

*На правах рукописи*

**САТАНОВСКИЙ АНДРЕЙ АРКАДЬЕВИЧ**

**РАЗРАБОТКА НАУЧНО-МЕТОДИЧЕСКИХ ОСНОВ  
МЕТРОЛОГИЧЕСКОЙ АТТЕСТАЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ  
СРЕДСТВ ИЗМЕРЕНИЙ**

Специальность 05.11.15 – Метрология и метрологическое обеспечение

**АВТОРЕФЕРАТ**

**диссертации на соискание ученой степени  
кандидата технических наук**

Москва – 2007

Работа выполнена во Всероссийском научно-исследовательском институте метрологической службы (ФГУП «ВНИИМС»)

**Научный руководитель:**

Кандидат технических наук      **Ю.Е. Лукашов**

**Научный консультант:**

Доктор физико-математических наук      **Ю.А. Кудеяров**

**Официальные оппоненты:**

Доктор технических наук      **А.А. Данилов**

Кандидат технических наук      **Р.И. Генкина**

**Ведущая организация:**      Московский институт электронного машиностроения (МИ-ЭМ)

Защита состоится " 11 " октября 2007 г. в 14-00 на заседании диссертационного совета Д 308.001.01 в ФГУП " ВНИИМС" по адресу: 119361, Москва, ул. Озерная, 46.

**С диссертацией можно ознакомиться в библиотеке ФГУП «ВНИИМС».**

Автореферат разослан 06.09.2007 г.

*Ученый секретарь диссертационного совета*

Доктор технических наук \_\_\_\_\_ **В. Г. Лысенко**

Актуальность работы. Для решения многих измерительных задач используются программные средства, которые применяются как для управления измерительным процессом, так и для реализации функций сбора, передачи, обработки, хранения и представления результатов измерений. Вместе с тем, расширяя возможности измерительного оборудования, программные средства могут вносить дополнительные ошибки в результаты измерений, которые обусловлены несовершенством используемых алгоритмов, возможностью возникновения программных или аппаратных сбоев, потерь и искажений данных и т.д.

Учитывая все возрастающую надежность механических, электрических и электронных компонентов средств измерений (СИ) можно сделать вывод, что качество измерений все в большей степени определяется правильной работой программного обеспечения (ПО).

Качество и надежность СИ традиционно обеспечиваются проведением их испытаний и утверждением типа, периодической поверкой или калибровкой, сертификацией. В настоящее время свойства ПО как самостоятельного объекта не оцениваются с помощью этих процедур, а оцениваются только в составе СИ. Однако особенности функционирования ПО, его высокая мобильность ведут к необходимости рассматривать его как самостоятельный объект оценки. В связи с этим высокую актуальность приобретает задача метрологической аттестации ПО. Эта задача не может быть решена в рамках традиционных подходов к верификации (сверка) программных средств, поскольку свойства ПО интересны в данном случае не сами по себе, а в их связи с функционированием СИ. Анализ состояния данной проблемы показал, что в нашей стране, несмотря на значительное количество статей и монографий по вопросам влияния программных средств и вычислительных устройств на достоверность результатов измерений отсутствует единый и систематизированный подход к решению задачи метрологической аттестации ПО. Решению этой задачи посвящена настоящая работа.

Цель и задачи работы. Целью данной работы является анализ, исследование и разработка методических основ метрологической аттестации ПО СИ, а также методов оценки влияния ПО СИ на достоверность результатов измерений.

В соответствии с целью работы основными задачами являются:

1. Исследование и классификация причин недостоверности результатов измерений, связанных с использованием ПО СИ. Разработка системы метрологических показателей ПО СИ.
2. Разработка системы требований к ПО СИ по каждой из выделенных его характеристик. Разработка подхода к установлению требований к ПО СИ, позволяющего решать задачу выбора методов его аттестации.
3. Разработка математических и программных методов, используемых при оценке погрешности, вносимой ПО в результаты измерений.

Методы исследования. В работе использованы методы системного анализа, оптимизации требований к организационным системам, теории погрешностей, математического программирования, имитационного моделирования, теории вероятностей и математической статистики.

Научная новизна.

1. Проведен анализ и классификация источников ошибок ПО СИ.
2. Выявлены характеристики ПО СИ, оказывающие наиболее значимое влияние на достоверность результатов измерений.
3. Разработана система требований к ПО СИ, позволяющая обеспечить заданный уровень достоверности результатов измерений.
4. На основе исследования разработан ряд алгоритмов генерации эталонных данных для оценки погрешности, вносимой ПО СИ в результаты измерений при их обработке.

Комплекс полученных результатов позволил сформулировать методические основы метрологической аттестации ПО СИ.

Практическая ценность. Практическая ценность диссертационной работы состоит в том, что полученные результаты позволяют системно проводить работы по метрологической аттестации ПО СИ. Разработаны основы системы метрологической аттестации ПО СИ, а именно: классификация ПО СИ, общие требования к ПО СИ и подход к их назначению различным видам ПО СИ, методика аттестации ПО СИ на соответствие общим требованиям и порядок ее проведения.

Полученные результаты позволяют:

1. Обеспечить рациональные требования к различным видам ПО СИ;
2. Осуществить достоверную проверку соответствия ПО СИ установленным требованиям;
3. Разработать типовую методику аттестации ПО СИ, применимую в большинстве практических случаев;
4. Разработать и программно реализовать алгоритмы генерации эталонных данных для оценки погрешности, вносимой ПО СИ в результаты измерений.

