

This Document is executed in Russian and in English. In case of any inconsistency, the Russian text shall prevail.

**FEDERAL AGENCY FOR TECHNICAL REGULATION AND
METROLOGY**



**METROLOGY
RECOMMENDATIONS**

**R 50.2.077—
2014**

State System for Ensuring the Uniformity of Measurements

MEASURING INSTRUMENT TYPE APPROVAL TESTING

Software protection check

Official edition

**Moscow
Standartinform
2014**

**ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ**



**РЕКОМЕНДАЦИИ ПО
МЕТРОЛОГИИ**

**R 50.2.077—
2014**

Государственная система обеспечения единства измерений

**ИСПЫТАНИЯ СРЕДСТВ ИЗМЕРЕНИЙ В ЦЕЛЯХ
УТВЕРЖДЕНИЯ ТИПА**

Проверка защиты программного обеспечения

Издание официальное

**Москва
Стандартинформ
2014 г.**

Foreword

1 DEVELOPED by the Federal State Unitary Enterprise “All-Russian Scientific and Research Institute of Metrological Service” (FGUP “VNIIMS”)

2 INTRODUCED by the Technical Committee for Standardization TK 53 “Basic Standards and Rules in the Field of Ensuring the Uniformity of Measurements”

3 APPROVED AND BROUGHT INTO EFFECT by the Order of the Federal Agency for Technical Regulation and Metrology as of December 4, 2014 No. 69-st

4 REPLACING R 50.2.077—2011

Rules for the application of the present Recommendations are specified in GOST R 1.0—2012 (Section 8). Information on amendments to the present Recommendations is published in the annual (as of January 1 of the current year) informative index “National Standards”, and the official text of the amendments and updates is published in the monthly informative index “National Standards”. In case of revision (replacement) or cancellation of the present Recommendations, the relevant notification shall be published in the upcoming issue of the monthly information index “National Standards”. The relevant information, notification and texts will also be available in the public information system – on the official web-site of the Federal Agency for Technical Regulation and Metrology on the Internet (gost.ru)

© Standartinform, 2014

The present Recommendations shall not be completely or partially reproduced, duplicated and distributed as an official edition without the permission of the Federal Agency for Technical Regulation and Metrology.

Предисловие

1 РАЗРАБОТАНЫ Федеральным государственным унитарным предприятием «Всероссийский научно-исследовательский институт метрологической службы» (ФГУП «ВНИИМС»)

2 ВНЕСЕНЫ Техническим комитетом по стандартизации ТК 53 «Основные нормы и правила по обеспечению единства измерений»

3 УТВЕРЖДЕНЫ И ВВЕДЕНЫ В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 4 марта 2014 г. № 69-ст

4 ВЗАМЕН Р 50.2.077—2011

Правила применения настоящих рекомендаций установлены в ГОСТ Р 1.0—2012 (раздел 8). Информация об изменениях к настоящим рекомендациям публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящих рекомендаций соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (gost.ru)

© Standartinform, 2014

Настоящие рекомендации не могут быть полностью или частично воспроизведены, тиражированы и распространены в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Introduction

The present Recommendations are developed according to the Article 9 of the RF Federal Law No. 102-FZ dd. June 26, 2008 “On Ensuring the Uniformity of Measurements” in order to prevent unauthorized configuration and interference in the software of measuring instruments that can result in measurement result distortions.

The Recommendations give details on the provisions of the Procedure for Standard Sample or Measuring Instrument Type Approval Testing and the Procedure for Issuing Type Approval Certificates for Standard Samples or Measuring Instruments, Setting or Change of the Validity Term for the Said Certificates and Verification Intervals for the Measuring Instruments approved by the Order of the RF Ministry of Industry and Trade No. 1081 dd. November 30, 2009, and sequence of operations at measuring instrument testing to approve its type is recommended as far as the check of the measuring instrument software protection against unauthorized configuration and interference is concerned.

