681.2.082/.083

Структура и особенности Руководства WELMEC 7.2

Ю. А. КУДЕЯРОВ, А. Н. ПАНЬКОВ

Всероссийский научно-исследовательский институт метрологической службы,

e-mail: gamelab@vniims.ru

Рассмотрены структура и особенности Руководства WELMEC 7.2, относящегося к программному обеспечению средств измерений. Приведен пример конкретных требований к таким программным продуктам.

Ключевые слова: программное обеспечение, средства измерений, юридически значимое программное обеспечение, идентификация, алгоритмы, электронная подпись.

The structure and main points of Guidance WELMEC 7.2 for software of measuring instruments are considered. Examples of certain requirements for such software are shown.

Key words: software, measuring instruments, legally relevant software, identification, algorithms, electronic signature, certificate system.

Руководство [1], о котором идет речь, основано на «Требованиях к программному обеспечению и руководстве по подтверждению», разработанных и представленных Европейской сетью развития «Measuring Instruments Directive – Software» (MID-Software). Напомним, что WELMEC – Европейская организация по сотрудничеству в области законодательной метрологии – региональная организация, объединяющая промышленно развитые страны Западной Европы.

Этому Руководству предшествовало Руководство [2], разработанное рабочей группой 7 WELMEC. Оба Руководства основаны на одинаковых принципах и были производными от требований Директивы по измерительным приборам 2004/22/EC (MID). Руководство [2] было апробировано и вышло в виде Издания 2, но носило, в основном,

информационный характер. Тем не менее, оно сыграло определенную роль в разработке и создании некоторых отечественных нормативных документов в этой области.

В Руководстве [2] акцентировано внимание на том, что нормирования только метрологических характеристик средств измерений (СИ) без должного внимания к программному обеспечению (ПО), используемому в них, в настоящее время совершенно недостаточно, так как для большинства современных приборов, управляемых микропроцессорами, или приборов на базе персональных компьютеров программное обеспечение и его целостность являются существенными факторами, определяющими метрологические свойства и надежность таких приборов. Это Руководство охватывало различные категории измерительных приборов и систем и было также разработано на основе MID, содержащей требования, предъявляемые к измерительным приборам, используемым в области, регулируемой законодательной метрологией. Некоторые из этих требований могут быть напрямую применены к ПО, используемому в этих приборах, другие необходимые требования могут быть применены как к аппаратным средствам, так и к ПО измерительного прибора.

В [2] вводилось понятие критичности ПО как показателя степени его влияния на метрологические характеристики СИ. Кроме того, в нем впервые была сформулирована идея разделения ПО на части, подлежащие и не подлежащие метрологическому контролю, так как оно постоянно совершенствуется. При модификациях программного продукта следует контролировать только его метрологически значимую часть.

Что касается Руководства [1], то оно является логическим развитием Руководства [2] и рекомендуется WELMEC для использования при разработке, проверке и утверждении ПО, контролирующего СИ, подпадающие под действие MID. Оно также является чисто рекомендательным и не налагает каких-либо ограничений или дополнительных технических требований сверх тех, которые содержатся в

MID. Альтернативные методы могут рассматриваться, но рекомендации, приведенные в этом документе, представляют точку зрения WELMEC, основанную на наилучших результатах использования. Хотя Руководство [1] ориентировано на СИ, включенные как объекты регулирования в MID, его рекомендации носят общий характер и могут быть применимы и к другим средствам измерений.

В [1] даны пояснения специфических терминов и определений, используемых в области информационных технологий и не очень хорошо известных специалистам, занимающимся традиционной метрологической деятельностью. Значительное внимание при этом уделено пояснению терминов, применяемых при защите измерительной информации (алгоритмы хэширования, электронные подписи и т. п.).

Руководство организовано как структурированный набор блоков требований. Из его общей структуры следуют классификации СИ на основе базовых конфигураций и так называемых информационно-технологических (ИТ) конфигураций. Руководство рассматривает две основные базовые конфигурации СИ: предназначенных для решения частных измерительных задач (тип *P*) и основанных на использовании персональных компьютеров (тип *D*). Иногда СИ первого типа называют средствами измерений со встроенным ПО. Набор требований дополняют специальные требования к СИ, следовательно, имеется три типа требований:

1) для двух основных конфигураций СИ;
2) для четырех ИТ-конфигураций (Приложения *L, T, S* и *D*),
3) специальные (Приложения I.1, I.2 и т. д.).

