	Рекомендация КООМЕТ	
	Программное обеспечение средств измерений. Общие технические требования	**COOMET R/LM/10:2004**
Утверждена на 14 заседании Комитета КООМЕТ (Албена, Болгария, 27 – 28 мая 2004 г.)		

СОДЕРЖАНИЕ

1 Область применения

Настоящая рекомендация* устанавливает минимально необходимые требования к программному обеспечению с измерительными функциями, используемому в области законодательной метрологии, а также критерии, определяющие объем испытаний программного обеспечения в целях его утверждения. Минимально необходимые требования не ограничивают разработчика программного обеспечения в применении новых технических решений и совершенствовании уже имеющихся разработок.

Настоящая рекомендация обязателен для применения разработчиками средств измерений с программным обеспечением и специализированного программного обеспечения, используемого в области законодательной метрологии, для обеспечения единства измерений на этапе изготовления средств измерений и организациями, проводящими испытания средств измерений с целью гармонизации требований к программному обеспечению на этапе внесения их в Национальный реестр средств измерений.

Испытания программного обеспечения для средств измерений выполняют организации, уполномоченные Национальным органом по метрологии на проведение испытаний с целью утверждения типа средств измерений. Для выполнения работ по исследованию алгоритмов и исходных кодов программ могут привлекаться аккредитованные испытательные лаборатории и сотрудники организаций, специализирующихся на разработке программного обеспечения.

* - Рекомендация разработана с учетом требований, изложенных в Руководстве WELMEC 7.1

Испытания по утверждения программного обеспечения могут совмещаться с испытаниями по утверждению типа.

Специальные требования к программному обеспечению отдельных категорий средств измерений могут устанавливаться в нормативных документах на данную категорию средств измерений.

2 Определения

В настоящей рекомендации применяют следующие термины с соответствующими определениями:

2.1 Законодательно контролируемое программное обеспечение - программное обеспечение, которое реализует функции или свойства законодательно контролируемого средства измерений. Законодательно контролируемое программное обеспечение включает части программы и данные, которые формируют программное обеспечение, подлежащее контролю со стороны законодательной метрологии. Программное обеспечение может быть представлено отдельной программой или пакетом программ.

Законодательно контролируемая часть программы - часть программы, которая выполняет функции, подлежащие контролю со стороны законодательной метрологии.

Законодательно контролируемые данные – данные, которые могут быть выделены в следующие типы параметров и данных:

- типоопределяющие параметры, которые зависят только от типа средства измерений. Типоопределяющие параметры устанавливаются при утверждении типа средства измерений;

- конструктивные параметры – параметры конфигурации и настройки средства измерений, содержащиеся в программном обеспечении и определяемые программно вводимыми данными (например, чувствительность, диапазон измерения, цена деления шкалы, единица измерения и т.д.). Конструктивные параметры могут быть установлены или изменены пользователем.

Законодательно-контролируемые функции программного обеспечения – операции, выполняемые программным обеспечением по обработке, передаче и хранению законодательно-контролируемых данных.

Испытание программного обеспечения – процедура установления компетентным органом правильности и однозначности законодательно контролируемых функций программного обеспечения и генерируемых им данных.

Метрологическое программное обеспечение – программное обеспечение, разработанное для выполнения метрологических функций как в составе средства измерений, так и отдельно от него в составе программных измерительных комплексов.

Переменные значения - обрабатываемые результаты измерений, которые находятся под управлением законодательно контролируемых частей программы (т.е. это элементы домена данных отдельной части программы), и конечные результаты измерений, к которым имеется свободный доступ из любого другого программного обеспечения. Кроме этого, имеются вспомогательные переменные, которые, например, содержат команды для управления функциями и потоком данных законодательно контролируемых частей программы (такие функции отслеживаются, например, счетчиками событий).

Регистрация программного обеспечения - процедура учета законодательно контролируемого программного обеспечения с присвоением ему уникального регистрационного номера и внесения в Национальный реестр средств измерений.

Утверждение программного обеспечения – процедура, проводимая Национальным метрологическим институтом в целях регистрации и официального подтверждения пригодности программного обеспечения для использования в области законодательной метрологии.