The Recommendations are intended to be used by the developers, manufacturers and applicants for type approval testing of measuring instruments, by the organizations that perform type approval tests of measuring instruments according to the valid Russian legislation as well as by Federal Executive Authorities and their subordinate organizations whose responsibilities involve the approval of measuring instrument type and accreditation of measuring instrument testing centers.

Введение

Настоящие рекомендации разработаны в соответствии со статьей 9 Федерального закона Российской Федерации от 26 июня 2008 г. № 102-ФЗ «Об обеспечении единства измерений» в целях предотвращения несанкционированных настройки и вмешательства в программное обеспечение средств измерений, которые могут привести к искажениям результатов измерений.

В рекомендациях детализируются положения Порядка проведения испытаний стандартных образцов или средств измерений в целях утверждения типа и Порядка выдачи свидетельств об утверждении типа стандартных образцов или типа средств измерений, установления и изменения срока действия указанных свидетельств и интервала между поверками средств измерений, утвержденных приказом Минпромторга России от 30 ноября 2009 г. № 1081, и рекомендуется последовательность действий при проведении испытаний средств измерений в целях утверждения типа в части проверки защиты программного обеспечения средств измерений от несанкционированных настройки и вмешательства.

Рекомендации предназначены для использования разработчиками, изготовителями и заявителями испытаний средств измерений в целях утверждения типа, организациями, проводящими испытания в целях утверждения типа средств измерений в соответствии с действующим законодательством Российской Федерации, а также Федеральными органами исполнительной власти и подведомственными им организациями, функции которых распространяются на утверждение типа средств измерений и аккредитацию центров испытаний средств измерений.

METROLOGY RECOMMENDATIONS

State System for Ensuring the Uniformity of Measurements

MEASURING INSTRUMENT TYPE APPROVAL TESTING

Software protection check

State System for Ensuring the Uniformity of Measurements. Pattern evaluations of a measuring instrument for pattern approval. Software validation for protection assurance

Effective as of October 01, 2014

1 Scope of Application

The present Recommendations specify the sequence of operations at testing of measuring instruments (hereinafter referred to as MI) to approve their type as it pertains to the check of software protection against unauthorized configuration and interference, as well as give details complying with the international requirements OIML D 31 [1] and Guidelines WELMEC 7.2 [2] to the procedures outlined in the Procedures [3] and [4] approved by the Order of the RF Ministry of Industry and Trade No. 1081 dd. November 30, 2009 as far as MI software protection is concerned.

The Recommendations can also be used to check the MI software protection level for the MI not subject to state regulation in terms of ensuring the uniformity of measurements.

2 Referenced Standards

The following Standard is referred to in the present Recommendations:

РЕКОМЕНДАЦИИ ПО МЕТРОЛОГИИ

Государственная система обеспечения единства измерений

ИСПЫТАНИЯ СРЕДСТВ ИЗМЕРЕНИЙ В ЦЕЛЯХ
УТВЕРЖДЕНИЯ ТИПА

Проверка защиты программного обеспечения

State system for ensuring the uniformity of measurements. Pattern evaluations of a measuring instrument for pattern approval. Software validation for protection assurance

Дата введения – 2014–10–01

1 Область применения

Настоящие рекомендации устанавливают последовательность действий при проведении испытаний средств измерений (далее – СИ) в целях утверждения типа в части проверки защиты программного обеспечения (далее – ПО) СИ от несанкционированных настройки и вмешательства и детализируют с учетом международных требований OIML D 31 [1] и руководства WELMEC 7.2 [2] процедуры, установленные в Порядках [3] и [4], утвержденных Приказом Министерства промышленности и торговли Российской Федерации от 30 ноября 2009 г. № 1081, в части, касающейся защиты ПО СИ.

Рекомендации также могут быть использованы для проверки уровня защиты ПО СИ, не входящих в сферу государственного регулирования в области обеспечения единства измерений.

