OIML D 11:2004, 3.9].

3.1.24 неизменная законодательно контролируемая часть ПО (fixed legally relevant software part): Часть законодательно контролируемого ПО, которая в исполняемом коде остается идентичной части, проверенной при утверждении типа.

Примечание – Эта часть, например, отвечает за контроль обновления ПО (загрузку ПО, аутентификацию, проверку целостности, установку и активизацию).

3.1.25 ХЭШ функция (hash function): Функция (математическая), которая переносит значения из большого (максимально большого) массива значений в узкий диапазон. Качественная хэш функция характеризуется тем, что полученные из (большого) набора значений одного массива результаты будут равномерно (и обязательно случайно) распределены в заданном диапазоне [ISO/IEC 9594-8:2001][4].

3.1.26 целостность программ, данных и параметров (integrity of programs, data, or parameters): Состояние программ, данных или параметров, характеризующееся их неизменностью как в случае неавторизованного так случайного изменения, при их эксплуатации, передаче, хранении, восстановлении или обслуживании.

3.1.27 интерфейс (interface): Часть устройства, предназначенная для связи. Интерфейс позволяет устанавливать связь между несколькими устройствами или блоками или между несколькими различными программными модулями (см. программный интерфейс) [ISO 2382-9:1995][5].

3.1.28 основная погрешность (intrinsic error): Погрешность средства измерения, применяемого в нормальных условиях [VIM3:2012, OIML D 11:2004, 3.7].

3.1.29 законодательно релевантный (legally relevant): Программное обеспечение/аппаратная часть/данные или часть программного обеспечения/аппаратной части/данных средства измерений, которые связаны с характеристиками, подлежащими контролю со стороны законодательной метрологии, например, точность измерений или правильность функционирования средства измерений.

3.1.30 законодательно контролируемый параметр (legally relevant parameter): Параметр средства измерений или блока, подлежащий контролю со стороны законодательной метрологии. Различают следующие типы законодательно контролируемых параметров: типоопределяющие параметры и устройство-определяющие параметры.

3.1.31 законодательно-контролируемая часть ПО (legally relevant software part): Часть всех программных модулей средства измерений, устройства или блока, которые подлежат контролю со стороны законодательной метрологии.

3.1.32 максимально допускаемая погрешность (измерительного прибора) (maximum permissible error (of a measuring instrument)): Максимальное значение погрешности, допускаемое технической спецификацией, нормативными документами, и т.д. для данного типа средства измерения [VIM3:2012, OIML D 11:2004, 3.6].

3.1.33 средство измерений (measuring instrument): Техническое устройство, используемое для выполнения измерений, в том числе в сочетании с одним или несколькими дополнительными устройствами и имеющее нормированные метрологические характеристики [VIM3:2012, 4.1].

3.1.34 непрерывные / прерываемые (дискретные) измерения (non-interruptible / interruptible measurement): Непрерывные измерения являются накопительным постоянным измерительным процессом без однозначно определенного момента завершения. Измерительный процесс не может быть остановлен и снова возобновлен пользователем или оператором без непозволительного прерывания измерений или прекращения поступления продукции или энергии.

Если накопительное измерение величины может быть легко и быстро прервано в нормальном режиме выполнения, т.е. кроме экстренных случаев, без искажения результата измерения, то такие измерения являются прерываемыми.

3.1.35 открытая сеть (open network): Сеть произвольных участников (электронные устройства с произвольными функциями). Число, идентичность и местоположение участника могут быть динамическими и неизвестными другим участникам (см. также Закрытую сеть).

3.1.36 функционирование (performance): Способность средства измерения выполнять заданные функции [OIML D 11:2004, 3.16].

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

3.1.38 опечатывание (sealing): Средства, предназначенные для защиты средства измерений от неавторизированных изменений, настроек, удаления функциональных частей, программного обеспечения и т.д. Опечатывание выполняется посредством аппаратных средств, программного обеспечения или комбинацией обоих.

3.1.39 защита (securing): Предотвращение неавторизованного доступа к аппаратной или программной части устройства.

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

3.1.41 экспертиза программного обеспечения (software examination): Техническое действие, включающее определение одной или более характеристик программного обеспечения в соответствии с определенной процедурой (например, анализ технической документации или выполнение программы в контролируемых условиях).

3.1.42 идентификация ПО (software identification): Последовательность читаемых символов (например, номер версии, контрольная сумма), которая неразрывно связана с ПО или программным модулем, подлежащим контролю. Идентификация может быть вызвана для просмотра во время использования прибора.

3.1.43 программный интерфейс (software interface): Программный интерфейс состоит из программного кода и выделенной области данных. Программный интерфейс выполняет функции по получению, фильтрации или передачи данных между частями ПО (части ПО не обязательно выполняют законодательно контролируемые функции).

3.1.44 программный модуль (software module): Логические объекты, такие как программы, подпрограммы, библиотеки и иные объекты включая их домены данных, которые могут быть связаны с другими объектами. Программное обеспечение средств измерений, устройств или блоков состоит из одного или более программных модулей [согласно IEC 61508-4:1998, 3.3.7] [6].

3.1.45 защита ПО (software protection): Защита программного обеспечения средства измерений или области данных посредством аппаратных или программных средств. Средство защиты должно быть удалено, повреждено или претерпеть изменения при попытке внести изменения в ПО или область данных.

3.1.46 разделение ПО (software separation): Программное обеспечение средств измерений может быть разделено на законодательно контролируемую часть и законодательно не контролируемую часть. Связь этих частей осуществляется через программный интерфейс.

3.1.47 исходный код (source code): Компьютерная программа, написанная (язык программирования) в форме, поддающейся чтению и редактированию. Исходный код компилируется или интерпретируется в исполняемый код.

3.1.48 устройство хранения (storage device): Устройство, используемое для хранения в состоянии готовности для изъятия результатов измерений после завершения измерений для последующих законодательно контролируемых целей (например, заключения коммерческой сделки).

3.1.49 функциональный блок (sub-assembly): Часть электронного устройства, содержащая электронные составляющие и выполняющее свою четко выраженную функцию [OIML D 11:2004, 3.3].

Пример – Усилители, компараторы, преобразователи питания и др.

3.1.50 испытание (test): Последовательность действий направленных на подтверждение соответствия испытываемого оборудования (ИО) установленным требованиям [OIML D 11:2004, 3.20].

3.1.51 метка времени (time stamp): Уникальное постепенно увеличивающееся значение времени, например, в секундах или формате даты и времени, соответствующей дате и/или времени появления события или сбоя. Данная информация представляется в единообразном формате, позволяющем легко проводить сравнение двух различных записей и последовательности записей во времени.

3.1.52 передача результатов измерений (transmission of measurement data): Передача результатов измерений, через коммуникационные сети или другие средства связи, удаленному устройству для дальнейшей обработки и/или использования в законодательно контролируемой области.

3.1.53 типоопределяющий параметр (type-specific parameter): Законодательно контролируемый параметр со значением, которое зависит только от типа средства измерений. Типоопределяющие параметры являются частью законодательно контролируемого ПО.

Пример – Рассматривая измерительную систему для жидкостей, не являющихся водой, диапазон кинематической вязкости для турбины является типоопределяющим параметром, установленным при утверждении типа турбины. Все турбины одного типа предназначены для одного диапазона вязкости измеряемой жидкости.

3.1.54 универсальный компьютер (universal computer): Компьютер, который не был специально разработан для конкретной задачи, но может быть использован для выполнения метрологических задач, с помощью установленного на него программного обеспечения. В основном, данное программное обеспечение базируется на операционной системе, которая позволяет загрузку и выполнение программного обеспечения, разработанного для специальной задачи.

3.1.55 интерфейс пользователя (user interface): Интерфейс, с помощью которого реализуется обмен данными между пользователем и средством измерений или между пользователем и аппаратными или программными компонентами, например, переключатели, клавиатура, мышь, монитор, принтер, сенсорный экран, окно программного обеспечения на экране, включая ПО, которое способствует отображению этого окна.

3.1.56 валидация (validation): Подтверждение методом исследования и предоставление объективных свидетельств (например, информации, которая может быть подтверждена основываясь на фактах, полученных из наблюдений, измерений, испытаний и т.п.) того, что определенные требования по предполагаемому применению выполняются. В данном случае определенные требования являются требованиями настоящего стандарта [ISO/IEC 14598 и IEC 61508-4:1998][7].

3.1.57 верификация (verification): Процедура (не являющаяся утверждением типа), которая включает исследование и маркировку и/или выдачу сертификата верификации, который устанавливает и подтверждает, что средство измерений соответствует обязательным требованиям [OIML V1: 2013, 2.13].

3.2 Обозначения и сокращения

ИО – Испытываемое оборудование
ИТ – Информационные технологии
МДП – Максимально допускаемая погрешность
ПО – программное обеспечение
СИ – средство измерений.

4 Рекомендации по использованию настоящего стандарта при разработке стандартов на конкретные виды средств измерений

4.1 Настоящий стандарт используется только при разработке новых и пересмотре действующих стандартов.

4.2 Целью настоящего стандарта является предоставление разработчикам стандартов на средства измерений руководства по установлению уровней защиты, соответствия и валидации. Кроме того, стандарт должен использоваться изготовителями средств измерений для обеспечения соответствия новых средств измерений требованиям законодательной метрологии.

5 Требования, предъявляемые к средствам измерения под управлением программного обеспечения

5.1 Основные требования

Общие требования настоящего стандарта соответствуют уровню развития сферы информационных технологий. Они в принципе применимы ко всем видам программного обеспечения средств измерений, электронных устройств и блоков и могут быть использованы во всех Рекомендациях МОЗМ. В отличие от этих простейших требований, специфические требования (5.2) связаны с техническими особенностями прибора, которые различны в зависимости от типа прибора или от области применения.

В примечаниях, где применимо, указаны два уровня безопасности: нормальный и повышенный. В настоящем стандарте пояснения приведены в виде:

(I) – Техническое решение приемлемо в случае обычного уровня риска

(II) – Техническое решение приемлемо в случае повышенного уровня риска (см. 8).

5.1.1 Идентификация ПО

Законодательно контролируемое ПО средства измерений/ электронного устройства/ функционального блока должно быть четко идентифицировано версией ПО или другим набором символов. ПО может иметь несколько идентификационных частей, но одна часть обязательно должна использоваться в целях законодательной метрологии.

Идентификация должна быть неразрывно связана с программным обеспечением и должна отображаться при запуске или по команде. Если функциональный блок/ электронное устройство не имеет средств для отображения информации, то должна быть предусмотрена возможность получить идентификации через интерфейс для отображения/ распечатки на другом блоке.

Как исключение, отображение идентификации программного обеспечения на средстве измерений/электронном устройстве будет приемлемым, если выполняются следующие условия:

1) Интерфейс пользователя не имеет функциональной возможности получить отображение идентификации на показывающем устройстве или показывающее устройство не имеет технической возможности отобразить идентификацию (аналоговое показывающее устройство или электромеханический счетчик);

2) Средство измерений/ электронное устройство не имеет интерфейса для отображения идентификации программного обеспечения;

3) После изготовления средства измерений/ электронного устройства изменение программного обеспечения невозможно или возможно только в случае полной замены аппаратной части или ее отдельного элемента.

Изготовитель аппаратной части или соответствующего элемента аппаратной части несет ответственность за корректное отображение идентификации программного обеспечения на средстве измерения/ электронном устройстве.

Идентификация программного обеспечения и средств ее получения должны быть указаны в сертификате утверждения типа.

Стандарты на конкретные средства измерений могут допускать или запрещать данное исключение.

Примечание – Каждое средство измерений, находящееся в эксплуатации, должно соответствовать утвержденному типу. Идентификация программного обеспечения позволяет инспекционным органам и лицам, заинтересованным в измерениях, убедиться в соответствии прибора утвержденному типу.

Примеры:

I) Программное обеспечение содержит текстовую строку или число, однозначно идентифицирующее установленную версию. Данная строка переносится на показывающее устройство средства измерений при его включении, нажатии соответствующей кнопки или циклически отображается под управлением таймера.

Версия программного обеспечения может иметь следующую структуру - A.Y.Z. Если рассматривать потоковый вычислитель, то буква A будет представлять версию основного программного обеспечения, считающего импульсы, буква Y будет представлять версию функции преобразования (отсутствие преобразования, преобразование при 150 °C, при 200 °C) и буква Z будет представлять язык пользовательского интерфейса.