Апробация и реализация результатов исследований.

Основные положения работы докладывались и обсуждались на НТК Ростехрегулирования, НТС ВНИИМС, научно-технических семинарах ВНИИМС.

На основе разработанных документов по метрологической аттестации ПО СИ были проведены испытания следующих программных средств:

- Программного обеспечения калибраторов семейства Veamex QCAL – программы QD3;
- Программного обеспечения по расчету вместимости технологических трубопроводов - программы “Труба”;
- трех коммерческих пакетов математического и статистического ПО, применяемого для автономной обработки результатов измерений.

Разработаны методики метрологической аттестации указанных программ, проведены практические работы по аттестации с применением разработанных методов испытаний.

Публикации. Основной материал диссертации опубликован в 4 работах в виде научных статей, отчетов по результатам НИР – 1, методик института - 2.

Структура и объем диссертации. Диссертация состоит из введения, 5 глав с выводами по каждой из них, заключения и списка литературы. Диссертация изложена на 123 страницах, включает 15 рис., 14 таблиц и список литературы из 74 наименований.

Основные положения, выносимые на защиту. На защиту выносятся:

1. Классификация источников ошибок результатов измерений, связанных с использованием ПО СИ и система метрологических показателей ПО СИ.
2. Выбор системы общих требований к ПО СИ;
3. Подход к установлению требований к различным видам ПО СИ на основе его классификации;
4. Методика аттестации ПО СИ и порядок ее проведения.

## СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность, новизна и практическая значимость разработки системы метрологической аттестации ПО СИ.

В главе 1 проведен обзор отечественной и зарубежной литературы посвященной вопросам оценки качества ПО СИ и методов его реализации при осуществлении практической деятельности. Проанализированы причины внесения искажений в результаты измерений связанные с использованием ПО.

Выявлены следующие основные источники ошибок:

- ошибки, связанные с погрешностью, вносимой ПО при обработке данных, т.е. ошибками выбора и реализации алгоритмов обработки данных,
- ошибки, связанные с преднамеренным или неумышленным искажением исходного кода ПО,
- ошибки связанные с искажением данных при их передаче, хранении и представлении.

Источники ошибок схематично изображены на рис. 1



Рис. 1 Источники ошибок ПО СИ

На основе анализа ряда публикаций подробно проанализированы основные источники погрешностей, которые могут возникнуть при обработке и преобразовании результатов измерений и которые могут быть связаны с:

- обрывом бесконечных рядов, являющихся представлениями большинства используемых при вычислениях библиотечных функций,
- округлением на промежуточных этапах вычислений,
- переводом чисел из десятичной системы счисления в двоичную и наоборот,
- неудачным выбором алгоритмов вычислений, в частности, использование так называемых неустойчивых (необусловленных) алгоритмов а также ошибки их программной реализации и др.

С учетом проведенного исследования определяются особенности ПО СИ и строятся в соответствии с ними система метрологических показателей ПО СИ.

К особенностям ПО СИ, в частности, относятся специальные требования, предъявляемые к ПО СИ:

- применяемое ПО не должно влиять на метрологические характеристики соответствующих СИ;

- ПО должно быть защищено от изменений (искажений) программного кода, параметров ПО, относящихся к метрологическим характеристикам СИ, а также измерительной информации;

- ПО, используемое в индивидуальных СИ данного типа, должно находиться в соответствии с ПО, документированным при утверждении типа СИ.

- продолжительность и усилия, необходимые для проведения испытаний ПО должны быть меньше продолжительности и усилий затрачиваемых на разработку соответствующего ПО.

Таким образом, может быть определена система метрологических показателей ПО СИ, а именно:

- Аттестуемость (свойство ПО, обеспечивающее возможность проверки предъявляемых к нему требований);

- Погрешность, вносимая ПО при обработке данных;

- Соответствие ПО утвержденной при аттестации версии;

- Защищенность ПО и данных от искажений.

На основе проведенного исследования и полученных результатов предложены рекомендации (требования) к процессу разработки ПО СИ:

- описание и спецификация каждого требования, предъявляемого к разрабатываемому ПО;

- описание и спецификация модели функционирования СИ совместно с ПО (интерфейсы передачи, ввода данных и т.д.), а также описание функциональных требований к системе (например, ПК) на основе которой будет функционировать система;

- описание модели функционирования управляющего системой ПО (например, предусматривается ли разделение ПО, описание модулей, реализующих функции сбора, хранения, представления, передачи измерительных данных, вопросы защиты данных и др.);

- оценка уровня риска, сопровождающего использование данного типа ПО и установление соответствующих технических средств защиты в целях обеспечения требуемого уровня соответствия и защиты кода программы и данных от искажений, в том числе учет фактора надежности;

- оценка алгоритмов, выбранных для реализации их в ПО, с точки зрения пригодности к решению конкретной измерительной задачи с установленной точностью;

При этом следует отметить, что разработчикам рекомендуется предусматривать возможность аттестации разрабатываемого ими ПО еще на стадии проектирования (например, наличие в ПО интерфейсов идентификации, ввода данных для тестирования и др.)

Таким образом, в главе 1 исследована и разработана система метрологических показателей ПО СИ, основывающаяся на классификации причин недостоверности результатов измерений, связанных с использованием ПО.

