ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ
ВСЕРОССИЙСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
МЕТРОЛОГИЧЕСКОЙ СЛУЖБЫ (ФГУП ВНИИМС)

РЕКОМЕНДАЦИЯ

ГОСУДАРСТВЕННАЯ СИСТЕМА ОБЕСПЕЧЕНИЯ ЕДИНСТВА ИЗМЕРЕНИЙ

ОБЩИЕ ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ СРЕДСТВ ИЗМЕРЕНИЙ

МИ 2891 - 2004

Москва
2004

ПРЕДИСЛОВИЕ

РАЗРАБОТАНА ФГУП ВНИИМС Федерального агентства по техническому регулированию и метрологии

ИСПОЛНИТЕЛИ Ю.Е. Лукашов, к.т.н. (руководитель темы), Ю.А. Кудеяров, д.ф.-м.н., А.А. Сатановский

УТВЕРЖДЕНА ФГУП ВНИИМС 07 декабря 2004 г.

ЗАРЕГИСТРИРОВАНА ФГУП ВНИИМС Федерального агентства по техническому регулированию и метрологии 07 декабря 2004 г.

ВВЕДЕНА впервые

СОДЕРЖАНИЕ

ГОСУДАРСТВЕННАЯ СИСТЕМА ОБЕСПЕЧЕНИЯ ЕДИНСТВА ИЗМЕРЕНИЙ. **ОБЩИЕ ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ СРЕДСТВ ИЗМЕРЕНИЙ.**	**МИ 2891 - 2004**

1. ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1 Настоящая Рекомендация устанавливает общие требования к программному обеспечению (ПО) средств измерений (СИ) и применяются при его разработке, испытаниях СИ с целью утверждения типа и идентификации (в том числе периодической).

1.2 Требования данной Рекомендации предъявляются к ПО следующих видов:
- ПО, являющемуся частью измерительной системы и функционирующему на базе персонального компьютера;
- ПО, являющемуся самостоятельным программным продуктом, который может применяться для сбора, обработки, хранения и представления измерительной информации;
- ПО, являющемуся неотъемлемой частью СИ (встроенному ПО);
- ПО для контроллеров и вычислительных блоков.

2. НОРМАТИВНЫЕ ССЫЛКИ

В настоящей Рекомендации использованы положения и рекомендации следующих документов:

ПР 50.2.009-94 ГСИ. Порядок проведения испытаний и утверждения типа средств измерений.

ГОСТ Р 8.596-2002 ГСИ. Метрологическое обеспечение измерительных систем. Основные положения.

ГОСТ Р ИСО/МЭК 17025-2000. Общие требования к компетентности испытательных и калибровочных лабораторий.

ГОСТ Р ИСО/МЭК 12119-2000. Информационная технология. Пакеты программ. Требования к качеству и тестирование.

ГОСТ Р ИСО 9127-94. Системы обработки информации. Документация пользователя и информация на упаковке для потребительских программных пакетов.

ГОСТ Р 34.11-94 Информационная технология. Криптографическая защита информации. Функция хэширования.

ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

Директива Европейского Союза 2004/22/ЕС по измерительным приборам.

Рекомендация OIML R76. Неавтоматические взвешивающие приборы.

Рекомендация OIML D-SW 0.11 Общие требования к программному обеспечению измерительных приборов.

Руководство WELMEC 7.1. Требования к программному обеспечению на основе Директивы по измерительным приборам.

Рекомендация КООМЕТ R/LM/10:2004 Программное обеспечение средств измерений. Общие технические требования.

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1 Данный документ устанавливает требования к метрологическому контролю ПО СИ в форме общих требований к документации ПО, его структуре, его идентичности ПО, аттестованному при испытаниях с целью утверждения типа, вносимой погрешности и защите.

3.2 Рекомендация предназначена для использования в организациях, осуществляющих разработку ПО СИ, проводящих испытания СИ с целью утверждения типа, испытания (аттестацию) ПО, а также использующих ПО для сбора, обработки, хранения и представления измерительной информации

3.3 Испытания (аттестацию) ПО выполняют Государственные центры испытаний средств измерений (ГЦИ СИ), уполномоченные федеральным органом исполнительной власти, осуществляющим функции оказания государственных услуг в сфере технического регулирования и метрологии, на проведение испытаний СИ для целей утверждения типа, а также органы системы сертификации ПО СИ. К испытаниям (аттестации) могут привлекаться специалисты организаций, занимающихся разработкой ПО.

4. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Программное обеспечение средств измерений – компьютерная программа или совокупность программ сбора, передачи, обработки, хранения и представления измерительной информации, а также программные документы, необходимые для функционирования этих программ.

Данные – измерительная информация, представленная в виде, пригодном для передачи, интерпретации или обработки.

Разделение программного обеспечения – выделение (описание) в ПО СИ, попадающих в сферу государственного метрологического контроля и надзора (ГМКиН), функций и частей, подлежащих метрологическому контролю.

Интерфейс – общая граница между двумя блоками с различными характеристиками, относящимися к функциям, физическим соединениям и обмену сигналами.

Интерфейс пользователя – интерфейс, обеспечивающий возможность обмена информацией между пользователем и компонентами технических или программных средств системы обработки информации.

Защищенный интерфейс – интерфейс является защищенным:

- если только через этот интерфейс может быть пропущен или изменен определенный набор параметров, данных и функций программной части;
- если через него невозможно ввести в ПО команды или данные, которые нечетко определены и могут быть ошибочно приняты за результат измерения, а также команды, которые могут быть использованы для искажения отображаемых, обработанных и сохраненных результатов измерения или других контролируемых данных, либо для несанкционированной корректировки или изменения настроек ПО.

Недопустимые изменения программного обеспечения – изменения ПО или его частей, подлежащих метрологическому контролю;

Утвержденное ПО – ПО средств измерений, прошедших испытания с целью утверждения типа, и аттестованное в процессе этих испытаний.

Защищенное программное обеспечение и данные - ПО и данные, изменение которых или невозможно, или обнаруживается и становится очевидным при запуске или работе.

Идентификация программного обеспечения - проверка и подтверждение целостности и подлинности ПО.

Целостность программного обеспечения и данных - состояние ПО и данных, характеризующееся отсутствием изменений преднамеренного или случайного характера.

Подлинность данных – состояние данных, происхождение которых может быть проверено, и которые могут быть однозначно приписаны определенным измерениям.

Контрольная сумма - суммирование 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 (ГОСТ Р 34.11-94).

Хэш-код – результат арифметической комбинации со всеми байтами программного кода или набора данных. Результат алгоритма хеширования включает только некоторые байты, а алгоритм построен таким образом таким образом, что любая модификация кода программы или данных с высокой вероятностью приводит к другому результату, т.е. к очевидности изменений.

Электронная подпись - электронная подпись для файла (кода программы или данных) генерируется в два этапа: сначала рассчитывается хэш-код и затем хэш-код шифруется (ГОСТ Р 34.10-2001). Электронная подпись обычно добавляется к коду программы или набору данных, по которым она была сгенерирована.

Погрешность, вносимая ПО – отличие результатов, полученных с помощью ПО, от результатов, полученных при тех же условиях эталонным ПО. Погрешность, вносимая ПО, может быть обусловлена неудачным выбором алгоритмов и их неустойчивостью, накоплением погрешности округления на промежуточных этапах вычислений, использованием при вычислениях конечных сумм вместо бесконечных рядов, программными сбоями и искажениями при передаче, обработке и представлении измерительной информации и т.п. Погрешность ПО может выражаться числом потерянных цифр точности по сравнению с эталонными результатами.

Эталонное ПО – программное обеспечение, отвечающее наивысшим требованиям к его точностным и функциональным характеристикам, подтвержденным (в ряде случаев независимыми методами) при его неоднократном тестировании и использовании.

5. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, ПОДЛЕЖАЩЕЕ МЕТРОЛОГИЧЕСКОМУ КОНТРОЛЮ

5.1 Общие положения

5.1.1 В структуре ПО СИ, попадающих в сферу ГМКиН, описываются (выделяются) все программные модули, подпрограммы, процедуры и т.д., реализующие функции ПО СИ, подлежащие метрологическому контролю, т.е. проводится разделение ПО на части, подлежащие метрологическому контролю, и не подлежащие контролю. Такое разделение предоставляет возможность модификации частей ПО, не подлежащих контролю, без нарушения требования соответствия ПО утвержденному типу.

5.1.2 Разработчики могут осуществлять разделение ПО на программном уровне, реализуя его в структуре программы.

