

Проблемы оценки качества программного обеспечения СИ



Современные средства измерений (СИ) в своём подавляющем большинстве представлены автоматизированными приборами, которые включают в себя или сопровождаются программным обеспечением (ПО) разного уровня сложности. Это программное обеспечение условно можно разделить на встроенное и автономное. Встроенное ПО характеризуется тем, что в этом случае микропроцессор, интерфейс для подключения периферийных устройств и инструментальная часть прибора заключены в общий корпус и, как правило, прямой доступ к программному обеспечению отсутствует. Подавляющее большинство автоматизированных СИ являются приборами со встроенным ПО. Автономное ПО реализуется на сменном носителе (дискета, компакт-диск, флеш-карта) и функционирует на базе универсального (в большинстве случаев персонального) компьютера.

В настоящее время при использовании ПО в СИ всё чаще ставятся вопросы о гарантиях правильности результатов, полученных с его помощью, о степени влияния программного продукта на метрологические характеристики СИ, об его уровне защищённости от преднамеренных и непреднамеренных воздействий и, в конечном итоге, о сте-

Ю.А. Кудеяров, доктор физ.-мат. наук

ВНИИМС, Москва

А.В. Шестаков

Автономная некоммерческая организация
 “Межрегиональный испытательный центр”
 (АНО “МИЦ”), Москва

Ключевые слова: метрологические характеристики СИ; программное обеспечение; несанкционированная настройка; погрешность; тестирование; опорный программный продукт; эталонные данные; метод моделей исходных данных

ПРОБЛЕМЫ ОЦЕНКИ КАЧЕСТВА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СРЕДСТВ ИЗМЕРЕНИЙ



пени доверия к результатам, полученным с помощью программного обеспечения.

В связи с этим в п. 2 ст. 9 Федерального закона РФ “Об обеспечении единства измерений” появилось положение о необходимости обеспечения ограничения доступа к определённым частям СИ (включая ПО) в целях предотвращения несанкционированных настройки и вмешательства, которые могут привести к искажениям результатов измерений. Для выполнения указанного положения Мипромторгом издан приказ от 30 ноября 2009 г. № 1081, определяющий порядок проведения испытаний стандартных образцов и СИ для целей утверждения типа. В Приложении 3 к этому приказу изложен порядок проверки защиты ПО при таких испытаниях. Для конкретизации названного приказа разработаны рекомендация Р 50.2.077-2011 [1], а также методики ВНИИМС: МИ 3286-2010 [2] и МИ 3290-2010 [3].

Необходимость указанных документов вызвана, в частности, тем, что наличие в составе СИ программного обеспечения сопряжено с возможным проявлением рисков [4], большинство из которых обусловлено, в первую очередь, возможностью внешних воздействий на ПО, влияющих на результаты измерений. Не исключено также возникновение погрешностей, причиной которых является ПО само по себе. Источники погрешностей, вносимых программным обеспечением в результаты вычислений, могут быть следующими:

- неадекватность используемых алгоритмов решаемой измерительной задаче;
- перевод чисел из десятичной системы счисления в двоичную и наоборот;

– ограниченность разрядной сетки;

– округление на промежуточных этапах вычислений;

– обрыв бесконечных рядов, являющихся представлениями большинства используемых при вычислениях библиотечных функций;

– неопределённость табличных значений констант, используемых при вычислениях;

– неудачный выбор алгоритмов вычислений, в частности использование так называемых неустойчивых (необусловленных) алгоритмов и т. д.

Вопросы, связанные с возможными источниками погрешностей, характерных для ПО, рассмотрены в пособии [5].

Таким образом, становится очевидной актуальность проблемы оценки качества ПО СИ и информационно-измерительных систем (ИИС), которая особенно обострилась в последние годы, когда автоматизированные СИ и ИИС стали широко применяться для коммерческого учёта сырья, электроэнергии, других энергоресурсов (автоматизированные системы контроля учёта энергоресурсов, или АСКУЭ).

Оценке качества программных продуктов, особенно тех, которые используются для коммерческого учёта и при производстве промышленной продукции, должно быть уделено самое серьёзное внимание. Имеется ряд нормативных документов, регламентирующих показатели качества ПО и методы их определения. Примером могут являться стандарты [6–8]. В этих стандартах в числе прочих методов качество ПО предлагается определять путём сравнения полученных расчётных значений показателей с соответствующими базовыми значениями показателей существующего

аналога или расчётного ПО, принимаемого за эталонный образец. В качестве аналогов выбираются реально существующие ПО того же функционального назначения, что и тестируемое, с такими же основными параметрами, подобной структуры и применяемые в схожих условиях эксплуатации.