II) ПО вычисляет контрольную сумму исполняемого кода и представляет результат в качестве идентификации вместо или дополнительно к строке (I). Алгоритм контрольной суммы должен быть формализованным, например алгоритм CRC16 является приемлемым решением.

Решение II) рекомендуется в случае повышенных требований к обеспечению соответствия (см. 5.2.5d) и 8.).

5.1.2 Правильность алгоритмов и функций

Измерительные алгоритмы и функции электронных устройств должны соответствовать решаемой задаче и типу устройства, а также функционально корректными (точность алгоритмов, расчет стоимости согласно определенным правилам, алгоритмы округления и т.п.).

Результат измерения и сопровождающая информация, требуемая в соответствии с соответствующими стандартами или национальным законодательством, должны отражаться или печататься правильно.

Должна быть предусмотрена возможность проверки алгоритмов и функций посредством метрологических испытаний, испытаний ПО или экспертизы ПО (см. 6)

5.1.3 Защита ПО

5.1.3.1 Предотвращение случайного неправильного применения

Средство измерений должно быть разработано таким образом, чтобы возможность случайного или преднамеренного неправильного использования была минимальной.

Примечание – Программно управляемые средства измерений обычно обладают большим количеством функциональных возможностей, в особенностях которых трудно разобраться. Поэтому, для правильного использования и для получения корректных результатов измерения, необходимо предоставить пользователю хорошее руководство по эксплуатации.

Пример – При работе пользователь руководствуется меню. Законодательно контролируемые функции объединены в ветку одного пункта меню. Если значения измерений могут быть потеряны вследствие какого-нибудь действия, пользователь должен быть предупрежден с выбором варианта продолжения до выполнения этого действия. См. также 5.2.2.

5.1.3.2 Защита от мошенничества

5.1.3.2.a) Законодательно контролируемое ПО должно быть защищено от недопустимой модификации, загрузки или изменения, посредством замены запоминающего устройства. Для защиты средства измерений со встроенной операционной системой или имеющей возможность обновления ПО дополнительно к механическому пломбированию могут потребоваться иные технические средства.

Примечание – Если ПО размещается в жестко установленной памяти (память, на которой данные неизменны, например, память ROM, для которой допускается только чтение) необходимость в технических средствах защиты меньше.

Примеры:

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

(II) Если используется перезаписываемое устройство, вход для перезаписи защищен переключателем, который может быть опечатан. Схема должна быть разработана таким образом, чтобы защита от записи не могла бы быть обойдена коротким замыканием контактов.

(I) В измерительной системе, состоящей из двух функциональных блоков, один из их них, содержащий метрологически критическое ПО, может быть механически опечатан. Другой функциональный блок находится на ЭВМ общего назначения с операционной системой. Некоторые функции, такие как индикация показаний реализована ПО на ЭВМ. Одним из простейших способов манипуляции ПО, особенно использующего стандартный протокол обмена между его составными частями, является подмена ПО на универсальной ЭВМ. Такая подмена может быть предотвращена использованием простейших криптографических средств, например, шифрованием данных передаваемых с функционального блока на ЭВМ. Ключ для декодирования скрыт в законодательно контролируемой программе, находящейся на ЭВМ. Только эта программа знает ключ к шифру и в состоянии прочитать, расшифровывать и использовать результаты измерений. Другие программы не могут использоваться для этих целей, поскольку они не могут расшифровать результаты измерений (см. также 5.2.1.2d)).

5.1.3.2.b) Только четко документированные функции (см. 6.1) допускается активизировать с помощью пользовательского интерфейса способом, не допускающим мошенническое использование. Представление информации должно соответствовать п. 5.2.2.

Примечание – Специалист, проводящий экспертизу, дает заключение о допустимости документированных команд.

Пример – (I)/(II) Все команды, поступившие с пользовательского интерфейса, переадресованы к программе, которая их фильтрует. Фильтрация способствует пропуску только зарегистрированные команд и игнорированию все других. Эта программа или программный модуль - законодательно контролируемая часть программного обеспечения.

5.1.3.2.c) Параметры, которые устанавливают законодательно контролируемые характеристики средства измерений, должны быть защищены от несанкционированной модификации. Должна быть предусмотрена возможность отображения на экране или вывода на печать текущих параметров настройки, если этого требует процедура верификации.

Примечание – Приборопределяющие параметры могут быть настроены или выбраны только в специальном режиме средства измерений. Они могут быть классифицированы как те параметры, которые должны быть защищены (неизменяемые параметры), и доступ к которым может получить лишь авторизированный пользователь, например, владелец прибора или поставщик (установочные параметры).
Типоопределяющие параметры имеют идентичные настройки для всех экземпляров типа. Они определяются и устанавливаются при утверждении типа средства измерений.

Пример – (I) / (II) Приборопределяющие параметры, подлежащие защите, должны храниться в энергонезависимой памяти, вход для перезаписи которой защищен выключателем, который может быть опломбирован. См. пример 5.1.3.2.d (1) к п.3 настоящего раздела.

5.1.3.2.d) Наличие механической пломбировки и электронной или криптографической защиты предотвращает несанкционированное вмешательство или делает его очевидным.

Примеры:

1) (I) Электронная пломбировка. Метрологические параметры средства измерений могут быть введены и изменены через пункт меню ПО. ПО фиксирует каждое отдельное изменение посредством увеличения числа счетчика событий. Значение счетчика событий может быть выедено на просмотр. Начальное значение счетчика событий должно быть зафиксировано (документально, на бирке прибора и т.п.). Если отображаемое значение отличается от зарегистрированного, считается что средство измерений не верифицировано (эквивалентно нарушению метрологической пломбы).

2) (I)/(II) ПО средства измерений разработано таким образом, (см. пример 5.1.3.2.a) что нет возможности изменять параметры и законодательно контролируемую конфигурацию кроме как через защищенное выключателем меню. Данный выключатель механически пломбируется в неактивном положении, исключающем возможность модификации параметров и законодательно контролируемой конфигурации. Для модификации параметров и конфигурации данный выключатель должен быть переведен в активное положение, что неизбежно приводит к нарушению (метрологической) пломбы.

3) (II) ПО средства измерений разработано таким образом (см. пример 5.1.3.2.a), что нет возможности получения доступа к параметрам и законодательно контролируемой конфигурации кроме авторизированного работника. Если работнику необходимо изменить параметр через меню, ему необходимо авторизоваться с помощью электронной карты с PIN, являющимся частью криптографического сертификата. ПО средства измерений должно позволять проверку аутентичности введенного PIN сверкой с сертификатом, положительный результат которой дает возможность на изменение параметра. Факт доступа фиксируется в журнале аудита, включая идентификацию личности (или ID использованной электронной карты).

Уровень (II) является приемлемым техническими решением, если требуется повышенная защита от мошенничества (см. 8).

5.1.4 Поддержка аппаратных средств

5.1.4.1 Обнаружение ошибок

Соответствующие национальные стандарты могут включить требование по наличию функции обнаружению неисправностей для определенных типов отказов (см. D11:2004 ((5.1.2 b)) и 5.3)). В данном случае изготовителю средства измерений следует предусмотреть наличие технических решений такого контроля в ПО, в аппаратных средствах или наличие программно-технических средств, обеспечивающих соответствующее взаимодействие программного обеспечения и аппаратных средств.

Требование: Если программное обеспечение участвует в процессе обнаружения ошибки, требуется его соответствующая реакция. Соответствующий национальный стандарт может содержать требование, чтобы прибор / устройство было отключено или сигнал тревоги / сообщение генерировалось в случае обнаружения состояния ошибки.

Документация, представленная на утверждение типа должна содержать список ошибок, которые обнаруживаются программным обеспечением и, в случае необходимости, описание алгоритма обнаружения.

Примеры:

(I) / (II) При запуске законодательно контролируемое ПО рассчитывает контрольную сумму программного кода и законодательно контролируемых параметров. Номинальные значения этих контрольных сумм рассчитываются заранее (при утверждении типа) и сохраняются в устройстве. Если рассчитанные и сохраненные значения не совпадают, прекращается выполнение программы.

Если измерение является непрерываемым, контрольная сумма рассчитывается циклически через определенный промежуток времени (контролируемый ПО). В случае обнаружения неисправности ПО выводит сообщение об ошибке или соответствующим образом изменяет состояние индикатора неисправностей и записывает время данного события в журнал событий, при наличии.

Для расчета контрольной суммы приемлемо использование алгоритма CRC16.

5.1.4.2 Обеспечение надежности

Изготовитель сам принимает решение о включении в конструкцию средства измерений или его ПО функции обеспечения надежности. Рекомендуемые технические решения могут быть указаны в соответствующих национальных стандартах на конкретное средство измерений.

Требование: Если ПО участвует в реализации функции обеспечения надежности, то его работа должна быть очевидна. Например, конкретным национальным стандартом может требоваться, чтобы средство измерений или связанное с ним устройство прекращало работу, выдавало предупреждающий сигнал и генерировало отчет о сбое, который влияет на надежность средства измерений.

Пример – (I)/(II) Некоторые типы средств измерений требуют настройки после предписанного изготовителем срока с тем, чтобы гарантировать надежность средства измерений. ПО может генерировать предупреждающий сигнал, когда данный срок истекает и даже прекращать работу средства измерений, если данный срок превышает определенное время.

5.2 Специальные требования для отдельных конфигураций

Требования, приведенные в настоящем разделе, основаны на типовых технических решениях в сфере информационных технологий, хотя могут различаться в зависимости от области применения. Согласно этим требованиям, возможны технические решения, которые имеют степень безопасности и соответствуют типам идентичных приборов, которые не управляются ПО.

Нижеследующие специальные требования предъявляются к ПО, при использовании в измерительных системах определенных технологий. Их следует учитывать дополнительно к требованиям, описанным в п. 5.1.

В примерах, если применимо, описаны как нормальный, так и повышенный уровни соответствия, с соответствующими обозначениями:

(I) – Техническое решение приемлемо в случае обычного уровня риска

(II) – Техническое решение приемлемо в случае повышенного уровня риска (см. 8)

5.2.1 Определение и разделение контролируемых частей, и определение их интерфейсов

Метрологически критичные части измерительной системы (программная или аппаратная часть) не должны подвергаться влиянию со стороны других частей измерительной системы.

Данное требование вводится, если средство измерения (или устройство, или блок) имеет интерфейсы связи с другими электронными устройствами, с пользователем, с другими частями ПО, помимо метрологически критичных, одного конкретного средства измерений (устройства, блока).

5.2.1.1 Разделение устройств и блоков

5.2.1.1.a) Блоки или электронные устройства измерительной системы, которые выполняют законодательно контролируемые функции, должны быть идентифицированы, четко определены и задокументированы. Они составляют законодательно контролируемую часть измерительной системы.

Примечание – Эксперт, проводящий испытание, решает, является ли эта часть основной и можно ли исключить другие части из дальнейшей проверки.

Примеры:

1) (I)/(II) Счетчик электроэнергии оборудован оптическим интерфейсом для подключения устройства для считывания результатов измерения. Счетчик хранит все законодательно контролируемые значения, которые могут быть считаны после продолжительного периода времени. В этой системе только счетчик электроэнергии является законодательно контролируемым устройством. Счетчик электроэнергии хранит все необходимые данные и позволяет получить их по запросу в течение значительного периода времени. В такой системе только счетчик электрической энергии является законодательной контролируемым устройством. Иные устройства, не выполняющие законодательно контролируемые функции, могут подключаться к интерфейсу средства измерений при выполнении требования 5.2.1.1.b). Защита самих передаваемых данных (см. 5.2.3) не требуется.

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

– Цифровой первичный преобразователь массы или объема;

– Универсальный компьютер для расчета стоимости;

– Печатающее устройство для вывода результатов измерений и стоимости.

Все устройства объединены в одну локальную информационно-вычислительную сеть. В данном случае цифровой первичный преобразователь, универсальный компьютер и принтер являются законодательно контролируемыми устройствами и, при необходимости могут подключаться к торговой информационно-вычислительной системе, которая не является законодательно контролируемым объектом. Законодательно контролируемые функциональные блоки должны отвечать требованиям 5.2.1.1.b) и, ввиду передачи данных по сети, требованиям 5.2.3. К торговой информационно-вычислительной системе требований не устанавливается.

5.2.1.1.b) При проведении испытаний с целью утверждения типа необходимо продемонстрировать, что отсутствует недопустимое воздействие на законодательно контролируемые функции и данные функциональных блоков и электронных устройств посредством команд, полученных через интерфейс.

