

Анализ типовых проблем, возникающих при проверке программного обеспечения

Н. Д. ЗВЯГИН

Всероссийский научно-исследовательский институт метрологии им. Д. И. Менделеева,
С.-Петербург, Россия, e-mail: n.d.zviagin@vniim.ru

Рассмотрены типовые вопросы, возникающие как при добровольной аттестации программного обеспечения, так и при испытаниях в ходе процедуры утверждения типа средств измерений, в частности, вопросы использования различных методов идентификации, обновления и применения в России программного обеспечения, прошедшего аттестацию за рубежом.

Ключевые слова: программное обеспечение, метрологическая аттестация, идентификация.

The paper considers basic typical problems with which developers and experts conducting tests face frequently both at voluntary software validation and at testing for type approval. In particular problems of using different methods for software identification, problems of software update, problems of using software, that has passed validation abroad etc.

Key words: software, metrological validation, identification.

Средства измерений (СИ), оснащенные программным обеспечением (ПО) в том или ином виде, используются достаточно давно, однако вопрос о его проверке в России не получил широкого распространения. Некоторое время активно применяли процедуру добровольной аттестации ПО, которая, в основном, опиралась на требования международных документов [1, 2], разработанных WELMEC и МОЗМ, и отечественных [3–5], которые также основывались на международном опыте аттестации ПО. Процедура добровольной аттестации, как правило, проходила в тесном сотрудничестве с разработчиками СИ, и все возникавшие вопросы могли быть решены достаточно оперативно. Ситуация изменилась в связи с введением методики по утверждению типа СИ [6] и сопутствующей ей методики испытаний ПО [7]. Эти документы обязали всех производителей проводить испытания ПО на этапе утверждения типа СИ. Число разработчиков, вовлеченных в этот процесс, резко увеличилось, и соответственно возросло количество вопросов, возникающих на стадии испытаний. В данной статье обсуждаются типовые вопросы, связанные с аттестацией ПО и процедурами утверждения типа СИ. Также рассмотрены перспективы развития и возможные трудности при аттестации ПО СИ.

В отечественных нормативных документах выделены три основных параметра, по совокупности которых проводится аттестация ПО СИ:

методы защиты от преднамеренных и непреднамеренных изменений;

методы идентификации;

влияние ПО на метрологические характеристики СИ.

При этом если методы защиты и степень влияния ПО на метрологические характеристики СИ являются факторами, которые разработчик несомненно учитывает при проектировании таких программируемых средств, то идентификация ПО как отдельного модуля СИ далеко не всегда оказывается очевидной. В первую очередь, это относится к СИ со встроенным ПО. В этом случае производитель может предполагать, что вполне достаточно идентификации прибора (указания его наименования и модели). Иногда такая точка зрения выглядит обоснованной, однако она вступает в противоречие с требованиями к ПО, которые должны выпол-

няться для успешного прохождения аттестации или процедуры утверждения типа. В частности, они связаны с необходимостью предоставления идентификатора ПО, которым согласно отечественным документам служит номер его версии или контрольная сумма (или оба этих параметра). При этом доступ пользователя к идентификатору должен быть обеспечен программными средствами.

В случае с автономным ПО, которое устанавливают на персональный компьютер, даже тогда, когда ни номер версии, ни контрольная сумма не выводятся самой программой, эта проблема решается достаточно легко. Возможно применение сторонних программ для расчета контрольных сумм по широко известным алгоритмам хэширования. Использование сторонних программ также возможно в случае использования встроенного ПО с предусмотренным интерфейсом связи. Трудности возникают, когда приходится работать с ПО, которое является встроенным и не имеет интерфейса связи, по которому можно получить доступ к идентификационным данным либо исполняемому коду программы.

При непосредственной работе с производителем СИ такую проблему можно разрешить предоставлением исполняемых кодов программы отдельно от СИ с одновременным предоставлением гарантии от производителя, что заложены именно эти коды. Однако такая проверка невозможна, если аттестация (утверждение типа) ведется не с разработчиком, а с продавцом (так часто бывает на практике) или же ПО проверяют в собранном СИ и получить доступ к исполняемым кодам по какой-то причине невозможно. Например, такой подход совершенно неприемлем при периодической поверке, поскольку согласно [6, 7] раздел о поверке является необходимой частью протокола испытаний ПО СИ в целях утверждения типа.