Первый тип требований применим ко всем СИ, второй – имеет отношение к следующим функциям, предусмотренным информационными технологиями: долговременному сохранению данных измерений (*L*), передаче этих данных (*T*), программной загрузке (*D*) и программному разделению (*S*). Каждый набор требований используют только в том случае, когда соответствующая функция существует. Последний тип –

дополнительные специальные требования к СИ. Нумерация следует за нумерацией дополнений в MID, относящихся к специальным требованиям.

В дополнение к описанной структуре, требования [1] различаются в соответствии с классами риска. Вводятся шесть классов, обозначаемых буквами от *A* до *F* в направлении повышения риска. Низший класс риска *A* и высший класс *F* не рассматриваются. Их вводят для возможного случая в будущем, когда они могут понадобиться. Остальные классы риска от *B* до *E* перекрывают все классы СИ, попадающие под регулирование MID. Более того, они обеспечивают достаточное поле возможностей в случае изменения оценок риска. Классы риска определены в главе 11 этого руководства, которая носит информационный характер. Для каждого СИ должна быть проведена оценка класса риска, так как конкретные требования к ПО определяются, прежде всего, классом риска, присущим прибору. На схеме (см. рисунок) показано, какие наборы требований существуют.

Каждый блок содержит отчетливо выраженное требование. Он состоит из текста, поясняющего определения и разъясняющего специальные примечания из предусмотренной документации, руководства по подтверждению и примеров приемлемых решений (если они имеются). Содержимое блока требований может подразделяться в соответствии с классами риска. Структура блока требований схематически представлена в таблице.

Структура блока требований

Название требования		
Главное содержание требования (возможно различающееся в соответствии с классами риска)		
Специальные примечания (область применения, дополнительные пояснения, исключительные случаи и т.п.)		
Предусмотренная документация (возможно различающаяся в соответствии с классами риска)		
Руководство по подтверждению для одного класса риска	**Руководство по подтверждению** для другого класса риска	**…**
Пример приемлемых решений для одного класса риска	**Пример приемлемых решен**ий для другого класса риска	**…**

Блок содержит технические требования, включая руководство по подтверждению, адресован как изготовителю, так и уполномоченным органам (организациям) с двумя целями: рассматривать это требование как минимальное условие и не налагать каких-то дополнительных требований.

Под уполномоченными органами (организациями) (notified bodies (NB)) понимаются органы (организации), уполномоченные (аккредитованные) в установленном порядке для проведения работ по испытаниям СИ с целью утверждения типа, по их поверке и калибровке и (или) подтверждению их соответствия (сертификации). Как известно, в Российской Федерации уполномоченными органами (организациями) являются органы государственной метрологической службы, в том числе государственные центры испытаний средств измерений, метрологические службы юридических лиц, аккредитованные на право их поверки и калибровки, а также органы обязательной и (или) добровольной сертификации соответствующих продукции и услуг.

Приведем пример конкретных требований, относящихся к основным конфигурациям СИ. Например, общие требования к идентификации встроенного ПО для риска классов *B, C* и *D* формулируются в следующем виде:

Идентификация программного обеспечения

Юридически значимое программное обеспечение должно быть четко и однозначно идентифицируемо. Идентификация должна быть привязана к самой программе и представлена либо в виде команды, либо проявляться в течение действия программы.

Специальные примечания

для риска класса B

- Изменения метрологически значимого ПО требуют информирования об этом уполномоченного органа (УО), который решает, необходима ли идентификация нового ПО или нет. Такая идентификация требуется только тогда, когда изменения ПО приводят к изменению уже утвержденных функций или характеристик;

для рисков классов C* и *D

- Каждое изменение юридически значимого ПО, зафиксированного при утверждения типа, требует новой программной идентификации;

для рисков всех классов (B, C* и *D)

- Программная идентификация должна иметь структуру, ясно идентифицирующую версии, которые необходимы при утверждения типа, а также версии, которые не нужны при таком утверждении.
- Если функции ПО могут переключаться при измерении типа СИ, то каждая функция или вариант могут идентифицироваться отдельно или, как альтернатива, весь программный пакет может быть идентифицирован целиком и т. д.