Это подразумевает однозначное назначение каждой команды по каждой инициализируемой функции или изменению данных в функциональных блоках или электронных устройствах.

Примечание – Если законодательно контролируемые функциональные блоки или электронные устройства взаимодействуют с другими законодательно контролируемыми функциональными блоками и электронными устройствами, то следует учитывать требования 5.2.3.

Примеры:

1) (I)/(II) Программное обеспечение счетчика электроэнергии (см. пример (1) п.5.2.1.1a)) может получать команды для выбора требуемых значений. Оно сопоставляет значение измерения с дополнительной информацией, например, временной отметкой, единицей величины измерений - и посылает этот набор данных устройству, пославшему запрос на получение данной информации. Программное обеспечение принимает только команды для выбора требуемых доступных значений. Также могут использоваться средства защиты передаваемых данных, однако это не является обязательным, поскольку пересылаемые данные не являются объектом законодательного контроля.

2) (I)/(II) Внутри корпуса, который может быть опломбирован, имеется переключатель, включающий требуемый режим работы счетчика электроэнергии: одно положение переключателя соответствует состоянию «поверено», другое положение – «не поверено» (иные защитные средства, кроме механических, также допускаются; см. примеры 5.1.3.2.a) / d)). При получении команд, ПО проверяет положение переключателя: в режиме «не поверено» ПО принимает расширенный набор команд в отличие от состояния «поверено», например, в таком режиме возможно изменить калибровочный коэффициент, который невозможно изменить в режиме «поверено».

5.2.1.2 Разделение ПО на части

Национальные стандарты могут устанавливать какие функциональные блоки, устройства или данные являются законодательно контролируемыми.

5.2.1.2.a) Все программные модули (программы, подпрограммы, объекты и т.д.), которые выполняют законодательно контролируемые функции или содержат законодательно контролируемые домены данных, являются законодательно контролируемой частью ПО средства измерений (устройств или функциональных блоков). Требование соответствия предъявляется к этой части (см. п. 5.2.5), и она должна быть четко идентифицируема как описано в п. 5.1.1.

Если разделение ПО невозможно или не требуется, всё ПО считается законодательно контролируемым.

Пример – (I) Измерительная система состоит из нескольких цифровых первичных преобразователей, связанных с персональным компьютером, который отображает результаты измерения. Законодательно контролируемое ПО на универсальном компьютере отделено от законодательно неконтролируемых частей, компилированием всех законодательно контролируемых функций в динамически связанную библиотеку. Одно или несколько законодательно неконтролируемых приложений могут вызвать процедуры программы в этой библиотеке. Эти процедуры получают результаты измерения от цифровых первичных преобразователей, обрабатывают их, и выводят на экран показывающего устройства. Когда законодательно контролируемые функции выполнены, управление возвращается законодательно неконтролируемому приложению.

5.2.1.2.b) Если законодательно контролируемая часть ПО обращается к другим частям, то программный интерфейс должен быть четко определен. Вся связь должна выполняться исключительно через этот интерфейс. Законодательно контролируемая часть ПО и соответствующий интерфейс должны быть четко документированы. Законодательно контролируемые функции и домены данных ПО должны описываться для установления корректности разделения ПО при утверждении типа.

Интерфейс состоит из программного кода и выделенного домена данных. Определенные кодовые команды или данные записываются одной частью в выделенный домен данных и считываются оттуда другой частью. Запись и чтение программного кода также является частью программного интерфейса. Домен данных, формирующий интерфейс программного обеспечения, включая код, который экспортирует данные из законодательно контролируемой части на интерфейс, и код, который импортирует данные с интерфейса в законодательно контролируемую часть, должен быть четко определен и документирован. Документированный программный интерфейс не должен быть обойден мошенническими способами.

Настоящее требование должно выполняться изготовителями. Технических средств (таких как пломбировка) для предотвращения доступа к программе, обхода интерфейса или ввода скрытых команд не должно быть. Разработчик законодательно контролируемой части ПО, как и разработчик неконтролируемой части должны быть информированы изготовителем о недопустимости таких технических решений.

5.2.1.2.c) Каждая команда во всех инициированных функциях или при изменении данных в законодательно контролируемой части ПО должна иметь однозначное назначение. Команды, реализуемые через программный интерфейс, должны быть задекларированы и документированы. Только документированные команды могут быть реализованы через программный интерфейс. Изготовитель должен подтвердить полноту описания команд.

Пример – (I) В примере пункта 5.2.1.2.a) программный интерфейс реализуется параметрами и ответными значениями процедур, прописанных в динамической библиотеке. Никаких маркеров, указывающих на домен данных в динамической библиотеке, не должно передаваться. Программное описание

интерфейса содержится в компилированной законодательно контролируемой динамической библиотеке и не может быть изменено какой-либо программой. Невозможно изменить программный интерфейс и получить прямой доступ к домену данных динамической библиотеки. Кроме того, что это технически сложно, любое подобное действие является противоправным.

5.2.1.2.d) В тех случаях, когда законодательно контролируемое ПО отделяется от неконтролируемого, законодательно контролируемое ПО должно иметь приоритет использования ресурсов перед неконтролируемым ПО. Измерительная задача (реализуемая законодательно контролируемой частью ПО) не должна замедляться или блокироваться выполнением других задач.

Изготовители должны соблюдать данное требование. Должны быть предусмотрены технические средства, предотвращающие помехи в работе законодательно контролируемого ПО со стороны неконтролируемого ПО. Разработчик законодательно контролируемой части ПО, как и разработчик неконтролируемой части должны быть информированы изготовителем о данном требовании.

Примеры:

1) (I) В примере 5.2.1.2.a/.c законодательно неконтролируемое приложение управляет началом работы законодательно контролируемых процедур в библиотеке. Игнорирование вызова этих процедур обязательно будет препятствовать выполнению законодательно контролируемой функции системы. Поэтому приводится следующий пример выполнения требования 5.2.1.2.d): Первичный цифровой преобразователь передает результат измерения в зашифрованном виде. Криптографический ключ храниться в библиотеке. Только процедуры библиотеки могут использовать ключ и в состоянии прочитать, расшифровать и вывести для просмотра значения измерений. Если разработчик приложения хочет считать и обработать результаты измерений он вынужден использовать законодательно контролируемые процедуры в библиотеке, которые выполняют все необходимые законодательные функции как сопутствующий эффект при их вызове. Библиотека содержит процедуры, которые экспортируют расшифрованные значения измерений, позволяющие разработчику приложения использовать их для собственных потребностей после завершения работы законодательно контролируемой части.

2) (I)/(II) ПО счетчика электрической энергии считывает первичные результаты измерений из цифроаналогового конвертера (ADC). Для правильного вычисления результатов измерений задержка между событием «данные готовы» от ADC для завершения буферизации результатов измерений является функционально необходимой. Первичные результаты считываются в режиме прерываний, инициируемых сигналом «данные готовы». Средство измерений может параллельно с помощью интерфейса взаимодействовать с другими электронными устройствами используя иные прерывания (законодательно неконтролируемые задачи). Интерпретируя требование п.5.2.1.для данной конфигурации, следует, что приоритет получения прерываний для обработки результатов измерений должен быть выше чем для передачи данных.

Техническое решение, приведенное в примерах 5.1.2.1.a), 5.1.2.1.b), 5.1.2.1.c), 5.1.2.1.d) приемлемо только в случаях нормального уровня безопасности (I). В случае если требуется повышенный уровень безопасности (см раздел 8), разделение ПО описанным методом не достаточно. В этом случае ПО рассматривается как законодательно контролируемое целиком.

5.2.2 Совместное отображение и печать информации

Совместное отображение или совместная печать законодательно контролируемой и иной информации могут быть реализованы в средстве измерений. Содержание и форма представления информации индивидуальны для каждого типа средства измерений, области применения и устанавливаются в соответствующих национальных стандартах. Тем не менее, если для отображения результатов используется многооконный пользовательский интерфейс должно выполняться следующее:

ПО, которое реализует отображение результатов измерений и иной измерительной информации, является законодательно контролируемой частью ПО. Окно пользовательского интерфейса, содержащее указанные данные должно иметь наивысший приоритет, т.е. окно не может быть убрано другой работающей программой, перекрыто окнами другой программы, минимизировано или сделано невидимым в течение проведения измерений, и текущие результаты необходимы для законодательно контролируемых целей.

Пример – (I) В системе, описанной в п. 5.2.1.2.a) - 5.2.1.2.d) результаты измерений отображаются в отдельном окне пользовательского интерфейса. Средства, описанные в п.5.2.1.2.d) гарантируют, что только законодательно контролируемая часть программы может считывать результаты измерений. В многооконной операционной системе должны применяться дополнительные технические средства для выполнения п.5.2.2: Окно, отображающее законодательно контролируемые данные, генерируется и контролируется процедурами соответствующей подключаемой динамической библиотеки (см. 5.2.1.2). Во время измерений данные процедуры циклически проверяют нахождение требуемого окна поверх всех остальных окон. Если это не так, соответствующая процедура размещает его поверх остальных окон.

Если требуется повышенная защита от мошенничества (II), одной распечатки, используемой в качестве отображения информации, может быть недостаточно. Должен быть предусмотрен функциональный блок со средствами защиты высокого уровня, который может отображать результаты измерений.

Использование для указанных целей универсального компьютера как части измерительной системы не приемлемо, если требуется повышенная степень защиты от мошенничества (II). Дополнительные меры предосторожности по предотвращению или минимизации риска мошенничества как в виде аппаратных, так и программных средств, следует предусмотреть, если требуется повышенная защита в случае использования универсального компьютера (например, PC, PDA и др.).

5.2.3 Хранение данных, передача через системы связи

Если результаты измерений используются не на месте проведения измерений или спустя некоторое время, возможно их перемещение из средства измерений и хранение (функционального блока, электронного устройства) в незащищенной среде перед их использованием в законодательно контролируемых целях. В этом случае вводятся должны выполняться следующие требования:

5.2.3.1 Для дальнейшего использования в сфере законодательной метрологии сохраненный или переданный результат измерения должен сопровождаться всей необходимой информацией.

Пример – (I)/(II) набор данных, например, состоит из следующих записей:
– результат измерения, включая единицу;
– время проведения измерения (см.5.2.3.7);
– место измерения или идентификацию средства измерения, которое использовалось для измерений;
– однозначная идентификация измерения, например, последовательность чисел, обеспечивающая прослеживаемость значений, напечатанных на чеке.

5.2.3.2 Данные должны быть защищены программными средствами для гарантии аутентичности, целостности, и, если необходимо, правильности информации в отношении времени измерения. ПО, которое отображает или обрабатывает результаты измерений или сопутствующие данные должно проверять время измерения, аутентичность и целостность данных после прочтения их из среды небезопасного хранения или получив их через небезопасный канал передачи данных. Если обнаружено несоответствие, то данные должны быть отвергнуты или отмечены как непригодные к применению.

Программные модули, которые подготавливают данные для хранения или передачи, или проверяют данные после чтения или получения, относятся к законодательно контролируемой части программного обеспечения.

Примечание – Необходимо предусмотреть высокий уровень защиты в случае использования открытой информационно-вычислительной сети.

Пример – (I) Программа прибора, передающего данные, рассчитывает контрольную сумму посылаемого набора данных (алгоритмы расчета контрольной суммы BCC, CRC16, CRC32 и др.) и добавляет полученное значение к передаваемым данным. При этом для расчета используется секретное начальное значение вместо значения, приведенного в стандарте. Это начальное значение сохраняется в программном коде в качестве константы. В программном коде посылающей или принимающей программы также сохранено это начальное значение. Перед использованием данных программа, их получившая, рассчитывает контрольную сумму и сравнивает рассчитанное значение со значением, содержащимся в полученном наборе данных. Если значения совпадают, набор данных не фальсифицирован. В противном случае программа предполагает фальсификацию и отвергает набор данных.

5.2.3.3 Для высокого уровня защиты необходимо использовать криптографические методы. Конфиденциальные ключи, используемые для этой цели, должны быть сохранены и защищены в средствах измерений, устройствах, или компонентах. Эти ключи могут быть введены или прочитаны только при нарушении средств защиты средства измерений.