Полученные результаты являются основой для дальнейшего исследования и разработки следующих компонентов системы аттестации ПО СИ, а именно:

- система требований к ПО СИ (гармонизированная с международными рекомендациями) и подход к установлению требований к ПО СИ, позволяющий решать задачу выбора методов его испытаний при аттестации ПО СИ;

- методика оценки соответствия по каждому из требований, а также организационный и методический порядок проведения аттестации ПО СИ;

- программные средства для проведения работ по оценке погрешности ПО при обработке данных.

В главе 2, на основе обзора, проведенного в главе 1, проанализированы подходы к классификации ПО, содержащиеся в отечественной и зарубежной литературе. Сделан вывод о нецелесообразности однозначного заимствования изложенных в литературе подходов к классификации. К недостаткам указанных подходов можно отнести недостаточный учет особенностей функционирования ПО в составе СИ, а в литературе, ориентированной на общие подходы к классификации программных средств, подобные особенности вообще не учитываются. Наиболее приемлемый подход изложен в рекомендации WELMEC 7.1, однако и он не может быть использован для этой цели т.к. не учитывает такую важную особенность ПО СИ, как возможность его влияния на результаты измерений и некоторую перегруженность классификационными признаками.

В работе предложена схема классификации ПО СИ, учитывающая положительные стороны проанализированных подходов и способов классификации, и при этом наиболее полно отвечающая особенностям функционирования ПО в составе СИ.

Разработанная схема классификации ПО СИ представлена в таблице 1.

Таблица 1

Схема классификации ПО СИ

Классификационный признак (вид)	Классы вида
Аппаратная реализация	- Встроенное ПО - Автономное ПО
Критичность	- Не критично - Критично - Высококритично
Изменяемость	- Закрытый код (коммерческое) - Ограниченно модифицируемый код (модифицируемое) - Открытый код (целевое)
Функциональность	- Сбор, передача, хранение, представление данных - Обработка данных

Под перечисленными классификационными видами понимается:

*Аппаратная реализация* - классификация ПО СИ на основе его аппаратного обеспечения (микропроцессорные устройства, вычислители, ПК, смешанное). Данный классификационный вид в существенной мере определяет дальнейшие подходы к установлению требований, предъявляемых к ПО СИ, и методам оценки его соответствия.

*Критичность* – характеризует уровень экономической и/или социальной значимости последствий в случае искажения измерительных данных, неправильного использования и/или ошибок ПО.

*Изменяемость* – указывает на доступность изменений функций ПО (модификация, расширение функций).

*Функциональность* – классификация ПО в соответствии с выполняемыми функциями.

Для выработки рациональных методов оценки качества ПО СИ целесообразно установить систему требований к различным видам ПО и ввести определенные уровни для каждого из таких требований. В качестве подобных требований могут быть предложены жесткость испытаний, степень соответствия утвержденной версии и уровень защиты от умышленных или случайных искажений. Иллюстрация возможного подхода к назначению уровней перечисленных требований является описание, приведенное в таблице 2.

Таблица 2

## Уровни требований к программному обеспечению средств измерений

	<i>Низкая</i>	<i>Средняя</i>	<i>Высокая</i>
<i>Жесткость испытаний</i>	Функции ПО проверяются в соответствии с программой испытаний СИ. По некоторым характеристикам, не охватываемым программой испытаний, допускается принимать декларацию разработчика о соответствии ПО	ПО испытывается на основании описания программных функций, предоставленных разработчиком. Оцениваются средства идентификации и защиты ПО, его влияние на результаты измерений.	Проверяется исходный код ПО. Предметом испытаний исходного кода программы может являться, например, реализация алгоритма вычислений.
<i>Степень соответствия</i>	ПО не имеет идентификации или алгоритм идентификации не является частью испытываемого ПО.	Изменение утвержденной, законодательно контролируемой части ПО приводит к формированию его новой версии и требует дополнительных работ по аттестации. Изменение частей ПО, не подлежащих обязательному метрологическому контролю, не приводит к изменению версии ПО.	ПО полностью идентично утвержденному. Любые изменения в коде автоматически приводят к формированию новой версии.
<i>Уровень защиты</i>	Не требуется специальной защиты контролируемого ПО и данных от недопустимых изменений.	ПО и данные, подлежащие метрологическому контролю, защищены от недопустимых изменений с использованием простых программных средств, например текстовых редакторов.	ПО и данные, подлежащие метрологическому контролю, защищены от недопустимых изменений с использованием специальных программных средств (отладчики и редакторы жестких дисков, ПО для разработки программ и т.д.).

Эти требования существенно связаны с определенными ранее классификационным признаками (табл. 3).

В работе приводится рассмотрение возможностей применения предложенной классификации к типовым конфигурациям ПО СИ. Для них описаны принципы назначения уровней требований по жесткости испытаний, степени соответствия и уровню защиты.

Таблица 3

## Связь и влияние классификационных видов ПО СИ на определение требований к нему

<i>Классификационный вид</i>	<i>Требование</i>	<i>Примечание</i>
Аппаратное обеспечение	Жесткость испытаний Соответствие	Встроенное ПО является более защищенным и менее поддается модификации.
Критичность	Жесткость испытаний Уровень защиты	Уровень требований зависит от последствий искажения вносимых в результаты измерений.
Изменяемость	Соответствие	Возможности модификации ПО существенно зависят от его класса (доступности кода).
Функциональность	Жесткость испытаний	Источники погрешностей вносимых ПО зависят от реализуемых им функций.



Основным способом назначения уровней требований конкретным видам ПО является экспертный метод. Пример применения такого подхода приведен в таблице 4.