Содержание упомянутых документов в значительной степени совпадает с той методологией оценки качества ПО СИ, которая фактически реализована в настоящее время, например, в рамках действующей Системы добровольной сертификации программного обеспечения, о которой будет сказано далее.

Таким образом, применительно к СИ показатели качества ПО должны в первую очередь измерять отклонение тестовых результатов, полученных при тестировании ПО СИ, от опорных, полученных так называемым опорным ПО. Под опорным ПО понимается программное обеспечение, используемое для сравнения с тестируемой программой и отвечающее наивысшим требованиям к вычислительным и функциональным характеристикам, подтверждённым (в ряде случаев независимыми методами) неоднократным тестированием и применением [9].

Эти отклонения могут быть выражены в разных формах:

– в виде отличия между тестовыми и опорными результатами, т. е. как абсолютная характеристика точности ПО;

– в виде числа совпадающих цифр, т. е. как относительная характеристика точности;

– в виде исполнительной характеристики (*англ.* performance measure) [10], рассчитываемой для различных факторов, включая расчётную точность математического аппарата, используемого для

получения тестовых и опорных результатов, и коэффициенты обусловленности;

– в виде относительного отличия тестовых результатов от опорных.

Могут использоваться и другие показатели качества, такие как, например, требуемый объём памяти, время исполнения и т. п.

Необходимость оценки качества программного обеспечения средств измерений настоятельно подчёркивается в ряде международных и отечественных рекомендаций [11–16], в которых раскрываются различные аспекты требований к ПО СИ.

В настоящее время в нашей стране разработана нормативная база, позволяющая в большинстве случаев решить на приемлемом уровне проблему оценки качества ПО СИ и ИИС систем. Эта база в первую очередь представлена методиками [9] и [17].

Если говорить о содержательной части работы по оценке качества ПО СИ, то она сводится, главным образом, к тестированию программных продуктов методом “чёрного ящика”. Опыт тестирования ПО, накопленный как зарубежными метрологическими организациями (NPL, Великобритания; NIST, США; PTB, ФРГ), так и отечественными, показывает, что в большинстве метрологических приложений метод “чёрного ящика” характеризуется относительной простотой, дешевизной и достаточной глубиной тестирования, и это хорошо соотносится с требованием минимизации усилий по оценке качества ПО.

Метод “белого ящика”, или “сквозного прохода” (*англ.* walk through method), когда производится проверка исходного кода и детальное исследование программных функций, используется лишь при испытаниях очень сложных изме-

рительных систем, или когда к этим системам предъявляются исключительные требования по безопасности и надёжности функционирования. Опыт тестирования программных продуктов показывает, что в ряде случаев при согласии заказчика тестирования приходится использовать анализ исходного кода или его фрагментов для того, чтобы сделать определённые необходимые заключения о свойствах ПО. Но это, как правило, исключение.

Существенные сложности возникают при тестировании встроенного ПО. Уже говорилось, что к встроенному ПО нет непосредственного доступа, что в свою очередь в большинстве случаев приводит к невозможности непосредственного тестирования и оценивания его свойств. Указанные проблемы и возможные подходы к их решению были рассмотрены в работе [18]. Стремление к повышению качества и конкурентоспособности выпускаемых приборов, необходимость защиты измерительной информации от преднамеренных изменений в расчётных операциях между поставщиками и потребителями сырья, энергетических и других ресурсов, требования заказчиков и пользователей автоматизированных СИ, а также настоятельные рекомендации международных и отечественных организаций по стандартизации и метрологии приводят к необходимости оценки свойств и характеристик встроенного ПО СИ и их соответствующего документирования. Для решения этой задачи, а также для проверки СИ со встроенным ПО производители вводят в соответствующее средство измерений специальный режим или предоставляют в распоряжение организаций, проводящих проверку (тестирование)

ПО СИ, специальные аппаратные и программные средства, позволяющие реализовать тестирование программного обеспечения [19].

В силу ряда причин, не связанных с содержанием настоящей статьи, на текущий момент в нашей стране отсутствует приемлемая и надлежаще функционирующая система аккредитации организаций на проведение тестирования программных продуктов, используемых в СИ и ИИС. В этих условиях специалисты, занимающиеся тестированием ПО СИ, отвечая на вызов времени, в соответствии с Федеральным законом “О техническом регулировании” выступили с инициативой создания Системы добровольной сертификации программного обеспечения средств измерений и информационно-измерительных систем (СДС ПО СИИИС). Поначалу в качестве организации, создавшей в мае 2006 г. названную систему, выступил ФГУП “ВНИИМС”. В настоящее время СДС программного обеспечения, продолжающая выполнять работы по тестированию ПО СИ и ИИС, представлена автономной некоммерческой организацией “Межрегиональный испытательный центр” (АНО “МИЦ”), Москва. Указанная система зарегистрирована Федеральным агентством по техническому регулированию и метрологии в мае 2012 г. Таким образом общий срок апробации методов решения описываемых в настоящей статье проблем оценки качества ПО СИ составляет более 6 лет.