2.2 Защита данных

Аутентифицированное программное обеспечение - программный код, к которому у пользователя и заказчика (участвуют обе стороны) имеется доверие как к коду идентичному утвержденному. Аутентифицированная программа поставляется авторизованным субъектом, несущим ответственность за соответствие кода исходному (т.е. утвержденному) или ее соответствие утвержденному (законодательно) коду.

Аутентифицированные данные - передаваемые данные в сложной измерительной системе, происхождение которых может быть проверено получателем или, в случае хранения результатов измерения в памяти с общим доступом для последующего использования, данные, которые могут быть однозначно приписаны определенному измерению.

Метод аутентификации - метод, позволяющий каждому участнику проверить аутентичность (подлинность) программы или данных.

Пример - Генерирование электронной цифровой подписи для определенных данных или файлов с помощью аутентифицированной программы перед записью (хранением) или передачей. При получении или чтении: повторное вычисление электронной цифровой подписи и сравнение результата с номинальным значением, используя аутентифицированную программу одним из участников.

Контрольная сумма - логическая сумма всех байтов программного кода или набора данных. Чтобы получить результат с фиксированным числом цифр часто используется суммирование по модулю.

Контрольная сумма часто используется как простой хэш-код. Хэш-код является результатом арифметической комбинации всех байтов программного кода или набора данных. Результат алгоритма хэширования включает только некоторые байты, а алгоритм такой, что любая модификация кода программы или данных с высокой вероятностью приводит к другому результату.

Идентификация программы – определение объекта в ряду подобных с помощью имен и реквизитов.

Имитоприставка – криптографическая контрольная сумма информации, вычисляемая с использованием ключа шифрования.

Законодательно контролируемая идентификация программы – идентификация программы, которая приписывается законодательно контролируемому программному обеспечению.

Одним из приемлемых технических решений для законодательно контролируемой программной идентификации является метод, с помощью которого программе присваивается код, состоящий из трех частей: A, B и C.

Часть А - код, установленный изготовителем средства измерений. Эта часть учитывает каждое законодательно контролируемое изменение в программном обеспечении.

Часть В – код, формируемый по специальному алгоритму, который является частью законодательно контролируемого программного обеспечения, формирующего номер, который автоматически изменяется при изменении конструктивных параметров средства измерений.

Идентификация может содержать часть, которая рассчитывается по исполняемому коду законодательно утвержденного программного обеспечения.

Ключ шифрования – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования, обеспечивающее выбор одного преобразования из совокупности возможных для данного алгоритма преобразований.

Электронная цифровая подпись – набор символов, вырабатываемый средствами электронной цифровой подписи и ассоциированный со специальной (особенной) частью документа, кото-

рый обеспечивает однозначную идентификацию создателя и неоспоримость происхождения содержательной (общей) части документа.

Электронная цифровая подпись для файла (кода программы или данных) генерируется в два этапа: сначала рассчитывается хэш-код и затем хэш-код шифруется.

Электронная цифровая подпись обычно добавляется к коду программы или набору данных, по которым она была сгенерирована.

Целостность программы – состояние программного обеспечения, идентичного образцовой версии (например, утвержденной), характеризующееся отсутствием изменений преднамеренного или случайного характера.

2.3 Защита программного обеспечения

2.3.1 Защищенное программное обеспечение - программное обеспечение, представленное программным кодом и данными, изменение которых невозможно или обнаруживается и становится очевидным с использованием встроенных программных функций или внешней защиты, например, в виде контрольных тестов, ограничения доступа или механического опечатывания.

2.3.2 Контрольный тест - программный счетчик и/или информационная запись изменений конструктивных параметров. Контрольный тест может быть реализован, например, как "счетчик событий" или как "журнал событий":

Счетчик событий - необнуляемый счетчик, который включается каждый раз при включении специального рабочего режима средства измерений или при внесении одного или нескольких изменений конструктивных параметров или других законодательно контролируемых данных.

Журнал событий - файл, содержащий ряд записей, каждая из которых содержит данные, описывающие вид и время возникновения события. Например, изменение конструктивного параметра, с обязательной идентификацией времени и даты, когда параметр был изменен и новым значением параметра. Части программы, которые реализуют регистрацию события, и файлы, которые содержат информацию о событии, расцениваются как законодательно контролируемые и должны быть соответствующим образом защищены.