5.1.3 Разделение ПО проводится разработчиками ПО СИ, попадающих в сферу ГМКиН. Такое разделение рекомендуется проводить всем разработчикам ПО СИ. Корректность разделения проверяется при аттестации ПО в процессе испытаний СИ с целью утверждения типа.

5.2 Методы разделения

Используются два метода разделения ПО:

- *Разделение ПО на «низком» уровне* – разделение в рамках программы, т.е. разделение на уровне языка программирования (например, инкапсуляция[*] в объектно-ориентированном программировании).
- *Разделение ПО на «высоком» уровне* – разделение на уровне операционной системы. Это означает, что только определенные программы или библиотеки (например, DLL – “Dynamic Link Libraries” в Windows) выполняют подлежащие контролю функции.

5.3 Реализация разделения

5.3.1 Как в случае разделения на «низком» уровне, так и на «высоком» уровне метрологическому контролю подлежат все части программы (подпрограммы, процедуры, функции, классы, переменные и т.д.), которые используются при обработке результатов измерений или влияют на них, или используются в таких вспомогательных функциях, как отображение, защита, хранение и передача данных, идентификация ПО.

5.3.2 Другие части программы, переменные или параметры (например, подпрограммы, библиотеки, процедуры взаимодействия с операционной средой и периферийными устройствами ПК (кроме СИ)) не являются контролируемыми. Модификация этих частей разрешается без уведомления ГЦИ СИ и органов сертификации ПО.

[*] Инкапсуляция (encapsulation) - механизм, объединяющий в элементе языка программирования (объекте) данные и код, оперирующий этими данными.

6. ОБЩИЕ ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ СРЕДСТВ ИЗМЕРЕНИЙ.

Общие требования предъявляются к ПО указанных в п.1.2 видов и приведены в таблице 1.

Таблица 1

№№ п/п	Содержание требования	Пункт Рекомендации с пояснениями требований
1. Документация		
1.1	ПО, представляемое для испытаний (аттестации), должно сопровождаться документацией в соответствии с требованиями данной Рекомендации.	6.1
2. Структура		
2.1	ПО разрабатывается таким образом, чтобы оно не было подвержено недопустимому влиянию со стороны другого ПО.	6.2.1
2.2	ПО, подлежащее метрологическому контролю, разрабатывается таким образом, чтобы на него невозможно было оказать недопустимое воздействие через интерфейсы пользователя и другие интерфейсы.	6.2.2
3. Соответствие ПО утвержденному типу (идентификация)		
3.1	После утверждения (аттестации) ПО, подлежащее метрологическому контролю, не должно изменяться. Для каждого СИ используется ПО, идентичное утвержденному.	6.3.1
3.2	Для проверки соответствия ПО утвержденному типу, а также для подтверждения его целостности и подлинности осуществляется идентификация ПО.	6.3.2
4. Погрешность, вносимая ПО		
4.1	Погрешность, вносимая ПО, оценивается в ходе испытаний (аттестации), а ее значение не должно превышать пределов, установленных нормативной документацией или техническими требованиями.	6.4
5. Защита		
5.1	ПО СИ содержит средства обнаружения, обозначения и/или устранения сбоев (функциональных дефектов) и искажений, которые нарушают целостность результатов измерений.	6.5.1
5.2	Осуществляется защита ПО от случайных или непреднамеренных изменений. Изменения ПО и данных становятся очевидными за короткий интервал времени.	6.5.2

6.1 ДОКУМЕНТАЦИЯ

6.1.1 ПО, представляемое для испытаний (аттестации), должно сопровождаться документацией в соответствии с требованиями данной Рекомендации.

6.1.2 Набор документов, сопровождающих ПО, включает:

- описание структуры ПО и выполняемых функций, в том числе последовательность обработки данных;
- описание функций и параметров ПО, подлежащих метрологическому контролю;
- описание реализованных в ПО расчетных алгоритмов, а также их блок-схемы;
- описание модулей ПО;
- перечень интерфейсов и перечень команд для каждого интерфейса, включая заявление об их полноте;
- список, значение и действие всех команд, получаемых от клавиатуры, мыши и других устройств ввода;
- описание реализованной методики идентификации ПО;
- описание реализованных методов защиты ПО и данных;
- описание интерфейсов пользователя, всех меню и диалогов;
- описание хранимых или передаваемых наборов данных;
- руководство пользователя;
- характеристики требуемых системных и аппаратных средств, если эта информация не приведена в руководстве пользователя.