В практической деятельности по сертификации ПО одним из основных методов тестирования является сравнение его результатов с результатами расчётов, выполненных опорной программой (*англ.* reference software). Соответствующая схема сравнения аналогична



ПРОБЛЕМЫ ОЦЕНКИ КАЧЕСТВА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СРЕДСТВ ИЗМЕРЕНИЙ



схеме, используемой, например, при поверке и калибровке СИ (рис. 1).

Критерии отнесения программного продукта к опорному условны, в значительной степени несут субъективный характер и являются предметом соглашения между заказчиком и исполнителем сертификации ПО. По нашему убеждению, это нормальная ситуация, поскольку в общем случае невозможно сформулировать критерии отнесения программного продукта к опорному. Для каждой программы эта проблема должна решаться с учётом измерительной и функциональной конкретики. Объединяет опорные программные продукты то, что каждый такой продукт обязан удовлетворять критериям, сформулированным в его определении.

В качестве опорных программных продуктов могут быть использованы или уже разработанные и хорошо известные специалистам программы, или специально разработанные для целей тестирования программы, написанные в стандартных программных пакетах типа Excel, MathCad, Matlab и т. п. Такое действие допустимо для значительного числа случаев тестирования ПО, поскольку алгоритмы, “защитные”, например, в СИ со встроенным ПО, как правило, не являются сложными.

Описанная методология была реализована при сертификации таких встроенных программных продуктов, как ПО АСКУЭ типа “Пульсар” (разработка ООО “Ценнер-Водоприбор Лтд.”), программное обеспечение расходомера электромагнитного типа РМ-5 и счётчиков количества теплоты КМ-5 и КМ-9 (разработчик – ООО “ТБН энерго-сервис”) [19] и ряда других.

Типичная ситуация, с которой приходится сталкиваться при сер-

тификации автономного ПО, характеризуется тем, что нередко опорное ПО отсутствует или недоступно. В этом случае предлагаются к использованию метод генерации так называемых эталонных данных (англ. reference data set) [10] или метод моделей исходных данных (рис. 2), предложенный методикой МИ 2174 [17].

Сравнение схемы тестирования на рис. 2 со схемой тестирования ПО с использованием генерации “эталонных данных” (рис. 3) приводит к выводу, что метод моделей исходных данных может рассматриваться как частный случай метода генерации “эталонных данных”. На рис. 2 отсутствует генератор “эталонных данных”, а модели исходных данных играют роль как “эталонных” (модельных) результатов, так и “эталонных данных”.

Метод генерации “эталонных данных” в сочетании с методом моделей исходных данных был использован, например, при сертификации такого сложного программного продукта, как программное обеспечение сканирующих зондовых микроскопов [20].

Таким образом, несмотря на все трудности, оценка качества ПО СИ и ИИС в отечественной метрологической практике постепенно находит свои приемлемые очертания, особенно при сертификации ПО через Систему добровольной сертификации. Однако проверка уровня защиты ПО при испытаниях для целей утверждения типа в последнее время сталкивается с определёнными трудностями, вызванными возражениями ряда разработчиков автоматизированных СИ против некоторых положений нормативных документов в этой области. Особенно сильное сопротивление встречают процедуры определения идентифи-



Рис. 1 Тестирование ПО с использованием опорного программного продукта

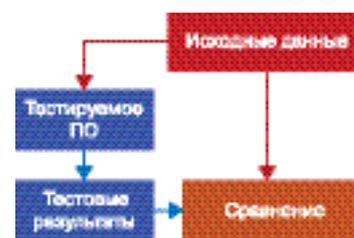


Рис. 2 Тестирование ПО методом моделей исходных данных



Рис. 3 Тестирование ПО с использованием генерации “эталонных” данных

кационных признаков ПО и установления соответствия ПО утверждённому типу, описанные в Рекомендации Р 50.2.077 [1] и в методике МИ 3286 [2], в связи с чем создана рабочая группа по пересмотру Рекомендации [1]. Требуется переработки и ГОСТ Р 8.596 [15] ввиду избыточ-

ности некоторых требований и необходимости его максимальной гармонизации с международными рекомендациями. Наряду с дальнейшим совершенствованием используемых методов тестирования ПО, основанных на методологии “чёрного ящика”, необходимо постепенно переходить там, где это необходимо, к освоению анализа исходного кода программ или его фрагментов.