В сложившейся ситуации целесообразно расширить список параметров, которые могут служить в качестве идентификатора ПО. В [2] номер версии и контрольная сумма приведены как примеры возможного решения вопроса об идентификации. Однако параметры идентификации не должны ограничиваться только ими. Поэтому в [2] в качестве одного из допустимых решений предлагается номер сертификата об утверждении типа (ТЕС). На взгляд автора, в отдельных

случаях (сходных с теми, что описаны выше) в качестве идентификатора могут также служить:

часть серийного номера прибора, причем несколько цифр в номере часто могут обозначать партию приборов, на которую устанавливалось именно данное конкретное ПО;

наименование и модель СИ. Этих параметров вполне достаточно, когда исследуемый прибор выпускается серийно и разработчик дает гарантию, что никакое иное ПО кроме прошедшего аттестацию на него не устанавливается и отсутствует возможность его замены без нарушения защиты.

Также не стоит ограничивать возможность предоставления идентификационных данных только программными средствами. Внесение данных в документацию на ПО (например, паспорт СИ), которая по определению является частью ПО, также вполне приемлемо. Возможно нанесение идентификационных признаков на сам прибор или конкретные микросхемы.

Обновление ПО, в том числе и автоматическое с использованием Интернет, в настоящее время является привычной процедурой для любого пользователя. В [1, 2] вопросам обновления ПО или его загрузки через интерфейсы связи посвящены отдельные разделы. Отечественные документы, касающиеся ПО СИ, к сожалению, практически не затрагивают эти вопросы. Можно отметить два типа обновления: метрологически значимой части ПО СИ, т. е. части, к которой относятся программы и программные модули, выполняющие функции сбора, передачи, обработки, хранения и представления измерительной информации, а также параметры, характеризующие тип СИ и внесенные в ПО [4]; части ПО, которая не является метрологически значимой. В последнем случае вопрос контроля такого обновления сводится к проверке правильности разделения ПО и взаимодействия между его частями, которая выполняется при аттестации или в ходе процедуры утверждения типа. Дополнительный контроль в данном случае не требуется.

Сложнее вопрос обновления метрологически значимой части ПО, которая согласно отечественным документам после утверждения типа СИ не должна изменяться. Любая её модификация приводит к изменению идентификационных данных (признаков) и необходимости повторной аттестации ПО [4]. Такое категоричное требование часто вызывает удивление у разработчиков и пользователей, так как в ходе эксплуатации любого ПО могут возникать неисправности (так называемые «баги»), которые не удалось выявить на стадиях тестирования. Загрузка обновлений ПО с исправлениями подобных ошибок (bug fixes) — стандартная практика для большинства современных программ. Требовать переаттестацию в таком случае нелогично.

Приемлемым выходом из сложившейся ситуации служит контролируемое или прослеживаемое обновление, происходящее автоматически. При этом все изменения ПО заносятся в контрольный журнал (журнал событий) программы, а в метрологически значимой части программы, в свою очередь, выделяются неизменяемая и необновляемая части, которые контролируют корректность вносимых изменений, соблюдение уровня защиты и целостности ПО. Достаточно подробно такой механизм обновления описан в [1, 2]. Подобный раздел следовало бы внести и в отечественные нормативные документы.

Значительная часть вопросов, возникающих при проведении аттестации ПО или проверке в ходе процедуры по утверждению типа СИ, относится к использованию в России СИ иностранного производства. Несмотря на то, что отече-

ственные нормативные документы в достаточной степени гармонизированы с международными требованиями, получить от зарубежного производителя всю необходимую информацию часто не удается. Это может происходить по разным причинам: от сложностей в квалифицированном обмене информацией между производителями СИ или отдельного программного продукта и их распространителями (а иногда вообще из-за отсутствия какой-либо связи) до слабой заинтересованности со стороны иностранного производителя в распространении своего СИ в России. Однако решать подобные вопросы необходимо, и, возможно, приведенные выше предложения могут этому способствовать.

С данной проблемой также тесно связан вопрос правомерности использования в России СИ, прошедших аттестацию ПО за рубежом и имеющих соответствующие сертификаты. Отечественные документы не дают ответа на вопрос, как поступать в подобной ситуации. На взгляд автора, возможны три варианта решения:

признать зарубежный сертификат и не проводить проверку;

проводить проверку, основываясь на сведениях, представленных в зарубежном сертификате;

проводить полную проверку, игнорируя зарубежный сертификат.

Каждый вариант имеет свои плюсы и минусы, но оставлять вопрос открытым нецелесообразно.

Недостаток информации о ПО СИ также возникает при использовании программного продукта, разработанного еще до введения дополнительных требований. Применять к такому ПО полный перечень требований вряд ли имеет смысл.

В ходе аттестации часто приходится сталкиваться с ПО, функции которого ограничиваются только сбором, передачей и представлением данных и никак не влияют на метрологические характеристики СИ. К такому ПО также нецелесообразно предъявлять полные требования. Возникает вопрос о необходимости именно метрологической аттестации подобного ПО: если данные передаются в неизменном виде, то их характер (т. е. являются ли эти данные результатами измерений или же какими-либо другими данными), не может оказывать влияния на итог того или иного вида проверки. Сложность в данном случае заключается в правильном разделении ПО на части, одна из которых влияет на метрологические характеристики СИ, а другая не влияет (значимой может оказаться даже такая простая операция, как округление).