Таблица 4

Аппаратное обеспечение	Критичность	Изменяемость	Функция	Характеристики испытаний			
				Жесткость испытаний	Степень защиты	Уровень соответствия	
Встроенное ПО	Низкая	Коммерческое	Сбор, передача, хранение	низкая	низкая	низкий	
			Обработка	низкая	низкая	низкий	
		Модифицируемое	Сбор, передача, хранение	низкая	низкая	низкий	
			Обработка	низкая	Низкая	средний	
	Средняя	Коммерческое	Сбор, передача, хранение	средняя	Низкая	низкий	
			Обработка	средняя	средняя	низкий	
		Модифицируемое	Сбор, передача, хранение	средняя	низкая	средний	
			Обработка	средняя	средняя	средний	
	Высокая	Коммерческое	Сбор, передача, хранение	средняя	средняя	средняя	
			Обработка	высокая	высокая	средняя	
		Модифицируемое	Сбор, передача, хранение	высокая	средняя	высокий	
			Обработка	высокая	высокая	высокий	
Автономное ПО	Низкая	Коммерческое	Сбор, передача, хранение	низкая	низкая	низкий	
			Обработка	средняя	низкая	низкий	
		Целевое	Сбор, передача, хранение	низкая	низкая	низкий	
			Обработка	средняя	низкая	низкий	
		Модифицируемое	Сбор, передача, хранение	низкая	низкая	низкий	
			Обработка	средняя	Низкая	средний	
	Средняя	Коммерческое	Сбор, передача, хранение	низкая	Средняя	низкий	
			Обработка	средняя	Средняя	низкий	
		Целевое	Сбор, передача, хранение	средняя	Средняя	низкий	
			Обработка	средняя	Средняя	низкий	
		Модифицируемое	Сбор, передача, хранение	низкая	Средняя	средний	
			Обработка	средняя	Средняя	средний	
		Высокая	Коммерческое	Сбор, передача, хранение	средняя	средняя	средний
				Обработка	высокая	высокая	средний
	Целевое		Сбор, передача, хранение	высокая	средняя	средний	
			Обработка	высокая	высокая	Средний	
Модифицируемое	Сбор, передача, хранение		высокая	средняя	Высокий		
	Обработка		высокая	высокая	Высокий		

На рис. 2 схематично отображен процесс применения схемы классификации ПО СИ к установление требований к ПО СИ.



Рис. 2

Таким образом, в главе 2 решена задача установления уровней требований к ПО СИ различных видов. Далее необходимо детализировать требования к отдельным характеристикам ПО и методам его документирования.

В главе 3 предлагается подход к детализации требований к различным структурным элементам ПО СИ на различных этапах его жизненного цикла (разработка, применение, модификация). Среди общих принципов разработки ПО можно выделить такие как полнота, недвусмысленность, осуществимость, необходимость, корректность, проверяемость, согласованность и др.

С учетом предложенной в главе 2 классификации и указанных общих принципов ПО можно сформулировать набор требований, которые необходимо учитывать при разработке и эксплуатации ПО СИ (таблица 4).

Таблица 5

## Общие требования к программному обеспечению средств измерений

№№ п/п	Содержание требования	Учитываемые общие принципы	Пример реализации требований при разработке
<b>Этап разработки</b>			
1. Требование к документации			
1.1	ПО, представляемое для испытаний (аттестации), должно сопровождаться документацией в соответствии с установленными требованиями.	полнота, недвусмысленность	Перечень специальной документации, представляемой на аттестацию
2. Требования к структуре			
2.1	ПО разрабатывается таким образом, чтобы оно не было подвержено недопустимому влиянию со стороны другого ПО.	проверяемость, согласованность	Реализация защитного (внутреннего) интерфейса, охватывающего законодательно контролируемые части ПО
2.2	ПО, подлежащее метрологическому контролю, разрабатывается таким образом, чтобы на него невозможно было оказать недопустимое воздействие через интерфейсы пользователя и другие интерфейсы.	Необходимость, согласованность	Интерпретатор команд, фильтрация поступающих команд через программные и аппаратные интерфейсы
<b>Этап испытаний</b>			
3. Требования к соответствию ПО утвержденному типу (идентификация)			
3.1	После утверждения (аттестации*) ПО, подлежащее метрологическому контролю, не должно изменяться. Для каждого СИ используется ПО, идентичное утвержденному.	необходимость, проверяемость	Алгоритм версии ПО
3.2	Для проверки соответствия ПО утвержденному типу, а также для подтверждения его целостности и подлинности осуществляется идентификация ПО.	Осуществимость, проверяемость	Алгоритм идентификации
4. Требование к погрешности, вносимой ПО			
4.1	Погрешность, вносимая ПО, оценивается в ходе испытаний (аттестации), а ее значение не должно превышать пределов, установленных нормативной документацией или техническими требованиями.	Корректность	Применение стабильных алгоритмов с повышенной точностью вычислений
<b>Этап применения</b>			
5. Требования к защите			
5.1	ПО СИ содержит средства обнаружения, обозначения и/или устранения сбоев (функциональных дефектов) и искажений, которые нарушают целостность результатов измерений.	проверяемость, корректность	Программные методы избыточности, журнал событий, контрольная сумма
5.2	Осуществляется защита ПО от случайных или непреднамеренных изменений. Изменения ПО и данных становятся очевидными за короткий интервал времени.	необходимость, корректность	Программные средства фильтрации вводимых данных, контрольная сумма

\* Под аттестацией понимается исследование (тестирование) программного обеспечения средств измерений с целью определения и/или оценки его характеристик и установления их соответствия предъявляемым к ним требованиям с последующей регистрацией полученных результатов исследования в свидетельстве об аттестации (с указанием использованных методов исследования).