Можно констатировать, что проблемы оценки качества ПО СИ и ИИС находят всё больший отклик в среде разработчиков и пользователей соответствующего программного обеспечения. За время существования СДС программного обеспечения на базе описанной ранее методологии было сертифицировано более тысячи программных продуктов самого широкого назначения, в том числе относящихся к программным средствам для автоматизированных систем управления технологическими процессами (АСУ ТП) и их моделирования, для систем автоматизированного проектирования (САПР), для систем управления (СУ), функционирующих с использованием измерительного оборудования или элементов измерительных систем, для систем управления базами данных (СУБД), связанных с передачей, хранением, актуализацией, защитой, обеспечением доступа и использованием измерительной, вычислительной и иной информации, а также для АСКУЭ, в том числе коммерческого учёта электроэнергии, нефтепродуктов, газа, тепловой энергии, воды и т.п., для устройств с измерительными функциями, тренажёров и иных имитационных систем, для контроллеров и вычислительных блоков.

Нельзя не отметить, что, исходя из сиюминутных экономических соображений, некоторые произведе-

ли программных продуктов для СИ и ИИС, ссылаясь на добровольность сертификация ПО, не соглашаются на независимую оценку качества программного обеспечения. Однако спрос на сертификацию ПО СИ и ИИС непрерывно растёт. Недалеко

то время, когда выход на рынок автоматизированных СИ будет возможен только с документальным подтверждением качества используемого в них ПО. Соответственно, будет уменьшаться стоимость проведения сертификационных процедур.



Литература

1. Р 50.2.077-2011. ГСИ. Испытания средств измерений в целях утверждения типа. Проверка обеспечения защиты программного обеспечения.
2. МИ 3286-2010. Проверка программного обеспечения средств измерений при испытаниях с целью утверждения типа.
3. МИ 3290-2010. ГСИ. Рекомендация по подготовке, оформлению и рассмотрению материалов испытаний средств измерений в целях утверждения типа.
4. Grottke U., Schwartz R. Software in legal metrology // OIML bulletin. – 2003. – № 2. – Р. 24.
5. Кудяров Ю. А. Испытания (тестирование) программного обеспечения средств измерений: Учеб. пос. – М.: АСМС, 2010.
6. ГОСТ 28195-89. Оценка качества программных средств. Общие положения.
7. ГОСТ Р ИСО/МЭК 9126-93. Оценка программной продукции. Характеристики качества и руководства по их применению.
8. ISO/IEC 14598 series. Information technology – Software product evaluation.
9. МИ 2955-2010. ГСИ. Типовая методика аттестации программного обеспечения средств измерений.
10. Cook H. R., Cox M. G., Dainton M. P., Harris P. H. Methodology for testing spreadsheets and other packages used in metrology / Report to National Measurement System Policy Unit, September 1999.
11. Руководство WELMEC 7.1. Версия 5.23. Требования к программному обеспечению на основе директивы по измерительным приборам. – Июль, 1999.
12. WELMEC 7.2. Issue 1. Software Guide. (Measuring Instruments Directive 2004/22/EC). – March, 2012.
13. ГОСТ Р ИСО/МЭК 17025-2006. Общие требования к компетентности испытательных и калибровочных лабораторий.
14. Рекомендация КООМЕТ R/LM/10:2004. Программное обеспечение средств измерений. Общие технические требования.
15. ГОСТ Р 8.596-2002. ГСИ. Метрологическое обеспечение измерительных систем. Основные положения.
16. ГОСТ Р 8.654-2009. ГСИ. Требования к программному обеспечению средств измерений. Основные положения.
17. МИ 2174-91. ГСИ. Аттестация алгоритмов и программ обработки данных при измерениях. Основные положения.
18. Дудыкин А. А., Кудяров Ю. А., Паньков А. Н. Проблемы аттестации встроенного программного обеспечения // Законодательная и прикладная метрология. – 2007. – № 1. – С. 22.
19. Бурдуниин М. Н., Кудяров Ю. А., Паньков А. Н. Оценка качества программного обеспечения счётчика-расходомера РМ-5 и счётчика количества теплоты // Главный метролог. – 2007. – № 3. – С. 32.
20. Голубев С. С., Козлов М. В., Кудяров Ю. А. Тестирование программного обеспечения сканирующих зондовых микроскопов // Измерительная техника. – 2012. – № 6. – С. 21–25.