2.4 Изменения программного обеспечения

2.4.1 Неумышленные изменения - изменения частей программы или данных, подлежащих контролю со стороны законодательной метрологии, которые возникают вследствие случайных физических или программных эффектов (сбои, присутствие программ-вирусов) или которые неумышленно выполняются пользователем средства измерений.

2.4.2 Намеренные изменения с использованием простых общедоступных программных средств – изменения частей программы или данных, вносимые с использованием программных средств, доступных широкой публике. Например, все виды текстовых редакторов расцениваются как простые общедоступные программные средства, в то время как, например, отладчики или дисковые редакторы не являются таковыми.

2.4.3 Намеренные изменения с использованием специальных программных средств - изменения частей программы или данных, вносимые с использованием программных средств, не доступных широкой публике и требующие специальных знаний. Все виды отладчиков, дисковых редакторов или программного обеспечения, служащего для разработки программных средств, расцениваются как сложные программные средства.

2.5 Интерфейсы

2.5.1 Аппаратный интерфейс - электрический вход и/или выход устройства для обмена данными с другими устройствами. Ими могут быть средства измерений, модули средства измерений или периферийные устройства.

Термин "интерфейс" относится ко всем механическим, электрическим и логическим характеристикам в точке обмена данными и к таким понятиям как передаваемые данные и команды.

2.5.2 Защищенный интерфейс

Интерфейс является защищенным если:

а) только определенный набор параметров, данных и функций законодательно контролируемой программной части может быть изменен или пропущен через этот интерфейс;

б) невозможно ввести в средство измерений(или модуль средства измерений) команды или данные, предназначенные или подходящие для:

- отображения данных, которые ясно не определены и могут быть приняты за результат измерения;

- фальсификации отображаемых, обработанных или сохраненных результатов измерения или других законодательно контролируемых данных (например, в случае прямых продаж населению, цена за единицу, отпускная стоимость, единица величин);

- неавторизированной корректировки или изменения настроек средства измерений, или неавторизованного изменения любых типоопределяющих параметров или конструктивных параметров;

- порчи законодательно контролируемого программного кода программного обеспечения средства измерений.

2.5.3 Программный интерфейс

Программный интерфейс – совокупность переменных и организация исходного кода, с помощью которых реализуется обмен данными между функциональными частями программного обеспечения.

Если помимо законодательно контролируемых частей программного обеспечения существуют другие неконтролируемые части, то они должны быть разделены с законодательно контролируемыми частями и связаны между собой через программный интерфейс. Переменные интерфейса могут быть реализованы, например, как глобальные переменные программы, как функциональные параметры или как файлы данных.

2.5.4 Защищенный программный интерфейс - программный интерфейс между законодательно контролируемой программной частью и другими программными частями является защищенным при следующих условиях:

а) если только определенный набор позволенных данных законодательно контролируемой программной части может быть изменен или пропущен через этот интерфейс;

б) если обе части обмениваются информацией только через этот интерфейс, т.е. исключая любой другой канал связи.

Переменные и программный код защищенного программного интерфейса является частью законодательно контролируемого программного обеспечения.

2.6 Код программы

Исходный код - код программы, выполненный в читаемой для человека форме, в общем случае при помощи текстового редактора.

Исполняемый код - последовательность двоичных чисел, которые считываются и интерпретируется центральным процессором. Данный код понятен для человека, только если он использует инструментальные средства подобно отладчикам, деассемблерам или декомпиляторам. Текстовый редактор не может быть использован для этой цели.

3 ОСНОВНЫЕ ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

3.1 Проект и структура программного обеспечения

3.1.1 Программное обеспечение средства измерений должно быть разработано так, чтобы можно было провести оценку соответствия его законодательно контролируемых функций требованиям настоящей рекомендации.

3.1.2 Законодательно контролируемое программное обеспечение должно быть разработано таким образом, чтобы**, чтобы его законодательно контролируемые функции** не были подвержены влиянию другого программного обеспечения, параллельно работающего или обеспечивающего его функционирование.

3.1.3 Законодательно контролируемое программное обеспечение должно иметь функции защиты от несанкционированного воздействия на это программное обеспечение через его интерфейсы или интерфейсы средства измерений.

3.2 Защита программного обеспечения

3.2.1 Законодательно контролируемые программы и данные должны быть защищены от искажений и неумышленных изменений.

3.2.2 Законодательно контролируемые программы и данные должны быть защищены от намеренных изменений.