Пример – (II) Программа, хранящая или посылающая данные, генерирует «электронную подпись» вычислением значения хеш-функции и шифрованием этого значения, используя секретный ключ криптосистемы с открытым ключом. Результатом действий является электронная подпись. Она присоединяется к сохраняемому или передаваемому набору данных. Получающая данные программа рассчитывает значение хеш-функции набора данных и расшифровывает подпись, присоединенную к набору данных с открытым ключом. Сравниваются рассчитанное и расшифрованное значение. Если они равны, набор данных не фальсифицирован (целостность доказана). Чтобы подтвердить, что данные пришли от нужного источника, принимающая сторона должна знать, действительно ли открытый ключ принадлежит отправителю, то есть устройству отправки. Поэтому открытый ключ отображается на устройстве вывода информации измерительного прибора и может быть зарегистрирован единожды, например, вместе с регистрационным номером устройства при утверждении типа. Если принимающая сторона уверена, что использовался правильный открытый ключ для декодирования подписи, в этом случае также доказана подлинность набора данных.

5.2.3.4 Автоматическое сохранение

5.2.3.4.a) Если в зависимости от применения средства измерений требуется хранение данных измерений, они должны сохраняться автоматически после завершения измерений, то есть когда было получено окончательное значение, которое используется в законодательно контролируемой области.

Устройство, используемое для долгосрочного хранения данных, должно быть достаточно надежным для обеспечения их сохранности в нормальных условиях хранения. Устройство должно иметь достаточную емкость хранения, отвечающую задачам конкретного применения.

Если окончательный результат измерений, используемый в законодательно контролируемых целях, получается расчетом, все данные участвующие в расчетах должны автоматически сохраняться с окончательным результатом измерений.

Примечание – Результат кумулятивного измерения, например, электрическая энергия или объем газа, постоянно обновляются. Поскольку всегда используется один и тот же домен данных (переменная в программе), требование, касающееся емкости устройства хранения, на кумулятивные измерения не распространяется.

5.2.3.4.b) Сохраненные данные могут быть удалены, при следующих условиях:

– работы с данными официально завершена;

– результаты измерений выведены на печать устройством, подлежащем законодательному контролю.

Примечание – Иными требованиями национального законодательства (например, налоговое законодательство) могут устанавливаться жесткие требования касательно удаления измерительных данных.

5.2.3.4.c) Если выполнены условия п. 5.2.3.4.b) и память средства измерений переполнена, допустимо удалять сохраненные данные при выполнении следующих двух условий:

– данные удаляются в последовательности, соответствующие последовательности записи результатов измерений с учетом правил, установленных для конкретного применения;

– удаление осуществляется автоматически или после инициализации процедуры удаления вручную.

Примечание – В случае ручного удаления информации необходимо дополнительно предусмотреть права доступа.

5.2.3.5 Задержка передачи данных

Задержка передачи данных никоим образом не должна влиять на измерение.

5.2.3.6 Прерывание передачи

Если сетевые службы становятся недоступными, результаты измерений не должны быть потеряны. Для предотвращения утери данных измерения должны быть прекращены.

Примечание – Следует принимать во внимание, являются ли измерения статическими или динамическими.

Пример – (I) / (II) передающее устройство ждет, пока принимающее устройство не пошлет сигнал подтверждения получения правильного набора данных. Пересылающее устройство хранит набор данных в буфере обмена данными пока не получено подтверждение. Буфер обмена данными может иметь возможность хранить более одного набора данных в формате FIFO .

5.2.3.7 Временной штамп

Временной штамп должен считываться с встроенных часов средства измерений. В зависимости от вида средства измерений или области его применения правильная установка времени часов может являться законодательно контролируемой операцией и, соответственно, должны быть использованы средства защиты установки времени, с учетом установленного уровня риска (см 5.1.3.2.c)).

Встроенные часы обособленного средства измерений имеют тенденцию к увеличению значения неопределенности, поскольку не имеют возможности синхронизации с глобальным временем. Если время важно в конкретной области применения, метрологическая надежность встроенных часов должна обеспечиваться специальными средствами или процедурами.

Пример – (II) Надежность встроенных кварцевых часов средства измерений повышается методом избыточности: Таймер принимает новое значение от часов микроконтроллера, которое генерируется другим кварцевым кристаллом. Когда значение таймера достигает предустановленного значения, например, 1 секунда, микроконтроллером генерируется специальная метка и процедура ПО дает сигнал на увеличение значения второго счетчика. В результате, например, в установленный момент ПО считывает значение встроенных кварцевых часов и рассчитывает разность в секундах. Если разность находится в установленных границах счетчик ПО обнуляется и процедура повторяется. Если разность превышает границы, ПО выполняет соответствующую корректировку ошибки.

5.2.4 Совместимость операционных систем и аппаратных средств, портативность

5.2.4.1 Разработчик должен идентифицировать приемлемые условия работы программных и аппаратных средств. Должны быть задекларированы минимальные ресурсы и приемлемая конфигурация (процессор, RAM, HDD, версия операционной системы и др.) необходимые для корректного функционирования.

5.2.4.2 В законодательно контролируемом ПО должны быть предусмотрены технические средства, предотвращающие выполнение операций, если минимальные конфигурационные требования не соблюдены. Система должна функционировать только в тех условиях, которые указаны изготовителем.

Если предусмотрено правильное функционирование в инвариантной среде, должны быть предусмотрены средства поддержания конкретной операционной среды в неизменном состоянии. Это особенно относится к универсальной ЭВМ, выполняющей законодательно контролируемые функции.

В общем случае, необходимо обеспечить неизменность аппаратных средств, операционной системы или системной конфигурации универсальной ЭВМ или даже исключить использование универсальной ЭВМ в следующих случаях:

– если требуется высокая степень соответствия (см. 5.2.5.d));

– если требуется определенное программное обеспечение (например, 5.2.6.3.b) для прослеживаемости обновления программного обеспечения);

– если должны использоваться криптографические алгоритмы или ключи (см. 5.2.3).

5.2.5 Соответствие утвержденному типу

5.2.5.1 Изготовитель должен выпускать приборы и законодательно контролируемое ПО, которые соответствуют утвержденному типу и представленной на утверждение типа документации. Различают следующие уровни соответствия:

a) идентичность законодательно контролируемых функций, описанных в документации (6.1) каждого отдельного средства измерений, с утвержденным типом (исполняемый код может отличаться);

b) идентичность законодательно контролируемых частей исходного кода, а остальная часть законодательно контролируемого программного обеспечения имеет степень соответствия a);

c) идентичность всего законодательно контролируемого исходного кода;

d) идентичность всего исполняемого кода.

Подходящая степень соответствия для каждого типа прибора или области применения должна быть установлена соответствующим национальным стандартом. Настоящий стандарт также может устанавливать набор степеней соответствия.

В случае разделения ПО в соответствии с п. 5.2.1.2, к части ПО не предъявляются требования соответствия (за исключением варианта d)).

Для очевидности соответствия утвержденному типу должны использоваться средства, описанные в п.5.1.1 и п.5.2.1.

Примечание – Перечисления a) и b) должны применяться в случае установления нормального уровня безопасности, а c) и d), в случае повышенного уровня безопасности.

5.2.6 Техническое обслуживание и изменение конфигурации

Обновление законодательно контролируемого ПО средства измерений, находящегося в эксплуатации, рассматривается следующим образом:

– модификация средства измерений, когда происходит замена ПО его другой утвержденной версией;

– ремонт средства измерений, когда происходит восстановление текущей версии ПО.

Средство измерений, которое было модифицировано или отремонтировано, находясь в эксплуатации, требуют проведения внеочередной поверки.

ПО, которое не является обязательным для правильного функционирования средства, не подвергается проверке после обновления.

5.2.6.1 Должны использоваться только те версии законодательно контролируемого ПО, соответствие которых было подтверждено при утверждении типа средства измерений (см. 5.2.5). Применимость данных условий зависит от вида средства измерений и должна быть установлена конкретными стандартами на данное средство измерений. Нижеприведенные варианты п. 5.2.6.2 и 5.2.6.3 являются эквивалентными альтернативными решениями. Данное требование касается проверки ПО средств измерений, находящихся в эксплуатации. Дополнительные требования указаны в разделе 7.

5.2.6.2 Верифицированное обновление

Обновление ПО может быть загружено локально, то есть непосредственно с использованием функций средства измерения, или удаленно по сети. Процесс загрузки и инсталляции может быть представлен как двумя разными действиями (как показано на рисунке 1) так и одним, в зависимости от реализации технического решения. На момент изменения ПО в месте установки средства измерений должен присутствовать оператор для удостоверения успешного завершения обновления. После обновления законодательно контролируемого ПО средства измерений (замена другой утвержденной версией или переустановка) не разрешается использование средства измерений в сфере законодательной метрологии до тех пор пока не будет проведена поверка прибора (как указано в главе 7) и пока не будет возобновлено действие средств защиты (если иное не предусмотрено национальным стандартом или не указано в описании типа утвержденного типа средства измерений).

5.2.6.3 Прослеживаемое обновление

ПО, применяемое в составе средства измерений, соответствует требованиям к прослеживаемому обновлению (с 5.2.6.3.a) по 5.2.6.3.g)) если выполняются требования соответствующего стандарта на средство измерений. Прослеживаемое обновление это процедура изменения ПО в поверенном приборе или устройстве, после которого не требуется проведения уполномоченным органом внеочередной поверки. Обновление программного обеспечения может быть загружено локально, то есть непосредственно на средстве измерения или удаленно по сети. Отметка об обновлении ПО должна быть занесена в соответствующий журнал аудита (см. 3.1.2). Процедура прослеживаемого обновления включает несколько

шагов: загрузка, проверка целостности, проверка происхождения (аутентификация), инсталляция, регистрация и активация.

5.2.6.3.a) Прослеженное обновление программного обеспечения должно быть автоматическим. По окончании процедуры обновления защита программного обеспечения должна соответствовать уровню, требуемому процедурой утверждения типа.

5.2.6.3.b) Средство измерения (устройство, функциональный блок) должно иметь неизменное законодательное контролируемое ПО, которое не может быть обновлено и которое содержит все необходимые функции для выполнения требований предъявляемых при прослеживаемом обновлении.

5.2.6.3.c) Должны использоваться технические средства для гарантии аутентичности загружаемого ПО, т.е. того что обновление поступает от владельца сертификата об утверждении типа. Если загруженное ПО не проходит эту проверку, средство измерений должно отклонить это обновление и использовать предыдущую версию ПО.

Пример – (II) Это может быть достигнуто, например, такими криптографическими средствами, как система открытых ключей. Держатель сертификата утверждения типа (обычно им является изготовитель средства измерений) генерирует в рамках производственного процесса цифровую подпись обновленной версии ПО, используя закрытый (секретный) ключ. Подпись проверяется во время загрузки ПО в средство измерений с использованием открытого ключа. Если цифровая подпись загруженного ПО является правильной, происходит установка ПО в средство измерений и его активация. Если цифровая подпись загруженного ПО некорректна, установка не проводится и используется предыдущая версия ПО или работа средства измерений блокируется.

5.2.6.3.d) Технические средства должны использоваться для гарантии целостности загруженного ПО, то есть, чтобы гарантировать, что не были внесены недопустимые изменения перед загрузкой. Это может быть достигнуто добавлением контрольной суммы (хеш-кода) загружаемого ПО и её (его) сличением во время процедуры загрузки. Если загруженное ПО не пройдет этот тест, средство измерений должно игнорировать это обновление и использовать предыдущую версию ПО или работа средства измерений блокируется. Возобновить процедуру обновления ПО невозможно, если пропущен один из этапов диаграммы прослеживаемого обновления.

5.2.6.3.e) Соответствующими техническими средствами, например, журналом аудита, должно гарантироваться, что прослеживаемые обновления законодательно контролируемого ПО прослеживаемы для целей последующего надзора или метрологического контроля. Это требование позволяет инспекционным органам, которые ответственны за метрологический контроль за средствами измерений, отслеживать прослеживаемое обновление законодательно контролируемой части ПО через определенный промежуток времени (который установлен в национальном законодательстве).

Журнал аудита должен содержать следующую информацию: успешное / неудачное завершение процедуры обновления, идентификацию программного обеспечения установленной версии, временной штамп события, идентификация исполнителя загрузки. Запись создается для каждой попытки обновления, независимо от её результата.

Средства хранения, которые участвуют в реализации прослеживаемого обновления ПО, должны иметь достаточную емкость для сохранения информации об обновлениях как минимум в течение срока периодической поверки. Должны быть предусмотрены технические средства, которые после достижения предела ёмкости запоминающего устройства для журнала аудита не позволяют осуществлять процедуру обновления без вскрытия пломб средства измерений.