Набор способов реализации перечисленных в таблице требований зависит от классификационных признаков ПО СИ. В частности, например, реализации алгоритма идентификации

ции ПО будет зависеть от класса его модифицируемости, реализация защитного интерфейса от класса его критичности и др.

В главе 3 решена задача детализации требований и выбора подходов к их реализации на различных этапах жизненного цикла ПО СИ. Полученные в главе результаты реализованы в виде рекомендации МИ 2891-2004. Методы реализации требований, изложенных в главе 3 не затрагивают вопросов оценки погрешности вносимой ПО в результаты измерений. Более подробно методы оценки соответствия ПО установленным требованиям, включая погрешность вносимую ПО в результаты измерений рассмотрены в главе 4.

Глава 4 диссертации посвящена исследованию и разработке методики оценки соответствия ПО СИ требованиям, предъявляемым к нему.

Проведено исследование существующих подходов и методов испытаний, на основе международных и отечественных руководств, рекомендаций, публикаций по проблеме. В частности, исследованы, применительно к аттестации ПО СИ, методы «черного» и «белого» ящиков (функционального и структурного тестирования соответственно), оценки защищенности ПО, проверки его соответствия утвержденной версии (идентификация). Большое внимание уделено методам оценки погрешности, вносимой ПО при обработке данных.

В рамках разработки системы метрологической аттестации ПО СИ предложен организационный порядок ее проведения (рис. 3), который представлен следующими основными этапами:

- регистрация, анализ и принятие решения по заявке на аттестацию;
- оформление договора на проведение работ по аттестации, определение комиссии экспертов;
- экспертиза ПО;
- проведение испытаний (тестирования) ПО;
- принятие решения о выдаче свидетельства об аттестации;
- выдача свидетельства об аттестации.

Из указанных этапов аттестации ПО СИ основными являются экспертиза и непосредственное проведение испытаний ПО СИ.

Целью экспертизы ПО СИ является его анализ, подготовка данных, необходимых для проведения работ по испытаниям (тестированию), а также перечень требований предъявляемых к данному ПО.

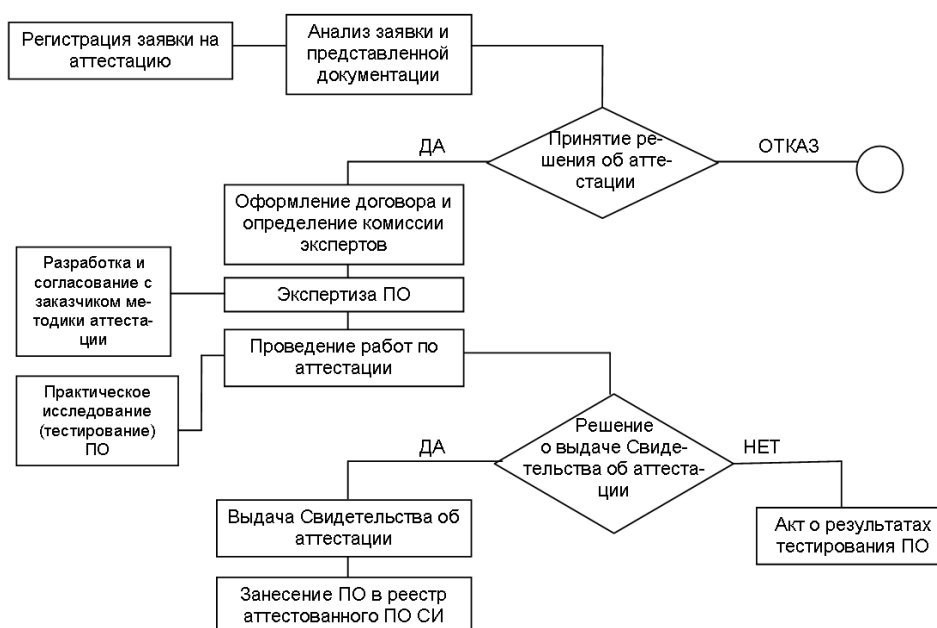


Рис. 3

Экспертиза ПО СИ представлена следующей последовательностью работ (рис. 4):

- Анализ представленной документации и копии ПО;
- Классификация ПО;
- Исследование структуры ПО (например, разделение ПО);
- Составление спецификации ПО;
- Разработка требований к ПО;
- Определение методов испытаний.



Рис. 4

Результатом экспертизы ПО СИ перечень требований, предъявляемых ПО, а также определенные методы испытаний. На основе результатов экспертизы ПО СИ может быть разработана методика его аттестации.

В работе определена типовая структура методики метрологической аттестации. Ее основными этапами является:

- Проверка документации
- Проверка структуры
- Проверка соответствия (идентификация)
- Оценка погрешности программного обеспечения
- Проверка защиты программного обеспечения

Кроме этого, методика проведения испытаний ПО СИ, характеризуется следующими этапами (рис. 5):

- разработка тестовых заданий в соответствии с требованиями к ПО и с указанием контролируемых параметров, исходных данных и эталонных значений (критериев);
- проведение испытаний и получение результатов функционирования испытываемого ПО при подготовленных тестовых заданиях;
- обработка результатов испытаний (сравнение тестируемых и эталонных результатов) и принятие решения о соответствии испытываемого ПО требованиям.