3.2.3 Только аутентифицированное программное обеспечение можно использовать для законодательно контролируемых целей. Факт использования результатов, полученных с использованием законодательно контролируемой программы, должен быть очевиден и однозначен.

3.2.4 Функциональные дефекты аппаратной части средства измерения с интегрированным программным обеспечением или аппаратной части программно-измерительных комплексов, которые могут исказить результаты измерений, должны автоматически обнаруживаться. При обнаружении данные дефекты должны быть устранены или однозначно обозначены.

3.2.5. В программно управляемых аппаратных средствах измерений должна быть обеспечена целостность законодательно контролируемого программного обеспечения и должны быть реализованы методы автоматического контроля целостности такого программного обеспечения.

3.3 Соответствие программного обеспечения утвержденному

3.3.1 После утверждения, законодательно контролируемое программное обеспечение не должно изменяться без уведомления органа, проводившего его утверждение.

3.3.2 Программное обеспечение должно иметь законодательно контролируемую идентификацию.

Алгоритм идентификации должен быть частью самой программы.

Идентификация должна осуществляться во время запуска программного обеспечения или по команде пользователя.

3.4 Готовность к испытаниям

Законодательно-контролируемые функции программного обеспечения должны быть неизменны и проверяемы.

3.5 Документация, требуемая для утверждения программного обеспечения

Законодательно контролируемое программное обеспечение, включая его аппаратную и программную среду, должно документироваться.

Документация программного обеспечения средства измерения должна включать:

а) описание законодательно-контролируемые функции программного обеспечения;

б) описание типоопределяющих и конструктивных параметров;

в) описание реализованных в программном обеспечении расчетных алгоритмов;

г) характеристики точности расчетных алгоритмов (например, округляющие алгоритмы);

д) описание методики идентификации программного обеспечения;

е) характеристики системных аппаратных средств, если эта информация не приведена в руководстве пользователя;

ж) руководство пользователя.

4 Критерии испытаний

Устанавливаются три критерия испытаний:

а) уровень защиты программного обеспечения;

б) жесткость испытаний программного обеспечения;

в) степень соответствия программного обеспечения;

и три характеристики для каждого критерия:

- низкий уровень защиты, средний уровень защиты, высокий уровень защиты;

- низкая жесткость испытаний, средняя жесткость испытаний, высокая жесткость испытаний;

- низкая степень соответствия, средняя степень соответствия, высокая степень соответствия.

При установлении критериев должны учитываться технические особенности средств измерений, ввиду чего требования к программному обеспечению могут устанавливаться в разном объеме.

Испытания программного обеспечения проводятся по согласованной с разработчиком и заказчиком программе испытаний.

4.1 Уровень защиты программного обеспечения

Защита программного обеспечения означает принятие адекватных мер, направленных на предотвращение неумышленных или намеренных его изменений. Уровень защиты программного обеспечения оказывает влияние на принимаемое техническое решение конструкции средства измерений и поэтому, должен учитываться, главным образом, изготовителем и/или разработчиком программного обеспечения.

Характеристики уровней защиты:

- низкий: программное обеспечение не имеет защиты от неумышленных или намеренных изменений;

- средний: законодательно контролируемое программное обеспечение защищено от неумышленных и намеренных изменений с использованием простых общедоступных программных средств;

- высокий: законодательно контролируемое программное обеспечение защищено от неумышленных и намеренных изменений с использованием специальных, сложных программных средств. Уровень защиты соответствует последним достижениям в области защиты данных (например, в области банковских технологий).

Изготовитель может подтвердить соответствие программного обеспечения требованиям более высокого уровня защиты, чем тот, который назначен.

Общепринятый метод защиты с помощью клейм и пломбировки, обеспечивающий очевидность преднамеренного вмешательства, эквивалентен программным средствам защиты для среднего и высокого уровней защиты для обособленных средств измерений целевого назначения.

4.2 Жесткость испытаний программного обеспечения

Жесткость испытаний программного обеспечения устанавливается в целях утверждения программного обеспечения.

Характеристики жесткости испытаний:

Низкая: функции программного обеспечения проверяются в соответствии с программой испытаний. Документация, относящаяся к законодательно контролируемым частям и функциям программного обеспечения, предоставляется изготовителем и необходима, главным образом, для понимания операций по использованию средством измерений и его испытаниям. Главный упор делается на результаты испытаний по определению метрологических характеристик и результаты испытаний, подтверждающие корректность информации эксплуатационных документов.