Все перечисленные вопросы требуют внимательного рассмотрения, а существующим методикам аттестации необходима тщательная доработка.

Программное обеспечение СИ постоянно развивается и усложняется. Многие наработки, которые были актуальны несколько лет назад, сейчас уже представляются устаревшими. В частности, в настоящее время наблюдается тенденция к использованию легко модифицируемых операционных систем (например, систем с открытым кодом типа Linux) в качестве встроеного ПО. Грань между автономным и встроенным ПО стирается, и поэтому принципиальная классификация, на которой ранее строились требования к ПО, может оказаться неприменимой. Многие проблемы, которые до этого разрешались при метрологической аттестации, оказываются слишком широкими и выходящими за рамки метрологии. Встает вопрос о возможном пересмотре изначальных подходов к аттестации ПО. Международные метрологические организации стараются отслеживать все изменения

и вносят коррективы в свои документы (например, выпущено уже 5-е издание [2]). Вместе с тем, ведутся разработки новых подходов к метрологической аттестации ПО.

В России применяются СИ отечественных и иностранных производителей. Нередко объектами аттестации и проверки становятся уникальные разработки, которые были невозможны на более ранней стадии развития компьютерных технологий. Многие системы представляют собой сложные программно-аппаратные комплексы, аттестация которых требует глубокого и тщательного анализа. Поэтому необходимо периодически пересматривать отечественные нормативные документы по аттестации ПО для их гармонизации с международными документами. Важны активное участие российских специалистов в международных Технических комитетах, занимающихся разработкой документов, регламентирующих подходы к аттестации ПО, а также проведение совместных семинаров по данной тематике (см., например [8]).

Л и т е р а т у р а

1. **Рекомендация МОЗМ D 31:2008.** Общие требования к программно-контролируемым средствам измерений.

2. **WELMEC 7.2.** Руководство по программному обеспечению. 2010.

3. **ГОСТ Р 8.654—2009.** ГСИ. Требования к программному обеспечению средств измерений. Основные положения.

4. **МИ 2955—2010.** ГСИ. Типовая методика аттестации программного обеспечения средств измерений.

5. **СК 02-30—10.** Программное обеспечение обработки данных при измерениях. Общие положения и порядок проведения метрологической аттестации.

6. **МИ 3290—2010.** Рекомендация по подготовке, оформлению и рассмотрению материалов испытаний средств измерений в целях утверждения типа.

7. **МИ 3286—2010.** Проверка защиты программного обеспечения и определение ее уровня при испытаниях средств измерений в целях утверждения типа.

8. **Математическая,** статистическая и компьютерная поддержка качества измерений. Аттестация программного обеспечения, используемого в метрологии // Труды Междунар. семинара. СПб., 2012 [Электрон. ресурс]. <http://mscsmq.vniim.ru> (дата обращения: 05.12.2012 г.).

Дата принятия 04.02.2013 г.

ИЗМЕРЕНИЯ В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ

621.317:621.37.39

Метрологическое обеспечение измерений количества и скорости передачи информации

И. А. ШАЙКО*, Е. И. ШАЙКО**

* ЗАО «Супертехприбор», Мытищи, Россия

** ФГКУ «ГНМЦ» Минобороны России, Мытищи, Россия, e-mail:skb@spribor.ru

Разработаны предварительные предложения по составу измеряемых параметров информации, облику и структуре измерителей данных параметров и средств их метрологического обеспечения.

Ключевые слова: метрологическое обеспечение, скорость передачи информации, количество информации.

The preliminary proposals on composition of measurable information parameters, appearance and structure of these parameters measuring instruments and means of their metrological assurance are carried out.

Key words: metrological assurance, information rate, amount information.

В настоящее время существует несколько определений и толкований понятия «информация». В информатике наиболее часто используется следующее толкование: информация — это осознанные сведения об окружающем мире, которые являются объектом хранения, преобразования, передачи и использования. В [1] дано определение: «Информация — сведения (сообщения, данные) независимо от формы их представления». К основным видам информации относятся: графическая, звуковая, текстовая, числовая, видеоинформация, органолептическая и т. д. Научный подход к оценке информации был предложен еще в 1928 г. американским инженером Р. Хартли. Количество информации рассчитывают по формуле

$$K = \log_2 N,$$

где N — количество равновероятных событий (число возможных выборов).

С разработкой общей теории информации и математической теории связи К. Шенноном в 1948 г. стало возможным хранить, обрабатывать и передавать информацию в виде двоично-кодированной последовательности. Расчетная формула К. Шеннона учитывает неодинаковую вероятность P событий:

$$K = -\log_2 P.$$