При этом подразумевается использование данных и результатов, полученных на этапе экспертизы ПО СИ.

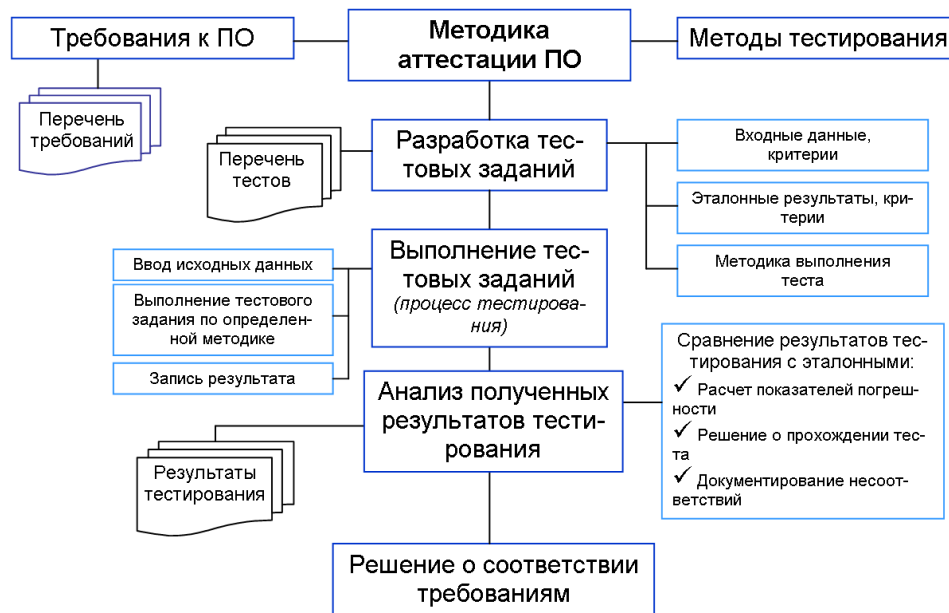


Рис. 5

Важной частью типовой методики аттестации ПО СИ является предложенные методы испытаний, среди которых можно выделить ряд методов, направленных на оценку погрешности, вносимой ПО в результаты измерений при обработке данных.

Методы оценки погрешности ПО изложены в ряде монографических работ, например Ronald F. Boisvert "The Quality of Numerical Software", F. Chaitin-Chatelin, E. Traviesas "Precise and the reliability of Numerical Software" и многих других, а также методических документов, в частности отчетов NPL по оценке численной точности электронных таблиц, некоторых математических алгоритмов и др., а также МИ 2174-91, МИ 2517-99, МИ 2518-99. Указанные методы основываются на применении моделей исходных данных (МИ 2174) и/или генерации эталонных наборов данных. При этом различают два основных подхода к методике оценки вносимой погрешности (рис. 6 и 7), которые представляют методы, основанные на применении эталонного ПО и методы, основанные на генерации эталонных данных.

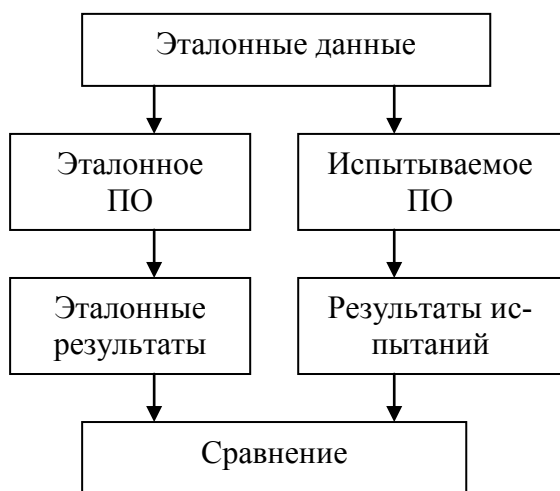


Рис.6

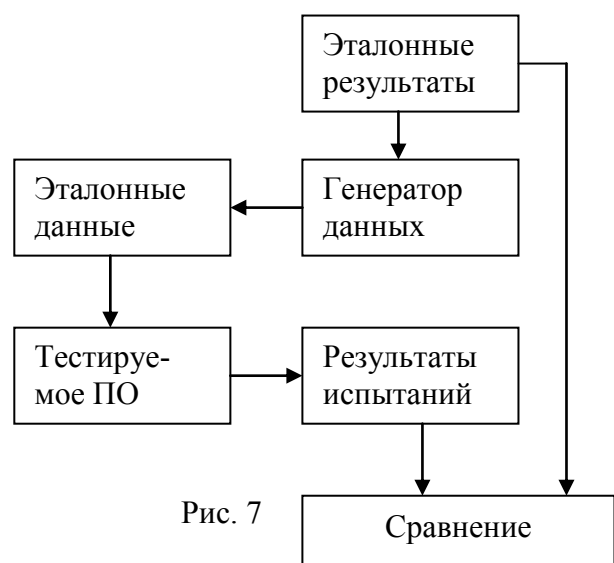


Рис. 7

Основными этапами предложенной методики являются:

- построение математической модели (спецификации) реализованных в ПО расчетных алгоритмов;
- определение программно-аппаратных особенностей интерфейса ввода исходных данных;
- определение характеристик эталонных наборов данных (эталонных пар);
- получение или генерация эталонных данных;
- применение эталонных данных (тестирование ПО) и расчет показателей его точности;
- обработка и представление результатов.