Примечание – Данное требование позволяет органам, которые отвечают за метрологический контроль законодательно контролируемых средств измерений проследить историю обновлений законодательно контролируемого ПО в течение предписанного периода времени.

5.2.6.3.f) В зависимости от требований законодательства может требоваться обязательное согласие владельца средства измерений на выполнение загрузки и обновления ПО. Средство измерений должно иметь функциональный блок или электронное устройство позволяющее владельцу или пользователю средства измерений заблаговременно выразить согласие на загрузку ПО, например, нажатием клавиши. Данный функциональный блок или устройство должно быть отключаемым, например, пломбируемым переключателем или командой программы. При активизированном переключателе включенного функционального блока или устройства каждая загрузка должна требовать участия пользователя или владельца средства измерений. При выключенном переключателе не требуется каких-либо действий со стороны пользователя или владельца средства измерений для осуществления загрузки ПО.

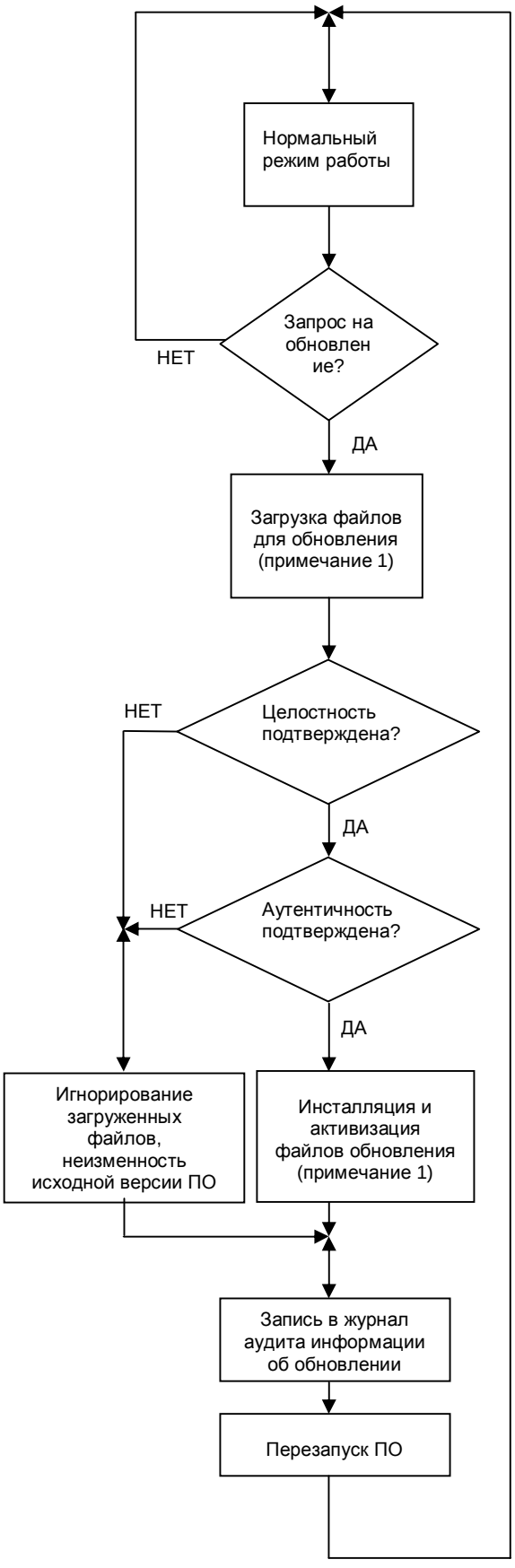
5.2.6.3.g) Если требования с п.5.2.6.3.a) по п.5.2.6.3.f) не могут быть выполнены, обновление законодательно неконтролируемую части ПО возможно, должны выполняться следующие требования:

– имеется явное разделение законодательно контролируемой и неконтролируемой частей ПО в соответствии с 5.2.1.

– законодательно контролируемая часть ПО не может быть обновлена без нарушения средств защиты;

– в сертификате утверждения типа указано, что допускается обновление законодательно контролируемой части.

Прослеживаемое обновление (5.2.6.3)



Верифицированное обновление (5.2.6.2)

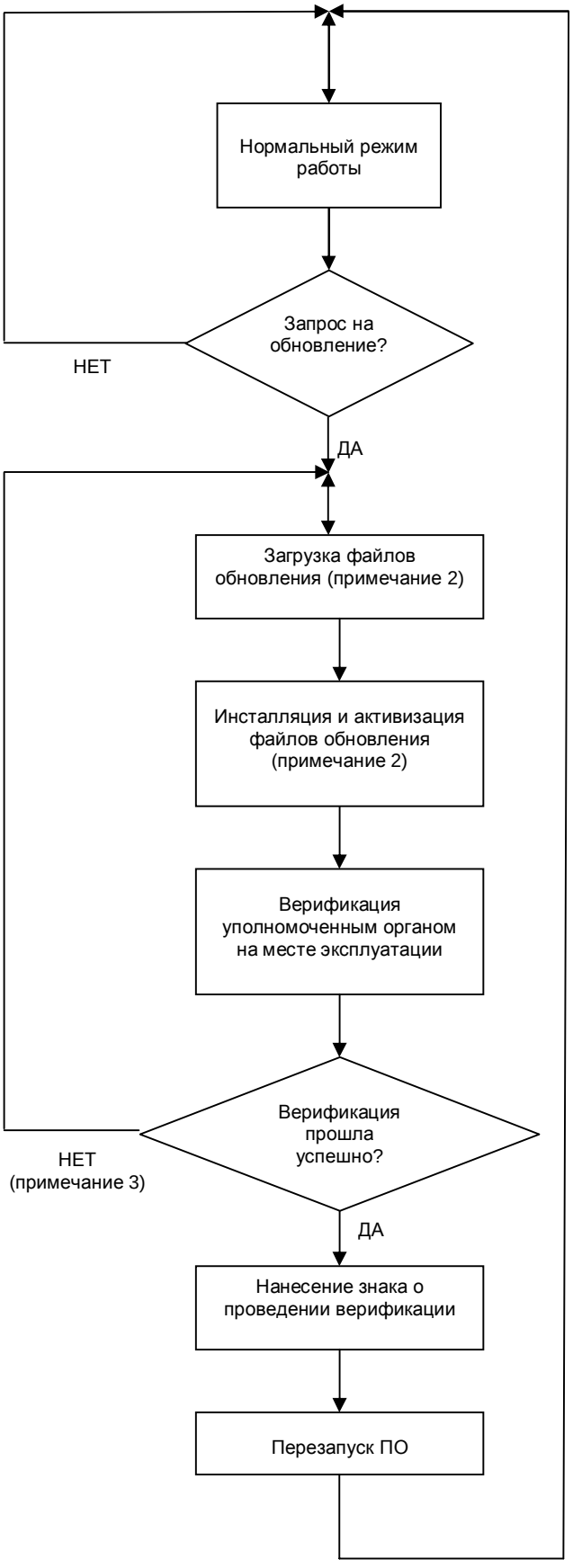


Рисунок 1 – Процедуры обновления ПО

Примечания:

1) В случае прослеживаемого обновления процесс обновления разделен на два этапа: «загрузка» и «установка/активизация». Подразумевается, что после завершения загрузки ПО временно сохраняется, не будучи активизированным, потому что, если загруженное ПО не проходит проверки, должна быть возможность отклонить установку загруженного ПО и оставить для использования старую версию.

2) В случае верифицированного обновления ПО может также быть загружено и временно сохранено перед установкой, но в зависимости от технической реализации, загрузка и установка может быть реализована одним действием.

3) Здесь подразумевается, что отрицательный результат верификации вызван исключительно проблемами загруженного обновления ПО. Невозможность обновления, вызванная другими причинами, не подразумевает повторной загрузки или повторной установки, обозначенной веткой алгоритма «нет».

5.2.6.4 Стандартами на конкретное средство может требоваться установка определенных устройство-определяющих параметров, доступных пользователю. В таком случае, средство измерений должно иметь техническое решение, которое автоматически и неудаляемо записывает факт изменения параметра, например, журнал аудита. Средство измерений должно иметь функцию отображения записей журнала.

Примечание – Счетчик событий не является приемлемым решением.

5.2.6.5 Средства обеспечения прослеживаемости и записи являются частью законодательно контролируемого ПО и должны иметь соответствующую защиту. ПО служащее для отображения журнала аудита (5.2.6.2; 5.2.6.3) рассматривается в качестве фиксированного законодательно контролируемого ПО.

6 Процедура утверждения типа

6.1 Документация, предоставляемая при утверждении типа

В целях утверждения типа изготовитель средства измерений должен заявить и документировать все функции ПО, контролируемые структуры данных и интерфейсы, которые реализованы в средстве измерений. Не должно быть скрытых функций, не отраженных в документации.

Команды и их действие должны быть описаны полностью в документации на ПО, предъявленной на утверждение типа средства измерений. Изготовитель должен заявить (в виде декларации) о полноте документации, описывающей используемые команды. Если команды могут быть введены через пользовательский интерфейс, они должны быть полностью описаны в документации на ПО, предоставляемой на утверждение типа.

Заявка на утверждение должна сопровождаться документом или иным доказательством, которое подтверждает, что структура и характеристики ПО средства измерений соответствуют требованиям стандарта на конкретный вид средства измерений, в котором присутствуют общие положения настоящего стандарта.

6.1.1 Типовая документация (для каждого измерительного прибора, устройства, или компонента) должна включать:

1) описание законодательно контролируемого ПО и того как выполняются требования:
   - перечень программных модулей, которые относятся к законодательно контролируемой части (приложение Б) включая декларацию, что все функции, которые влияют на измерение, документированы.
   - описание интерфейсов законодательно контролируемой части ПО (приложение В), команд и потоков данных через данные интерфейсы, включая декларацию о полноте данного писания;
   - описание метода получения идентификации ПО;
   - в зависимости от выбранного метода валидации, согласно стандарта на конкретное средство измерений (см. 6.3, 6.4), должен быть обеспечен доступ к исходному коду в зависимости от того требуется ли высокий уровень соответствия и защиты;
   - перечень параметров, подлежащих защите и описание средств защиты

2) описание приемлемой системной конфигурации и минимальных требуемых ресурсов (см. 5.2.4);

3) описание средств безопасности операционной системы (пароль и т.п., если применимо);

4) описание метода пломбировки (с помощью ПО);

5) описание аппаратной конфигурации, например, блочная диаграмма, тип компьютера, тип информационно-вычислительной сети , и т.д. Если компонент аппаратной части выполняет законодательно контролируемые функции, то это также должно быть описано;

6) описание точности алгоритмов (как фильтрование результатов аналогово-цифрового преобразования, вычисления цены, алгоритмы округления и т.д.).

7) описание пользовательского интерфейса, меню и диалогов;

8) идентификация ПО и инструкции по просмотру идентификации на средстве измерений, находящемся в эксплуатации;

9) перечень команд каждого аппаратного интерфейса средства измерений, электронного функционального блока или устройства, включая декларацию полноты описания;

10) перечень ошибок влияющих на надежность средства измерений, определяющихся ПО и, при необходимости, описание алгоритмов их определения;

11) описание сохраняемых или передаваемых наборов данных;

12) если предусмотрена процедура обнаружения сбоев в программном обеспечении, необходимо привести список ошибок, которые могут быть обнаружены и описание алгоритма их обнаружения;

13) руководство по эксплуатации.

6.2 Требования к проведению процедуры утверждения типа

Методы испытаний, проводимых во время утверждения типа базируются на отработанных подходах, условиях испытаний и точных сравнительных измерениях. Процедуры "Испытание" и "Валидация" ПО имеют разное смысловое значение. Точность или правильность ПО не могут быть измерены в метрологическом смысле, хотя есть стандарты, описывающие как "измерить" качество ПО [например, ISO/IEC 14598]. Процедуры, описанные в настоящем стандарте, учитывают подходы, используемые в законодательной метрологии, а также хорошо известные методы валидации и испытаний в области разработки ПО, не преследуя цели которые, например, ставит перед собой разработчик ПО в целях минимизации ошибок и оптимизации функционирования. Как показано в п. 6.4 каждое требование к ПО требует индивидуальной проработки процедур валидации. Объем работ в процедуре должен подтверждать требования, предъявляемые к точности, надежности и защите от мошенничества.

Целью работ по валидации является подтверждение того, что средство измерений, тип которого утверждается, соответствует требованиям действующего в отношении него стандарта, в котором также могут быть приведены требования к экспертизе, анализу, и испытаниям ПО.