6.1.3 Перечень документов, сопровождающих ПО, может корректироваться соглашением между исполнителем и заказчиком испытаний (аттестации) ПО.

6.1.4 Графическая и текстовая информация в документации выполняется таким образом, чтобы она была пригодна для полного и однозначного понимания.

6.2 СТРУКТУРА

6.2.1 Разделение программного обеспечения

6.2.1.1 ПО, подлежащее метрологическому контролю, разрабатывается так, чтобы оно не было подвержено недопустимому влиянию со стороны другого ПО.

Примечание:
Под другим ПО понимается ПО, работающее совместно с ПО, подлежащим метрологическому контролю (связанное ПО), например, различные модули в рамках одного программного комплекса, или части ПО, не подлежащие проверке (подпрограммы, процедуры и т.д.). Вопросы влияния программ, не входящих в состав утвержденного ПО, рассматриваются в соответствии с требованием 6.5.2.

6.2.1.2 В структуре ПО выделяются (описываются) части, осуществляющие функции, подлежащие метрологическому контролю, и части, осуществляющие функции, которые метрологическому контролю не подлежат, т.е. выполняется разделение ПО, в соответствии с п.5. Связь между этими частями ПО осуществляется через защищенный программный интерфейс.

6.2.1.3 Разделение ПО проводится как по отношению к программному продукту, так и к данным.

6.2.1.4 Отсутствует доступ к переменным величинам контролируемых частей ПО из частей ПО, не подлежащих контролю, т.е. реализуется защита на уровне языка программирования (инкапсуляция).

6.2.1.5 Измерительная информация (результаты измерений) поступает только в части

ПО, подлежащие метрологическому контролю. Передача результатов измерений в части ПО, не подлежащие контролю, может осуществляться только после их окончательной обработки контролируемыми частями ПО.

6.2.5.6 В случае модификации не подлежащих контролю частей ПО его разделение сохраняется.

6.2.2 Интерфейсы программного обеспечения

6.2.2.1 ПО, подлежащее метрологическому контролю, разрабатывается таким образом, чтобы на него невозможно было оказать недопустимое воздействие через интерфейсы ПО или другие интерфейсы. Команды, полученные через интерфейсы ПО или другие интерфейсы, влияют на функции и данные ПО только так, как это описано в документации.

6.2.2.2 Не допускается внесение изменений и искажение результатов измерений через интерфейсы ПО, т.е. программные интерфейсы должен быть защищенными.

Примечание:
Для реализации защищенного интерфейса может использоваться интерпретатор команд, осуществляющий фильтрацию вводимых команд и данных. Недопустимые команды и данные не оказывают воздействия на измерительную информацию

6.2.2.3 В документации ПО описывается предназначение и действие всех команд интерфейсов ПО или других интерфейсов.

Примечание:
При отсутствии интерфейса для ввода команд в ПО данное требование не применяется.

6.3 СООТВЕТСТВИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ УТВЕРЖДЕННОМУ ТИПУ (ИДЕНТИФИКАЦИЯ)

6.3.1 Целостность ПО и подлинность данных

6.3.1.1 После утверждения типа СИ, ПО этих СИ, подлежащее метрологическому контролю, не должно изменяться. Для каждого СИ используется ПО, идентичное утвержденному.

6.3.1.2 Не допускается нарушения разделения ПО, изменения программного интерфейса и частей, подлежащих метрологическому контролю. Изменение контролируемых частей ПО СИ приводит к нарушению результатов утверждения типа СИ и требует проведения нового испытания СИ и соответствующего ПО.

Примечания:
1. После утверждения типа СИ разработчик может изменять части ПО, не подлежащие контролю, однако, необходимо соблюдение требования 5.3.1.
2. В случае изменений частей, не подлежащих контролю, вносятся соответствующие изменения в документацию ПО.

6.3.1.3 Для СИ, прошедших испытания с целью утверждения типа, используется только утвержденное ПО.

Примечания:
1. Интерфейс пользователя ПО СИ, относящегося к сфере ГМКиН, отчеты о результатах измерений, файлы с данными содержат информацию об утверждении ПО и номер его версии;
2. Работа ПО возможна только после успешной процедуры его идентификации (см. п.6.3.2).