Из всего блока требований наибольший интерес представляет пример приемлемого решения.

Пример приемлемого решения

для всех классов риска

- Идентификация юридически значимого ПО содержит две части. В первой части *A* происходит изменение идентификации, если измененное ПО требует нового утверждения. Часть *B* показывает только незначительные изменения, которые не требуют нового утверждения.
- Идентификация генерируется и показывается по команде.

для риска класса B

- Часть *A* идентификации состоит из номера версии или номера TAC (Type Approval Certificate – Сертификат об утверждении типа).

для рисков классов C и D

- Часть *A* идентификации состоит из автоматически генерированной контрольной суммы, полученной на основе юридически значимого ПО, которое объявляется неизменным при утверждении типа. Для другой части такого ПО часть *A* состоит из номера версии или номера TAC.
- Примером приемлемого решения для получения контрольной суммы является алгоритм электронной подписи (the CRC-16 algorithm).

Требования к идентификации ПО содержат также требования для риска класса *E*.

Требования к документации (в дополнение к требованиям к документации для риска классов *B* и *C*)

- Исходный код, содержащий генерацию идентификации.

Руководство по подтверждению (в дополнение к руководству для риска классов *B* и *C*)

Проверки, основанные на анализе исходного кода:

- Проверяют, вся ли соответствующая программная часть охвачена алгоритмом генерации идентификации, и корректность исполнения алгоритма.

Необходимо обратить внимание на следующие обстоятельства:

1. В требованиях использован термин «юридически значимое программное обеспечение». Под «законодательно контролируемым (юридически значимым) программным обеспечением (параметром, характеристикой)» понимается та часть ПО (параметр, характеристика), которая может оказывать влияние на метрологические характеристики СИ. К таким частям относятся, как правило, модули ПО, ответственные за сбор измерительной информации, ее передачу, обработку, хранение и представление. Это как раз та часть, о которой говорилось при обсуждении разделения ПО.

2. В тексте требований присутствуют понятия, относящиеся к криптографическим методам защиты (контрольная сумма, алгоритм электронной подписи CRC-16, номер TAC и т. п.). Некоторые из этих терминов, поясняются в [1], некоторые, к сожалению, остаются понятными только узкому кругу специалистов по криптографическим методам защиты информации.

3. Основную ценность, прежде всего для разработчиков ПО, представляют содержащиеся в каждом блоке примеры приемлемых решений для удовлетворения конкретных требований к нему.

4. Дополнения для риска класса *E* содержат требования к исходному коду программы. Этот момент в нормативных документах по метрологии встречается впервые. До сих пор под предлогом сохранения авторских прав этот вопрос оставался за пределами рассмотрения. Как показывает практика тестирования ряда программных продуктов, в ряде случаев делать какие-то определенные заключения о качестве ПО можно только на основе анализа исходного кода или его фрагментов. Разумеется, это делается только с согласия разработчиков ПО, при этом в необходимых

случаях заключается дополнительное соглашение о соблюдении конфиденциальности при его тестировании.

Аналогичную структуру имеют блоки и по остальным аспектам требований к ПО, о которых говорилось выше.

Важная роль в Руководстве [1] отведена проблеме определения классов рисков, возникающих при использовании ПО. Так, согласно решению Рабочей группы 11 WELMEC (2-е заседание, 3 - 4 марта 2005 г.), для счетчиков количества теплоты, контролируемых ПО в соответствии с требованиями настоящего Руководства, устанавливается риск класса *C* для СИ типа *P*.

Из содержания Руководства [1] следует, что в промышленно развитых странах Западной Европы проблеме оценки качества программного обеспечения, используемого в средствах измерений, придается первостепенное значение. Разработчики и пользователи автоматизированных СИ должны быть уверены, что использование ПО сопровождается минимальным риском, что должно быть документально подтверждено независимым аудитом.

Литература

1. **WELMEC 7.2.** Issue 1. Software Guide (Measuring Instruments Directive 2004/22/EC).

2. **WELMEC 7.1.** Software Requirements on the Basis of the Measuring Instruments Directive (MID).

Дата одобрения 20.12.2007 г.

Подрисуночная подпись

Наборы требований к программному обеспечению средств измерений