Ключевым моментом в оценке погрешности, вносимой ПО СИ в результаты измерений при их обработке является получения или генерация эталонных данных.

В качестве метода оценки вносимой ПО погрешности рассмотрен метод сравнительного испытания с применением “эталонного” ПО, в качестве которого может быть использовано аттестованное ПО (например, некоторые пакеты коммерческого ПО), а также возможна разработка “эталонного” ПО при необходимости. Рассмотрены существующие библиотеки “эталонных” алгоритмов данных, поддерживаемые некоторыми зарубежными метрологическими институтами, например NPL, NIST.

На основе научных отчетов NPL исследован метод нуль-пространства для генерации эталонных данных. Метод нуль - пространства используется в публикациях NPL и NIST для генерации семейств или классов “эталонных данных” и может быть применен для генерации к широкому ряду задач по подбору эмпирических кривых (fitting problems) и задач оптимизации, например для линейной регрессии. При линейной зависимости  $\bar{y}$  от параметров  $\bar{b}$  искомая функция может быть записана как

$$y_i = b_1 + b_2 x_i + r_i \text{ или в векторном виде } \bar{y} = A\bar{b} + \bar{r}$$

где  $A$  - матрица наблюдений,  $\bar{b}$  - параметры функции,  $\bar{r}$  - вектор остатков (случайная величина) имеют вид:

$$A = \begin{pmatrix} 1 & x_1 \\ 1 & x_2 \\ \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \\ 1 & x_m \end{pmatrix}, \bar{y} = \begin{pmatrix} y_1 \\ y_2 \\ \cdot \\ \cdot \\ \cdot \\ y_m \end{pmatrix}, \bar{b} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}, \bar{r} = \begin{pmatrix} r_1 \\ r_2 \\ \cdot \\ \cdot \\ \cdot \\ r_m \end{pmatrix}$$

Задача заключается в построении такого набора “эталонных”  $\bar{y}$ , который имитировал бы экспериментальные данные при тестировании программных продуктов, реализующих метод наименьших квадратов (МНК) и эта задача решается методом нуль – пространства.

Решение задачи простой линейной регрессии МНК требует, чтобы выполнялось условие

$$A^T \bar{r} = 0 \quad (1),$$

где  $A^T$  - матрица, транспонированная по отношению к матрице  $A$ .

В свою очередь это условие (1) эквивалентно выполнению двух условий

$$\begin{aligned} \sum_{i=1}^m r_i &= 0, \\ \sum_{i=1}^m x_i r_i &= 0. \end{aligned} \quad (2)$$

Пусть теперь  $N$  будет базисом в нуль – пространстве матрицы  $A^T$ , т.е.

$$A^T N = 0 \quad (3)$$

Этот базис может быть выражен как набор линейно независимых векторов, которые и образуют матрицу  $N$ . Если известен базис нуль – пространства, то вектор  $\vec{r}$  может быть представлен в виде линейной комбинации базисных векторов, т.е.  $\vec{r} = N \cdot \vec{u}$ , где вектор  $\vec{u}$  представляет коэффициенты этой линейной комбинации. Замечательной особенностью рассматриваемого метода является то, что замена вектора  $\vec{y}$  на  $\vec{y} + \vec{r}$ , оставляет неизменным решение  $\vec{b}$  линейной регрессионной задачи:

$$A^T (\vec{y} + \vec{r}) = A^T \vec{y} + A^T \vec{r} = A^T \vec{y} + A^T N \cdot \vec{u} = A^T \vec{y},$$

т.е. ничего не меняется по сравнению со случаем, когда остаточного члена не было. Из написанного соотношения следует, что, построив один набор данных  $\vec{y}$ , выбором вектора  $\vec{u}$  можно построить множество наборов данных, имеющих одно и тоже решение линейной регрессионной задачи  $\vec{b}$ . Обычно векторы  $\vec{u}$  выбираются в виде набора случайных чисел, имитирующих измеренные данные.

Таким образом, процедура генерации эталонных данных в общих чертах состоит из последовательности следующих действий:

1. Предполагая строгую линейную зависимость (линейную модель) откликов системы на входные воздействия строится модельный вектор наблюдений  $\vec{y}_0 = A\vec{b}$ , где индексом «0» обозначены эталонные (модельные) результаты, являющиеся «входом» для генерации эталонных данных.
2. С помощью программной функции строится базис  $N$  нуль – пространства матрицы  $A^T$ .
3. С помощью соотношения  $\vec{r} = N \cdot \vec{u}$  строится вектор остатков, при этом компоненты вектора  $\vec{u}$  выбираются в виде случайных чисел, имитирующих ошибки измерений. Часто вектор  $\vec{r}$  необходимо видоизменять (масштабировать) таким образом, чтобы он представлял распределение случайных чисел с заданными средним значением и СКО.
4. По формуле  $\vec{y} = \vec{y}_0 + \vec{r}$  образуется вектор наблюдений, представляющий собой сгенерированные эталонные данные.

По результатам исследования программно реализован ряд алгоритмов генерации эталонных данных. Полученное программное обеспечение позволяет задавать параметры генерации и генерировать наборы эталонных данных различной сложности.

Кроме методики оценки погрешности вносимой ПО СИ в результаты измерений, и в целях их применения при метрологической аттестации ПО СИ, исследованы общие методы установления соответствия ПО СИ его спецификации и методы функционального тестирования, а также методы испытаний защищенности ПО СИ.