6.3.1.4 Не допускается нарушение разделения данных и изменения их частей, подлежащих метрологическому контролю. Целостность и подлинность данных

проверяется и подтверждается при испытаниях (аттестации) ПО путем их идентификации.

6.3.2 Идентификация программного обеспечения

6.3.2.1 Для проверки соответствия ПО утвержденному типу, а также для проверки и подтверждения целостности и подлинности ПО и данных, проводится идентификация ПО.

Примечание:

Технической реализацией метода подтверждения соответствия может являться номер версии ПО, который в соответствии с принципом разделения ПО должен состоять из двух частей. Первая часть отображает состояние частей ПО, подлежащих метрологическому контролю, и рассчитывается соответственно как контрольная сумма (CRC-16, CRC-32) или хэш-код (SHA-1, MD5 и т.д.) по контролируемым частям ПО. Вторая часть отображает состояние тех частей ПО, которые контролю не подлежат. Эту часть номера версии устанавливает разработчик. Любое изменение законодательно контролируемых частей ПО автоматически приводит к изменению первой части номера версии.

6.3.2.2 Алгоритм идентификации является частью ПО, подлежащей метрологическому контролю, и защищается. Идентификация осуществляется при запуске ПО, а также имеется возможность ее проведения по команде пользователя.

Примечание:

При идентификации не учитываются операционная система и драйверы низкого уровня, например видеодрайверы, драйверы принтера и т.д., но идентифицируются драйверы, обеспечивающие работу ПО вместе с СИ.

6.3.2.3 При любых изменениях в частях ПО, подлежащих метрологическому контролю, требуются его новое утверждение, при этом вносится новая программная идентификация.

6.3.2.4 При отсутствии разделения, идентификации подлежит все ПО.

6.4 ПОГРЕШНОСТЬ, ВНОСИМАЯ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ

6.4.1 Погрешность, вносимая ПО, оценивается в ходе испытаний (аттестации), а ее значение не должно превышать пределов, установленных нормативной документацией или техническими требованиями.

6.4.2. ПО, разработанное для функционирования в составе или совместно с СИ, оценивается на вносимую погрешность. При этом значения показателей погрешности устанавливаются индивидуального для каждого типа СИ, в состав которого входит ПО.

6.4.3 Оценка погрешности, вносимой ПО, производится по согласованным с заказчиком и исполнителем методикам (программам) испытаний (аттестации).

Примечания:

1. Универсальное ПО (например, электронные таблицы, математические и статистические программы), используемое для обработки результатов измерений, может считаться оцененным и соответствующим данному требованию. В этом случае не требуется оценивания вносимой погрешности, однако, следует проверять конфигурацию/модификацию используемого ПО.
2. Методы оценки погрешности, вносимой ПО, могут включать в себя:
   - разработку эталонного (высокоточного) ПО;
   - разработку (генерацию) эталонных наборов данных;
   - сличение ПО с утвержденным программным продуктом (эталонным ПО);
   - оценивание вносимой погрешности при использовании в качестве эталонного ПО универсальных программных пакетов.

6.5 ЗАЩИТА ПРОГРАММ И ДАННЫХ

6.5.1 Защита от сбоев

ПО, подлежащее метрологическому контролю, содержит средства обнаружения, обозначения и/или устранения сбоев (функциональных дефектов) и искажений, которые могут нарушить целостность результатов измерений.

Примечания:

1. В случае возникновения сбоя пользователь извещается об этом. Программа выдает предупреждение (визуальный и/или звуковой сигнал) о необходимости завершения работы до момента устранения сбоя.
2. В случае невозможности обозначения и/или устранения сбоя программа предусматривает ситуацию аварийного завершения работы с записью этого события при последующем запуске. Результаты работы программы, нарушенные сбоем, не должны использоваться далее.

6.5.2 Защита программного обеспечения и данных от изменений

6.5.2.1 Осуществляется защита ПО и данных, подлежащих метрологическому контролю, от случайных или непреднамеренных изменений. Изменения ПО и данных становятся очевидными за короткий интервал времени.

6.5.2.2 Для выполнения данного требования ПО и данные могут защищаться от изменений с помощью простых программных средств, например, с помощью текстового редактора.