Методы, описанные ниже, касаются только процедуры утверждения типа и не затрагивают вопросы метрологического контроля отдельных единиц средств измерений, находящихся в эксплуатации (см. раздел 7).

Методы валидации ПО описаны в п.6.3. Комбинации этих методов, формирующих полную программу валидации, адаптированную ко всем требованиям, определенным в разделе 5 указаны в п. 6.4.

6.3 Методы валидации (исследование ПО)

6.3.1 Обзор методов и их применения

Выбор и последовательность методов строго не определены и могут изменяться в каждом конкретном случае.

Таблица 1 – Обзор выбранных методов валидации

Аббревиатура	Описание	Применение	Предусловие, используемые средства	Требуемые специальные навыки
AD	Анализ документации, спецификации и валидации проекта (6.3.2.1)	Всегда	Документация	-
VFTM	Валидация метрологических функций ПО (6.3.2.2)	Корректность алгоритмов, неопределенность, компенсирующие и корректирующие алгоритмы, правила расчета цен.	Документация	-
VFTSw	Валидация функциональных возможностей ПО (6.3.2.3)	Корректное функционирование коммуникационных интерфейсов, индикации, защита от мошенничества, защита от ошибок оператора, защита параметров, обнаружение сбоев	Документация, текстовый редактор	-
DFA	Анализ потока метрологических данных (6.3.2.4)	Разделение ПО, оценка воздействия команд на функции средства измерений	Исходный код, текстовый редактор (простая процедура), специальные инструменты (сложная процедура)	Знание языков программирования. Инструкция для реализации метода

Окончание таблицы 1

Аббревиатура	Описание	Применение	Предусловие, используемые средства	Требуемые специальные навыки
CIWT	Анализ кода и переменных (6.3.2.5)	Для всех целей	Исходный код, текстовый редактор	Знание языков программирования, протоколов, и иных вопросов информационных технологий.
SMT	Испытание программных модулей (6.3.2.6)	Для всех целей, когда входные и выходные данные могут быть четко определены	Исходный код, средства тестирования, специальные программные средства	Знание языков программирования, протоколов обмена, и иных вопросов информационных технологий. Инструкция по использованию необходимых средств.
Примечание – Текстовые редакторы, редакторы в шестнадцатеричном формате, и т.п. рассматриваются в качестве “обычных программных средств”.				

6.3.2 Описание выбранных методов валидации

6.3.2.1 Анализ документации, спецификации и валидация проекта (AD)

Применение: Основная процедура, которая должна проводиться в каждом случае

Предусловие:

Процедура основана на изучении документации изготовителя средства измерений. В зависимости от требований, документация должна иметь соответствующее содержание:

1) Спецификация в общем виде внешне доступных функций средства измерений (Для простых средств измерений без интерфейсов, кроме показывающего устройства. Все функциональные возможности могут быть проверены в ходе испытаний. Низкий риск мошенничества).

2) Спецификация функций и интерфейсов ПО (Для средств измерений с интерфейсами и если функции прибора не могут быть функционально проверены, а также в случае высокого риска мошенничества). Описание должно охватывать и пояснять все функции, которые могут влиять на метрологические характеристики.

3) Документация, касающаяся интерфейсов, должна содержать полный перечень команд или сигналов, которые ПО может интерпретировать. Действие каждой команды должно быть подробно документировано. Должно быть описано, как средство измерений реагирует на недокументированные команды.

4) В случае необходимости, для правильного понимания и оценки функций ПО, должна быть представлена дополнительная документация для сложных измерительных алгоритмов, криптографических функций или критических временных ограничений.

5) Когда не ясно, как валидировать ПО, разработка методики испытаний должна быть возложена на изготовителя. Кроме того, программист разработчика должен быть доступен для ответа на все вопросы эксперта уполномоченного органа.

Общим условием проведения экспертизы являются полнота документации и ясная идентификация испытываемого средства измерений, т.е. пакетов программ, которые участвуют в выполнении метрологических функций (см. 6.1.1).

Описание:

Эксперт пробует понять функции и функциональные возможности средства измерений, используя устное описание и графические представления, и решает, соответствуют ли они требованиям соответствующего стандарта. Метрологические требования, так же как и функциональные требования, определенные в главе 5 (как, например, защита от мошенничества, защита параметров настройки, средства связи с другими устройствами, запрещенные функции, обновление программного обеспечения, обнаружение ошибки и др.) должны быть рассмотрены и оценены. Для этой задачи могут быть использованы контрольные листы (см. Приложение В).

Результат:

Эта процедура дает результат по проверке всех характеристик средства измерений, если необходимая документация была представлена изготовителем в полном объеме. Результат должен быть документирован в отчете об испытаниях ПО (см. Приложение В), являющемся частью отчета об испытаниях, форма которого может быть установлена стандартом на конкретное средство измерений.

Дополнительные процедуры:

Дополнительные процедуры должны быть применены, если экспертиза документации не может дать обоснованные результаты валидации. В большинстве случаев “Валидация метрологических функций опробованием” (см. 6.3.2.2) является дополнительной процедурой.

Ссылки:

FDA, Guidance for FDA Reviewers and Industry Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, 29 May 1998 [10];

IEC 61508-7: 2000 - 3 [9].

6.3.2.2 Валидация метрологических функций (VFTM)

Применение:

Правильность алгоритмов получения (расчета) результата измерения из исходных данных, поправка на условия окружающей среды, округление при вычислении цены и т.д.

Предусловие:

Руководство по эксплуатации, схема функционирования, метрологические нормы и испытательное оборудование.

Описание:

Большинство методов испытаний основано на эталонных измерениях в разных условиях. Их использование не ограничено технологическими решениями конструкции прибора. Хотя данный метод не ставит задачей валидировать ПО, результаты испытаний могут быть использованы для валидации отдельных частей ПО, особенно реализующих основные метрологические функции. Если испытания, описанные в стандарте на конкретный вид средства измерений, охватывают все законодательно контролируемые функции, соответствующие им части ПО, при положительных результатах испытаний, могут рассматриваться как валидированные. В этом случае не требуется проведение дополнительного анализа ПО или испытаний для валидации метрологических функций средства измерений.

Результат:

Алгоритмы корректны или нет. Результаты измерений при всех допустимых условиях превышают МДП или нет.

Дополнительные процедуры:

Этот метод обычно является дополнением к п. 6.3.2.1. В определенных случаях для упрощения и повышения эффективности работ можно комбинировать этот метод с экспертизой исходного кода (6.3.2.5) или имитировать входные сигналы (6.3.2.6), например, в случае динамических измерения.

Ссылки:

Стандарты на средства измерений и их функционирование.

6.3.2.3 Валидация функциональных возможностей ПО (VFTSw)

Применение:

Валидация, например, параметров защиты, отображения идентификации ПО, функции обнаружения ошибок, конфигурации системы (особенно программной среды) и т.д.

Предусловия:

Руководство по эксплуатации, документация ПО, схема функционирования, испытательное оборудование.

Описание:

Функциональные возможности, описанные в руководстве по эксплуатации, документации на средство измерений или документации на ПО проверяются практически. В случае корректной работы функций, реализуемых ПО, они принимаются как валидированные без дальнейшей экспертизы ПО. Такими функциями являются, например:

- нормальное функционирование средства измерений, в случае если оно контролируется ПО. Все переключатели или ключи, а также их возможные комбинации должны быть проверены и их влияние на работу средства измерений должно быть оценено. В графических интерфейсах пользователя все меню и другие графические элементы должны быть активизированы и проверены.

- эффективность защиты параметров может быть проверена активизацией защиты и попытки изменить параметр;
- эффективность защиты сохраненных данных может быть проверена изменением некоторых данных в файле с последующей проверкой реакции ПО на такое изменение;
- генерирование и отображение идентификации ПО может быть валидировано практической проверкой;
- если в ПО предусмотрена возможность обнаружения ошибки, законодательно контролируемые части могут быть валидированы имитацией ошибки и проверкой реакции на нее средства измерений;
- если конфигурация или программная среда законодательно контролируемого ПО должна быть неизменяемой, работа средств защиты ПО может быть проверена, внесением недопустимых изменений. ПО должно запретить эти изменения или прекратить работу.

Результат:

Исследуемые функции, реализуемые ПО, соответствуют требованиям или нет.

Дополнительные процедуры:

Некоторые функции ПО или функции средства измерений, управляемого ПО, не могут быть валидированы описанным способом. Если в приборе есть интерфейсы, невозможно обнаружить недопустимые команды только методом случайного перебора команд. В случае обычной валидации, включение в список документации, приведенного в п. 6.3.2.1, декларации изготовителя об отсутствии недокументированных команд или возможностей может быть достаточным. При проведении тщательной валидации необходим анализ ПО, как описано в п. 6.3.2.4 или п. 6.3.2.5.

Ссылки:

FDA Guidance for Industry Part 11, August 2003 [11]; WELMEC Guide 2.3 [12]; WELMEC Guide 7.2 [13].

6.3.2.4 Анализ потока метрологических данных (DFA)

Применение:

Структура потока данных измерения через области данных подлежит законодательному контролю. Экспертиза разделения ПО.

Предусловия:

Документация ПО, исходный код, текстовый редактор, программа поиска текста или специальные средства. Знание языков программирования.

Описание:

Целью данного метода является нахождение всех частей ПО, которые участвуют в расчете результата измерения или которые могут на него влиять. Проверяется структура данных, начиная с подпрограммы, которая считывает исходные данные, поступившие от первичного преобразователя на аппаратный интерфейс средства измерений. Подпрограмма присваивает значение исходных данных переменной, возможно, проделав некоторые вычисления. Значение, хранимое в этой переменной, считывается другой подпрограммой и т.д. до тех пор, пока окончательный результат измерения не отобразится на экране. Все переменные, используемые для хранения промежуточных результатов измерения, и все подпрограммы, транспортирующие эти значения, могут быть найдены в исходном коде с помощью текстового редактора, имеющего функцию поиска текста, в т.ч. переменных или имен подпрограмм в другом файле, открытом в текстовом редакторе в текущий момент. Другие потоки данных также могут быть найдены этим методом, например, с интерфейсов к интерпретатору полученных команд. Кроме того данный метод может выявить обход программного интерфейса (см. 5.2.1.2).

Результат:

Может быть валидировано разделение ПО в соответствии п. 5.2.1.2.

Дополнительные процедуры:

Этот метод рекомендуется, если реализовано разделение ПО, требуется высокая степень соответствия или повышенная защита от мошенничества. Этот метод является расширением возможностей проверки по п. 6.3.2.1, п. 6.3.2.3 и п. 6.3.2.5.

Ссылки:

IEC 61131-3

6.3.2.5 Анализ кода и переменных (CIWT)

Применение:

Любая функциональная возможность ПО может быть валидирована этим методом, если необходима детальная экспертиза.

Предусловия:

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

Описание:

Эксперт последовательно исследует исходный код, пробует понять соответствующую часть кода и решает, выполнены ли требования и соответствуют ли функции и функциональные возможности, следующие из программной документации.

Эксперт может также остановиться на алгоритмах или функциях, которые он идентифицировал как сложные, подверженные ошибками, недостаточно документированные и т.д. и изучает соответствующую часть исходного кода, анализируя и проверяя ее.

До выполнения этих этапов экспертизы обычно идентифицируется законодательно контролируемая часть ПО, например, используя анализ потока метрологических данных (см. 6.3.2.4). В общем случае, анализ кода ограничивается этой частью.

Результат:

Соответствие или несоответствие реализации ПО документации и требованиям к ПО.

Дополнительные процедуры:

Этот метод используется дополнительно к 6.3.2.1 и 6.3.2.4. Обычно этот метод применяется при выборочных проверках.

Ссылки:

IEC 61508-7:2000-3 [9].

6.3.2.6 Испытание программных модулей (SMT)

Применение:

Применяется только, если требуется высокая степень соответствия и усиленная защита от мошенничества. Этот метод применяется, когда функции программы не могут быть проверены только на основе письменной информации. Этот метод является подходящим и экономически выгодным при валидации динамических алгоритмов измерения.

Предусловия:

Исходный код, средства разработки (как минимум, программа компилятор), функционирующая программная среда исследуемого программного модуля, входной набор данных и соответствующий правильный набор выходных данных или средства для автоматизации. Обязательно иметь навыки в области информационных технологий, знание языков программирования. Необходимо сотрудничество с разработчиком испытываемого модуля.