К методам установления соответствия ПО СИ его спецификации и методам функционального тестирования относятся методы определения:

- полноты и корректности документации;
- согласованности интерфейса ПО его спецификации;
- полноты и корректности решения функциональных задач;
- корректности функционирования при различных условиях, характеризующихся различной внешней программной средой, диапазонами и граничными значениями данных, действиями пользователя и т.д.

Методология испытаний защищенности предложена с учетом анализа положений руководящих документов Гостехкомиссии России при Президенте РФ по защите от несанкционированного доступа к информации.



Основными этапами при проверке защищенности ПО СИ являются:

- анализ документации ПО СИ с целью определения примененных разработчиками средств защиты ПО и данных;
- анализ рисков при использовании ПО СИ;
- анализ конфигурации системы с целью выявления потенциальных угроз защищенности и определение необходимых требований по защите;
- практические испытания защищенности путем эмуляции действий потенциального злоумышленника и программно-аппаратных сбоев;
- сопоставление требований по защите и реализованных механизмов защиты с целью определения их достаточности. На основании этого сравнения принимается решение о соответствии требованиям защиты.

Полученные результаты реализованы при разработке МИ 2955-2005 "Типовая методика аттестации ПО СИ и порядок ее проведения".

Таким образом, разработанные документы (МИ 2891 и МИ 2955), содержащие общие требования к ПО СИ, а также типовую методику его аттестации являются важнейшими и необходимыми составляющими системы метрологической аттестации ПО СИ.

Разработанные научно-методические основы метрологической аттестации ПО СИ, а именно классификация, требования и методика аттестации ПО СИ нашли свое применение в практике работ по испытаниям ряда программных продуктов, проведенная работа по которым рассмотрена в главе 5.

*Глава 5* диссертации посвящена практике метрологической аттестации ПО СИ.

Апробация результатов работы проведена на примере аттестации следующего ПО:

- Программы QD3 - ПО калибраторов семейства Veamex QCAL;
- Программы "Труба" - Программного обеспечения по расчету вместимости технологических трубопроводов;
- коммерческих пакетов математического ПО: Microsoft Excel 2002, MathSoft MathCad 11 и MathWorks Matlab 6.5 (Release 13).

Для всех указанных программ в соответствии с разработанной классификацией были определены уровни требований и разработаны методики аттестации.

При испытаниях указанных пакетов коммерческого математического ПО было применено разработанное программное обеспечение генерации наборов эталонных данных в среде Matlab.

Испытания программы "Труба" проводились с помощью применения метода "эталонного" ПО.

При испытаниях пакетов математического ПО и программы "Труба" выявлена и оценена погрешность вносимая указанным ПО при обработке данных. Таким образом разработанные методы доказали свою применимость и эффективность при аттестации ПО СИ.

В заключении сформулированы основные научные и практические результаты, полученные в работе:

1. Исследованы особенности ПО СИ, исследованы и классифицированы источники ошибок, влияющих на результаты измерений, связанных с применением ПО СИ. В результате исследования получена система метрологических показателей ПО СИ.
2. Разработана классификация ПО СИ, применяемая при установлении требований к различным видам ПО СИ.
3. Разработана система требований к ПО СИ по каждому из выделенных его показателей. Разработан подход к установлению требований к различным видам ПО СИ
4. Исследованы математические методы, используемые при оценке погрешности, вносимой ПО в результаты измерений и программно реализован ряд алгоритмов генера-

- ции наборов эталонных данных, применяемых для при указанной оценке погрешности.
5. Разработанные основы системы метрологической аттестации ПО СИ реализованы в виде рекомендаций МИ 2891-04 “Общие требования к программному обеспечению средств измерений” и МИ 2955-2005 “Типовая методика аттестации программного обеспечения средств измерений и порядок ее проведения”.
  6. Разработанные требования и методы аттестации ПО СИ внедрены в практику путем проведения испытаний ряда программных продуктов.

Основное содержание диссертации опубликовано в следующих работах:

1. Ю.А. Кудеяров, Ю.Е. Лукашов, А.А. Сатановский. Требования к программному обеспечению средств измерений на основе зарубежных и отечественных стандартов и рекомендаций, “Законодательная и прикладная метрология”, № 4, 2003 г.;
2. Ю.А. Кудеяров, Ю.Е. Лукашов, А.А. Сатановский. Метрологическая аттестация программного обеспечения средств измерений (состояние и перспективы), “Законодательная и прикладная метрология”, № 5, 2003г.;
3. Ю.А. Кудеяров, А.А. Сатановский. Генерация эталонных данных методом нуль-пространства для тестирования электронных таблиц, прикладных математических пакетов и алгоритмов, “Законодательная и прикладная метрология”, № 2, 2005 г.;
4. Ю.Е. Лукашов, А.А. Сатановский. Классификация программного обеспечения средств измерений, “Законодательная и прикладная метрология”, № 2, 2006 г.
5. НИР 06.01.03.05. Исследование и разработка направлений развития системы поверки средств измерений в стране (Этап 2. Разработка рекомендация по метрологической аттестации программного обеспечения, входящего в состав поверки средств измерений).
6. МИ 2891-2004 "Общие требования к программному обеспечению средств измерений"
7. МИ 2955-2005 " Типовая методика аттестации программного обеспечения средств измерений и порядок ее проведения ".