Примечания:

1. Причинами случайных или непреднамеренных изменений являются в большинстве случаев ошибки обслуживания ПО и/или СИ.
2. Умышленные изменения ПО и/или СИ и данных с помощью специальных программных средств относятся к правонарушениям.

6.5.2.3 Данные (файлы), содержащие результаты измерений, защищаются от любых искажений.

Примечание:

Защита данных осуществляется с помощью электронной подписи или кодирования.

6.5.2.4 Осуществляется защита ПО, подлежащего метрологическому контролю, от любых изменений и влияния со стороны лиц, не имеющих допуск к работе с таким ПО (неавторизованных лиц). Перед началом работы с ПО пользователь получает соответствующий допуск к работе (проходит авторизацию).

Примечание:

При запуске программы у пользователя запрашивается его учетная запись (фамилия и пароль). В случае трех неудачных попыток ввода учетной записи программа закрывается и делается запись в специальный файл (log-файл) с идентификацией события (попытка неудачной авторизации), его даты и времени.

6.5.2.4 Осуществляется защита программного кода и параметров ПО, подлежащих метрологическому контролю.

Примечания:

1. Защита программного кода ПО, подлежащего метрологическому контролю, определена в соответствии с требованиями 6.5.2.1 и 6.5.2.2.
2. Защита параметров ПО осуществляется в соответствии с требованием 6.5.2.3, а также наличием в ПО счетчика или журнала событий, который содержит:

- информацию о любых изменениях в параметрах ПО (дата и время, информация о пользователе);
- все предыдущие конфигурации параметров ПО;

3. Журнал событий защищается в соответствии с п.п. 6.5.2.2.

7. УРОВНИ ТРЕБОВАНИЙ

Назначаются следующие уровни требований к ПО СИ по каждому виду требований: низкий, средний, высокий.

Назначение уровней производится ГЦИ СИ или органом, проводящим аттестацию ПО, по согласованию с заказчиками испытаний (аттестации) ПО.

При назначении уровней требований учитываются технические особенности СИ и их назначение, ввиду чего требования к ПО могут назначаться в различном объеме.

ПО СИ оценивается в соответствии с выбранными уровнями по:

- жесткости ***испытаний,***
- степени ***соответствия (идентификация),***
- уровню ***защиты.***

7.1 Жесткость испытаний программного обеспечения

Низкая:	Функции ПО проверяются в ходе обычных испытаний по утверждению типа СИ в соответствии с программой испытаний.
Средняя:	ПО испытывается на основании описания программных функций, предоставленных изготовителем. Оценивается влияние ПО на результаты измерений, средства идентификации и защиты.
Высокая:	В дополнение к обычным испытаниям по определению метрологических характеристик и правильности выполняемых функций проверяется исходный код ПО. Предметом испытаний исходного кода программы может являться, например, реализация алгоритма вычислений.

7.2 Степень соответствия программного обеспечения (идентификация)

Низкая:	Применяемое ПО каждого отдельного СИ находится в соответствии с утвержденным.
Средняя:	В дополнение к уровню соответствия «низкий», в отдельных случаях, обусловленных техническими особенностями, некоторые части ПО могут быть определены как «не подлежащие изменению» при утверждении типа. Части, не подлежащие изменению, идентичны утвержденному ПО в каждом СИ.
Высокая:	В каждом СИ используется ПО, полностью идентичное утвержденному.

7.3 Защита программного обеспечения

Низкая:	Не требуется специальной защиты контролируемого ПО и данных от недопустимых изменений.
Средняя:	ПО и данные, подлежащие метрологическому контролю, защищены от недопустимых изменений с использованием простых программных средств, например текстовых редакторов.
Высокая:	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.).

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ
ВСЕРОССИЙСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
МЕТРОЛОГИЧЕСКОЙ СЛУЖБЫ (ФГУП ВНИИМС)

УТВЕРЖДАЮ

Директор института

_____ С.А. Кононогов

«_____» _____ 2004 г.

РЕКОМЕНДАЦИЯ

ГОСУДАРСТВЕННАЯ СИСТЕМА ОБЕСПЕЧЕНИЯ ЕДИНСТВА ИЗМЕРЕНИЙ

ОБЩИЕ ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ СРЕДСТВ ИЗМЕРЕНИЙ

МИ 2891 - 2004

Москва
2004