По некоторым техническим характеристикам, которые не охвачены испытаниями по определению метрологических характеристик (например, защищенность интерфейсов) допускается принимать декларацию изготовителя о том, что программное обеспечение полностью соответствует предоставленной документации и не располагает какими-либо функциями, отличными от заявленных.

Изготовитель должен предоставить эксплуатационные документы и техническую документацию без специальной программной документации.

Средняя: в дополнение к испытаниям утверждения типа программное обеспечение испытывается на основании описания программных функций, предоставленных изготовителем. Проверяется целостность и однозначность документированных функций. Документация, представленная на испытания, должна включать описание программного обеспечения, алгоритма программы, используемых методов статистической обработки, формул, законов и др.

Для средств измерений на базе электронных вычислительных машин или открытых измерительных систем с возможным доступом пользователя проводятся практические испытания программы для удостоверения в том, что все меры защиты эффективны, команды работают в соответствии с документацией и правильно идентифицируется законодательно контролируемое программное обеспечение.

Высокая: в дополнение к испытаниям по определению метрологических характеристик и испытаний на правильность выполняемых функций, проверяется правильность исходного кода законодательно контролируемого программного обеспечения. Предметом испытаний исходного кода программы могут быть, например, реализация алгоритма вычислений, фильтрация данных, вводящихся через интерфейс программы, или насколько правильно выполнено разделение программы на законодательно контролируемые и неконтролируемые части.

4.3 Степень соответствия программного обеспечения

Программное обеспечение, находящееся в эксплуатации и проверяемое при метрологическом надзоре и контроле должно соответствовать программному обеспечению, которое проходило процедуру утверждения, в зависимости от выбранной характеристики степени соответствия.

При контроле соответствие утвержденному программному обеспечению проверяется по законодательно контролируемой идентификации программы, которая приводится в описании утвержденного программного обеспечения или описании типа средства измерений.

Характеристики степени соответствия:

Низкая: программное обеспечение не имеет идентификации или алгоритм идентификации не является частью программы, представленной на утверждение.

Изменение утвержденной законодательно контролируемой части программного обеспечения автоматически не приводит к формированию его новой идентификации.

Документация, требуемая для утверждения программного обеспечения, представлена не в полном объеме.

Средняя: любое изменение утвержденной законодательно контролируемой части программного обеспечения автоматически приводит к формированию его новой идентификации. В этом случае проводятся дополнительные работы по утверждению программного обеспечения.

Внесение изменений в законодательно контролируемое программное обеспечение допускаются до того момента, пока документированные функции и характеристики программного обеспечения или управляемого им средства измерений остаются неизменными.

При внесении изменений в документированные функции и характеристики законодательно контролируемого программного обеспечения требуется дополнительное утверждение и новая идентификация программного обеспечения.

Изменение частей программы, неконтролируемых со стороны законодательной метрологии, можно проводить без уведомления организации, проводившей утверждение, до того момента, пока соблюдается разделение частей программы и используется только утвержденный программный интерфейс.

Программная документация, представленная на испытания, и копия программы в скомпилированном виде хранятся в организации, проводившей испытания.

Высокая: все программное обеспечение идентично утвержденному программному обеспечению.

Ввиду обеспечения полной идентичности, изменение любой части программного обеспечения автоматически приводит к новой законодательно контролируемой идентификации программы. В этом случае проводится дополнительное утверждение.

При поверке соответствие утвержденному программному обеспечению проверяется по программной идентификации, которая приводится в описании типа на средство измерений.

Программная документация, представленная на испытания, и копия программы в скомпилированном виде хранятся в организации, проводившей испытания.

Приложение А

(рекомендуемое)

Предложения по назначению критериев испытаний программного обеспечения

Таблица А.1

Область применения	Группа	Уровень защиты ПО	Жесткость испытаний	Уровень соответствия ПО
Поставка потребителю по централям	1	средний	средняя	средний
		высокий	средняя	высокий
Коммерческие поставки / услуги	2	средний	средняя	средний
		высокий	средняя	высокий
Визуальные измерения	3	средний	высокая	высокий
Защита окружающей среды, безопасность труда, здравоохранение	4	средний	высокая	средний
				высокий