Описание: Исследуемый программный модуль интегрирован в испытательную программную среду, то есть существует специфический испытательный программный модуль, который вызывает исследуемый модуль и передаёт ему все необходимые входные данные. Испытательная программа получает выходные данные испытываемого модуля и сравнивает их с эталонными данными.

Результат:

Измерительный алгоритм или другие проверенные функций реализованы правильно или нет.

Дополнительные процедуры:

Это - расширенный метод, дополнительно к 6.3.2.2 или 6.3.2.5. Применяется в исключительных случаях.

Ссылки:

IEC 61508-7:2000 – 3 [9].

6.4 Программа валидации

Процедура валидации состоит из комбинации методов анализа и испытаний. Соответствующими стандартами могут устанавливаться детали программы валидации, включая:

a) какой из методов валидации, описанных в п. 6.3 будет использоваться для проверки рассматриваемого требования;

b) как оценивать результаты испытаний;

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

В Таблице 2 для процедур валидации определены два альтернативных уровня А и Б . Уровень Б подразумевает расширенную экспертизу по сравнению с А. Выбор между типом А и Б процедур валидации может быть определен стандартом на конкретное средство измерений или с учетом следующего:

- риск мошенничества;
- область применения;
- необходимая степень соответствия утвержденному типу;
- риск получения неправильного результата измерения из-за нарушения правил эксплуатации.

Таблица 2 – Рекомендации по комбинированию методов анализа и испытаний на различные требования (аббревиатуры см. в таблице 1)

Требование		Процедура валидации А (обычная экспертиза)	Процедура валидации Б (расширенная экспертиза)	Комментарий
5.1.1	Идентификация ПО	AD + VFTSw	AD + VFTSw + CIWT	“Б” - если требуется высокая степень соответствия
5.1.2	Правильность алгоритмов и функций	AD + VFTM	AD + VFTM + CIWT/SMT	
Защита ПО				
5.1.3.1	Предотвращение случайного неправильного использования	AD + VFTSw	AD + VFTSw	
5.1.3.2	Защита от мошенничества	AD + VFTSw	AD + VFTSw + DFA/CIWT/SMT	“Б” - в случае высокого риска мошенничества
Поддержка аппаратных средств				
5.1.4.1	Обнаружение ошибки	AD + VFTSw	AD + VFTSw + CIWT + SMT	“Б” – если требуется высокая степень надежности
5.1.4.2	Support of durability protection	AD + VFTSw	AD + VFTSw + CIWT + SMT	“Б” – если требуется высокая степень надежности
Определение и разделение контролируемых частей, и определение их интерфейсов				
5.2.1.1	Разделение устройств и блоков	AD	AD	
5.2.1.2	Разделение частей ПО	AD	AD + DFA/CIWT	
5.2.2	Совместное отображение	AD + VFTM/ VFTSw	AD + VFTM/ VFTSw + DFA/CIWT	
5.2.3	Хранение данных, передача через системы связи	AD + VFTSw	AD + VFTSw + CIWT/SMT	“Б” – в случае передачи данных измерения в открытой системе
5.2.3.1	Сохраненный или переданный результат измерений должен сопровождаться всей необходимой информацией для его дальнейшего использования в законодательно контролируемых целях. быть автоматически сохранены, когда измерения завершены.	AD + VFTSw	AD + VFTSw + CIWT/SMT	“Б” – в случае высокого риска мошенничества
5.2.3.2	Данные должны быть защищены средствами программного обеспечения для гарантии аутентичности, целостности и, если необходимо, правильности информации о времени проведения измерений	AD + VFTSw	-	
5.2.3.3	Для высокого уровня защиты необходимо использовать криптографические методы	-	AD + VFTSw + SMT	
5.2.3.4	Автоматическое сохранение	AD + VFTSw	AD + VFTSw + SMT	
5.2.3.5	Задержка передачи данных	AD + VFTSw	AD + VFTSw + SMT	“Б” – в случае высокого риска мошенничества, например, передача данных в открытых системах

Окончание таблицы 2

Требование		Процедура валидации А (обычная экспертиза)	Процедура валидации Б (расширенная экспертиза)	Комментарий
5.2.3.6	Прерывание передачи данных	AD + VFTSw	AD + VFTSw + SMT	“Б” – в случае высокого риска мошенничества, например, передача данных в открытых системах
5.2.3.7	Временная штамп	AD + VFTSw	AD + VFTSw + SMT	
5.2.4	Совместимость операционных систем и аппаратных средств, транспортабельность	AD + VFTSw	AD + VFTSw + SMT	
Техническое обслуживание и изменение конфигурации				
5.2.6.1	Верифицированное обновление	AD	AD	
5.2.6.2	Прослеживаемое обновление	AD + VFTSw	AD + VFTSw + CIWT/SMT	“Б” – в случае высокого риска мошенничества

6.5 Испытываемое оборудование

Обычно, испытания проводятся на полностью собранном средстве измерений (функциональное испытание). Если размер или конфигурация средства измерений не позволяют проведение испытаний как единого целого или если интерес представляет только отдельное устройство (модуль) средства измерений, в соответствующем стандарте может быть определено, что испытания могут проводиться отдельно на электронном устройстве или программных модулях, при условии, что смоделированное оборудование позволяет обеспечить нормальный режим работы испытываемого средства измерений.

7 Верификация

В процессе эксплуатации при проведении метрологического контроля средств измерений должна проверяться идентификация ПО, соответствие законодательно контролируемых настроек, соответствие утвержденному типу.

Стандартом на конкретное средство измерений может требоваться проведение проверки (верификации) программного обеспечения на одном или нескольких этапах метрологического контроля в соответствии с особенностями средства измерений.

Проверка программного обеспечения должна включать:

- оценку соответствия ПО утвержденной версии (например, сверка версии ПО и контрольной суммы);
- проверку минимально заявленной конфигурации, если указано в сертификате утверждения типа;
- проверку правильности конфигурации интерфейса входа/выхода средства измерений в программном обеспечении, если данная конфигурация является устройство-определяющим параметром;
- проверкой правильности устройство-определяющих параметров (особенно параметров настройки)

Процедуры обновления программного обеспечения описаны в п.5.2.6.2 и 5.2.6.3.

8 Оценка уровней жесткости (риска)

8.1 Настоящий раздел является руководством по определению уровня жесткости испытаний электронных средств измерений. Эта глава не может рассматриваться как классификация со строгими границами как в случае с классификацией точности.

Кроме того, уровни жесткости испытаний, отличные от описанных в настоящем стандарте, могут быть установлены в стандарте на конкретное средство измерений с указанием специальных пределов.

8.2 Уровень жесткости должен выбираться независимо для каждого требования.

8.3 Определяя уровни жесткости для специфической категории средств измерений и области применения (торговля, здравоохранение, ...), следующие аспекты могут быть приняты во внимание:

а) риск мошенничества:

- последствия и социальное\социалогическое влияние некорректного функционирования;
- ценность товаров, которые будут измеряться;
- используемая платформа (универсальный или специализированный компьютер);

- возможность возникновения ситуаций, потенциально приводящих к мошенничеству (устройство самообслуживания).

b) требуемое соответствие:

- практическая возможность для промышленности выполнить предписанный уровень.

c) требуемая надежность:

- окружающие условия;
- последствия и социальное\социалогическое влияние ошибок.

d) интерес мошенника:

- простота возможности мошенничества может являться достаточной мотивацией.

e) возможность повтора измерения или его прерывания.

В главе посвященной определению требований (см гл.5) приведены различные примеры приемлемых технических решений, иллюстрирующие фундаментальный уровень защиты от мошенничества, уровни соответствия, надежности, и типа измерения (отмечено как (I)). Где приемлемо, приведены примеры с повышенными мерами защиты, что предполагает повышенный уровень жесткости для выполнения вышеуказанных требований (отмечено как (II)).

Процедура валидации и уровни жесткости (риска) неразрывно связаны. Глубокий анализ программного обеспечения должен выполнятся для выявления недостатков или слабостей защиты при назначении повышенного уровня жесткости. С другой стороны, механическая пломбировка (пломбировка интерфейсов или корпуса) должна приниматься во внимание при выборе процедуры валидации.

Приложение А
(справочное)
Библиография

[1] International vocabulary of metrology – Basic and general concepts and associated terms (VIM), 3rd edition, 2012 (Международный словарь по метрологии - Основные и общих понятия и связанные с ними термины (VIM3:2012)*

[2] OIML B 3:2003 The OIML Certificate System for Measuring Instruments (OIML B 3:2003 «Система сертификатов МОЗМ для средств измерений»)

[3] OIML D 11:2004 General requirements for electronic measuring instruments
(OIML D 11:2004 «Общие требования к электронным средствам измерений»)

[4] ISO/IEC 9594-8:2001 Information technology -- Open Systems Interconnection -- The Directory: Publickey and attribute certificate frameworks
(ISO/IEC 9594-8:2001 «Информационные технологии. Взаимосвязь открытых систем. Директория. Структура сертификатов открытого ключа и атрибутов»)

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

[6] IEC 61508-4:1998-12 Contains the definitions and explanation of terms that Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations
(IEC 61508-4:1998-12 “Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Определения и сокращения”)

[7] ISO/IEC 14598 series Information technology – Software product evaluation
(Все части ISO/IEC 14598. «Информационные технологии. Оценка программного продукта»)

[8] OIML V 1:2013 International vocabulary of terms in legal metrology (VIML), (OIML V 1:2013 Международный словарь законодательной метрологии (VIML)**

[9] IEC 61508-7:2000 – 3 Functional safety of electrical/electronic/programmable electronic safety related systems - Part 5: Examples of methods for the determination of safety integrity levels
(IEC 61508-7:2000 – 3 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Обзор методов и средств»)

[10] FDA, Guidance for FDA Reviewers and Industry Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, 29 May 1998
(«FDA, Руководство по проведению FDA для специалистов и изготовителей медицинского оборудования на этапе подготовки документации для допуска на рынок», от 29 мая 1998)

[11] FDA Guidance for Industry Part 11, August 2003
(FDA. Руководство для изготовителей, Часть 11, Август 2003)

[12] WELMEC Guide 2.3, May 2005 Issue 3 Guide for Examining Software (Weighing Instruments)
(Руководство WELMEC 2.3 “Испытания программного обеспечения (Взвешивающие приборы)

[13] WELMEC Guide 7.2, May 2008 Issue 3 Software Guide (Measuring Instruments Directive 2004/22/EC)
(Руководство WELMEC 7.2 “Руководство по программному обеспечению”, 3 издание, май 2008, к Директиве по средствам измерений 2004/22/EC)

* Действует взамен VIM:1993
** Действует взамен OIML V1:2000

Приложение Б

(справочное)

Пример отчета об испытаниях программного обеспечения

Примечание – Отдельными стандартами может быть установлено какая информация должна быть включена в отчет об испытаниях и сертификат утверждения типа. Например, из нижеприведенного примера в отчет об испытаниях должна быть включена информация о названии, версии и контрольной сумме исполняемого файла.

Отчет испытаний № XYZ122344
Валидация программного обеспечения расходомера [обозначение типа] **модель** [обозначение]

Программное обеспечение средства измерений было валидировано, для подтверждения соответствия требованиям стандарта «Система обеспечения единства измерений Республики Беларусь. Общие требования к программно-управляемым средствам измерений».

Валидация проводилась в соответствии с указанным стандартом, в котором интерпретируются и объясняются требования, предъявляемые к ПО. Этот отчет описывает экспертизу программного обеспечения, которая должна быть проведена в целях оценки соответствия.

Изготовитель	Заявитель
[Название]	[Название]
[Адрес]	[Адрес]
[Контактное лицо]	[Контактное лицо]

Объект исследования

Расходомер [название типа] - средство измерений, предназначенное для измерения расхода жидкостей. Диапазон измерений: от 1 л/с до 2000 л/с. Основные функции:

– измерение расхода жидкостей,
– отображение измеренного объема,
– интерфейс с преобразователем.

Расходомер описан как средство измерений, разработанное для определенных целей (встроенная система), с долгосрочным хранением законодательно контролируемых данных.

Расходомер - независимый прибор, имеющий связь с преобразователем. Преобразователь осуществляет температурную компенсацию. Регулирование расхода можно осуществить с помощью параметров калибровки, хранимых в энергонезависимой памяти преобразователя. Память не может быть извлечена из преобразователя. Измеренный объем отображается на дисплее. Связь с другими устройствами не предусмотрена.

Встроенное ПО средства измерений было разработано фирмой [Название, Адрес]**.**

Исполняемый файл **“ tt100_12.exe”**.

Валидированная версия этого ПО - **V1.2c**. Версия ПО отображается на дисплее прибора при его включении и удержании кнопки «level» в течение 4 секунд.

Исходный код включает следующие законодательно контролируемые файлы:

-	main.c	12301 byte	23 Nov 2003
-	int.c	6509 byte	23 Nov 2003
-	filter.c	10897 byte	20 Oct 2003
-	input.c	2004 byte	20 Oct 2003
-	display.c	32000 byte	23 Nov 2003
-	Ethernet.c	23455 byte	15 June 2002
-	driver.c	11670 byte	15 June 2002
-	calculate.c	6788 byte	23 Nov 2003

Исполняемый файл "tt100_12.exe" защищен от модификации контрольной суммой. Значение контрольной суммы алгоритма XYZ - 1A2B3C.

При проведении валидации была представлена следующая документация изготовителя:

- Руководство по эксплуатации ТТ 100, Версия 1.6
- Руководство по техническому обслуживанию ТТ 100, Версия 1.1
- Описание ПО ТТ 100 (внутренний документ, датированный 22 ноября 2003)
- Электрическая схема ТТ 100 (№ 222-31, дата 15 октября 2003)

Окончательная версия объекта испытаний доставлена в Национальную лабораторию испытаний и измерений 25 ноября 2003.

Проведение валидации

Валидация была выполнена согласно стандарта «Система обеспечения единства измерений Республики Беларусь. Общие требования к программно-управляемым средствам измерений». Валидация проводилась в период с 1 ноября по 23 декабря 2003. Анализ проекта был проведен 3 декабря [Исполнитель] в главном офисе [Адрес]. Остальная работа по валидации была проведена в [Название организации, адрес] [Специалистами].

Следующие требования были валидированы:

- Идентификация ПО,
- Правильность алгоритмов и функций,
- Защита ПО,
- Предотвращение случайного неправильного использования,
- Защита от мошенничества,
- Поддержка функций аппаратных средств
- Хранение данных, передача через системы связи.

Следующие методы валидации были использованы:

- Анализ документации и валидации проекта,
- Валидация функциональным испытанием метрологических функциональных возможностей,
- Анализ кода,
- Испытание программного модуля calculate.c методом SDK XXX.

Результат:

При валидации на соответствие следующим требованиям не было обнаружено ошибок:
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.

Были найдены две команды, которые не были первоначально описаны в руководстве по эксплуатации. Две команды были включены в руководство по эксплуатации, датированное 10 декабря 2003.

Ошибка программного обеспечения по ограничению календаря до 28 февраля в високосном году была найдена в пакете программ V1.2b. Это было исправлено в версии V1.2c. Результат валидации распространяется только на испытанное изделие с серийным номером 1188093-B-2004.

Заключение:

ПО [Идентификация] соответствует требованиям стандарта «Система обеспечения единства измерений Республики Беларусь. Общие требования к программно-управляемым средствам измерений».

[Название организации,
проводившей испытания ПО]
[ФИО, должность]

Пример контрольного листа

Пункт	Требование	+	-	Примечание
5.1 **5.1.1**	**Основные требования** **Идентификация ПО** Законодательно контролируемое ПО должно быть четко идентифицировано			
5.1.2	**Правильность алгоритмов и функций** Измерительные алгоритмы и функции средств измерений должны быть корректными			
5.1.3 **5.1.3.1**	**Защита ПО** **Предотвращение случайного неправильного применения** Средство измерений, особенно ПО, должно быть разработано таким образом, чтобы возможность случайного или преднамеренного неправильного использования была минимальной.			
5.1.3.2 **a)** **b)** **c)** **d)**	**Защита от мошенничества** Законодательно контролируемое ПО должно быть защищено от недопустимой модификации, загрузки или изменения, посредством замены запоминающего устройства. Для защиты средства измерений со встроенной операционной системой или имеющей возможность обновления ПО дополнительно к механическому пломбированию могут потребоваться иные технические средства. Только четко документированные функции (см. 6.1) могут быть активированы через пользовательский интерфейс. Пользовательский интерфейс должен быть выполнен так, что бы не возникало возможности его мошеннического использования. Представление информации должно соответствовать п.5.2.2. Параметры, которые хранят законодательно контролируемые характеристики средства измерений должны быть защищены от неавторизированного изменения. При необходимости для целей верификации (поверки), текущая конфигурация параметров должна иметь возможность отображения или вывода на печать. Защита ПО включает соответствующую пломбировку механическими, электронными или криптографическими средствами, которые предотвращают или делают очевидным неавторизованный доступ.			
5.1.4 **5.1.4.1**	**Поддержка аппаратных средств** **Обнаружение ошибок** Изготовителем предусмотрено наличие технических решений контроля в ПО, в аппаратных средствах или наличие программно-технических средств, обеспечивающих соответствующее взаимодействие программного обеспечения и аппаратных средств.			
5.1.4.2	**Обеспечение надежности** Изготовитель может предусмотреть функцию обеспечения надежности, реализуемую ПО, аппаратными средствами или аппаратными средствами управляемыми ПО.			
5.2 **5.2.1**	**Специфические требования** **Определение и разделение контролируемых частей, и определение их интерфейсов** Метрологически критические части измерительной системы (программная или аппаратная часть) не должны подвергаться влиянию со стороны других частей измерительной системы			
5.2.1.1 **a)**	**Разделение устройств и функциональных блоков** Функциональные блоки или электронные устройства измерительной системы, которые выполняют законодательно контролируемые функции должны быть четко идентифицированы и документированы.			

Пункт	Требование	+	-	Примечание
b)	При проведении испытаний необходимо подтвердить, что законодательно контролируемые функции не подвержены недопустимому влиянию, посредством подачи команд через доступные интерфейсы.			
5.2.1.2	**Разделение ПО**			
a)	Требования соответствия применимы к законодательно контролируемой части ПО средства измерений (см. 5.2.5), которая должна иметь четкую идентификацию, как описано в п. 5.1.1.			
b)	Если законодательно контролируемая часть взаимодействует с другими частями, должен быть определен программный интерфейс. Обмен данными должен производиться исключительно через этот интерфейс. Законодательно контролируемые части ПО и интерфейса должны быть четко документированы.			
c)	Все законодательно контролируемые функции и области данных ПО должны быть описаны с тем, чтобы утверждающий орган мог дать заключение о корректном разделении ПО. Должно быть четкое и непротиворечивое назначение каждой команды для каждой активируемой функции или изменению данных в законодательно контролируемой части ПО. Команды, которые передаются через программный интерфейс должны полностью декларироваться разработчиком и документироваться. Только документированные команды могут быть активированы через программный интерфейс. Изготовитель должен подтвердить полноту документации по описанию команд.			
d)	В тех случаях, когда законодательно контролируемое ПО отделено от остального ПО, законодательно контролируемое ПО должно иметь приоритет на выполнение и использование ресурсов.			
5.2.2	**Совместное отображение** Должно быть четкое и однозначное разграничение Контролируемой и иной информации			
5.2.3 **5.2.3.1**	**Хранение данных, передача через системы связи** Хранимые или передаваемые измеренные значения должны сопровождаться соответствующей информацией, необходимой для их дальнейшего законодательно контролируемого применения.			
5.2.3.2	Данные должны быть защищены программными средствами для гарантии их идентичности, правильности информации о времени измерения, аутентичности, и целостности. ПО, которое отображает или обрабатывает данные измерений и сопутствующую информацию, должно проверять правильность времени измерений, аутентичность и целостность данных после их считывания из ненадежного хранилища или ненадежного канала связи. При обнаружении несоответствий данные должны быть отвергнуты или блокированы.			
5.2.3.3	Для высокого уровня защиты необходимо применять криптографические методы.			
5.2.3.4 **a)**	**Автоматическое хранение** По завершению измерения измеренные данные должны автоматически сохраняться. Устройство, используемое для долгосрочного хранения данных, должно быть достаточно надежным для предотвращения порчи данных и иметь емкость, которой будет достаточно для выполняемой задачи. Если окончательный результат измерений используемый для законодательно контролируемых целей получен вычислением вместе с ним должны сохраняться исходные данные расчетов.			

Пункт	Требование	+	-	Примечание
b)	Хранимые данные могут быть удалены в случае: – сделка завершена; – данные выведены на печать с использованием печатающего устройства, являющегося объектом законодательного контроля (КСА).			
c)	При выполнении требований п. 5.2.3.4.b и переполнении памяти разрешается удалять данные из памяти при выполнении следующего: – данные удаляются в порядке их записи в память и правилами, установленными для конкретной измерительной задачи, – удаление проводится автоматически или после специальной операции, выполненной вручную			
5.2.3.5	**Задержка передачи** Задержка передачи данных никоим образом не должна влиять на измерение.			
5.2.3.6	**Прерывание передачи** Если сетевые службы становятся недоступными, результаты измерений не должны быть потеряны. Измерения должны быть прекращены во избежание потери данных измерений.			
5.2.3.7	**Временной штамп** Временной штамп должен считываться из часов средства измерений. Соответствующие защитные меры должны быть использованы в зависимости от уровня жесткости (риска) (см. 5.1.3.2.c). Если информация о времени важна, то надежность встроенных часов средства измерений должна гарантироваться дополнительными техническими решениями.			
5.2.4 **5.2.4.1**	**Совместимость операционных систем и аппаратных средств, транспортабельность** Разработчик должен идентифицировать приемлемые программные и аппаратные средства. Изготовитель должен декларировать минимальные ресурсы и стандартную конфигурацию, необходимую для правильного функционирования ПО.			
5.2.4.2	Необходимо наличие технических решений, предотвращающих функционирование ПО при невыполнении требований к минимальной конфигурации.			
5.2.6 **5.2.6.1**	**Техническое обслуживание и изменение конфигурации** Только утвержденные версии законодательно контролируемого ПО допускаются к применению			
5.2.6.2	**Верифицированное обновление** После обновления законодательно контролируемого ПО средства измерений необходимо провести верификацию и обновить средства защиты			
5.2.6.3 **a)**	**Прослеживаемое обновление** Прослеживаемое обновление ПО должно быть автоматическим. По завершении процедуры обновления ПО условия защиты ПО должны оставаться на том же уровне, который был зафиксирован при утверждении типа.			
b)	Отдельно взятое средство измерений должно иметь фиксированное законодательно контролируемое ПО.			
c)	Должны быть использованы технические решения для гарантии аутентичности загружаемого ПО. Если загруженное ПО не проходит проверку по аутентичности, средство измерений не должно его устанавливать и вернуться к использованию предыдущей версии или перейти в нерабочий режим.			
d)	Должны быть использованы технические решения для обеспечения целостности загруженного ПО, т.е. проверка его неизменности перед загрузкой.			

Пункт	Требование	+	-	Примечание
e)	Должны быть использованы технические решения позволяющие сделать заключение о прослеживаемости обновления в пределах средства измерений.			
f)	Средство измерений должно иметь функциональный блок или электронное устройство, которое позволяет пользователю\владельцу дать свое согласие на установку обновления. Должно быть возможным отключить/включить данный функциональный блок или устройство, например, с помощью пломбируемого переключателя или программного параметра. При активизации данного функционального блока или электронного устройства каждая загрузка обновления должна инициироваться пользователем или владельцем средства измерений. В выключенном состоянии от пользователя или владельца не требуется каких либо действий на обновление ПО.			
g)	Если требования с 5.2.6.3.a по 5.2.6.3.e не могут быть выполнены, возможно обновить только законодательно неконтролируемую часть ПО. В данном случае должно выполняться следующее: – имеется четкое разделение между законодательно контролируемым и неконтролируемым ПО в соответствии с 5.2.1; – вся законодательная контролируемая часть программного обеспечения не может быть обновлена без нарушения пломбировки; – в сертификате утверждения типа указано, что законодательно неконтролируемая часть может быть обновлена.			
5.2.6.4	Средство измерений должно иметь устройства для автоматической и невытираемой записи об изменениях устройство-определяющих параметров, например, протокол аудита. Средство измерений должно иметь возможность отображения записанных данных.			
5.2.6.5	Средства обеспечения прослеживаемости и записи являются частью законодательно контролируемого ПО и должны защищаться соответствующим образом.			

Приложение С
(справочное)
Перечень терминов

Директор БелГИМ	Н.А. Жагора
Заместитель директора БелГИМ	Т.А. Коломиец
Начальник НИО ЗТМ, НТП БелГИМ	М.В. Шабанов