2 Нормативные ссылки

В настоящих рекомендациях использована нормативная ссылка на следующий стандарт:

Издание официальное

GOST R 8.654—2009 State System for Ensuring the Uniformity of Measurements. Requirements to measuring instrument software. Basic provisions

Note – When using the present Recommendations, it is expedient to verify the action of the referenced standard in the public information system – on the official site of the Federal Agency for Technical Regulation and Metrology on the Internet or by means of the annually published information index “National Standards”, which was published as of January 1 of the current year, and by means of the relevant monthly information indices “National Standards” published during the current year. In case the dated referenced standard is replaced, it is recommended to use the version of the standard with the above-stated year of approval (adoption). In case after the present Recommendations’ approval an amendment is introduced to the dated referenced standard and is related to the provision which is referenced to, the said provision is recommended to be used regardless of this amendment. In case the reference standard is cancelled without replacement, the provision containing a reference to it shall be used to the extent not covering this reference.

3 Terms and definitions

The following terms with the corresponding definitions are used in the present Recommendations:

3.1 Software protection check: Examination of software in order to confirm the identification data (features) and evaluation of its protection according to the legislation requirements in the field of ensuring the uniformity of measurements.

3.2 Unintentional software changes: Inadvertent, accidental impacts on the software and measurement data caused by measuring instrument design errors, programming errors, as well as by personnel activities and impact from occasional physical factors.

ГОСТ Р 8.654—2009 Государственная система обеспечения единства измерений. Требования к программному обеспечению средств измерений. Основные положения

Примечание — При использовании настоящими рекомендациями целесообразно проверить действие ссылочного стандарта в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодно издаваемому информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячно издаваемого информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящих рекомендаций в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящих рекомендациях применены следующие термины с соответствующими определениями:

3.1 проверка защиты программного обеспечения: Исследование программного обеспечения с целью подтверждения идентификационных данных (признаков) и оценки его защиты в соответствии с требованиями законодательства в области обеспечения единства измерений.

3.2 непреднамеренные изменения программного обеспечения: Непреднамеренные, случайные воздействия на программное обеспечение и измерительную информацию, вызванные ошибками в проектировании средств измерений, в программировании, а также действиями персонала и воздействиями случайных физических факторов.

3.3 **Deliberate software changes:** Deliberate interference in software and measurement data in order to distort the measurement data.

3.4 **Metrologically important software part:** Programmes and programme modules processing the measurement data and performing functions to identify and protect the measuring instrument software.

4 General provisions

4.1 MI software shall be checked by the organization that perform tests to approve the measuring instrument type according to the valid legislation of the Russian Federation (hereinafter referred to as the MI testing companies) and having experts on measuring instrument software on their staff.

The experts are to pass refresher training on the said specialty at least once per 5 years.

4.2 In the course of MI type approval tests the check of the MI software protection against unintentional and deliberate changes as well as evaluation of its level stated by the MI developer (see 4.4, 4.5 and 5.1.2) and the check of the MI software identification data shall be carried out.

4.3 It is permitted not to carry out the MI software protection check and its level evaluation for the MI whose design and/or operation peculiarities provide for complete access restriction to the metrologically important software part and measurement data (available mechanical protection and no hardware-software communication interfaces). In such cases the following note shall be made in the MI type description: “MI design eliminates the possibility of unauthorized interference in the MI software and measurement data”.

4.4 MI software protection level (low, medium, high) shall be stated (assigned) by the MI developer (manufacturer) or test applicant at submitting the MI for type approval testing (see 4.5, 5.3.1).

3.3 **преднамеренные изменения программного обеспечения:** Сознательные воздействия на программное обеспечение и измерительную информацию с целью искажения измерительной информации.

3.4 **метрологически значимая часть программного обеспечения:** Программы и программные модули, выполняющие обработку измерительной информации и реализующие функции по идентификации и защите программного обеспечения средств измерений.

4 Общие положения

4.1 Проверку защиты ПО СИ осуществляют организации, проводящие испытания в целях утверждения типа средств измерений в соответствии с действующим законодательством Российской Федерации (далее – организации, проводящие испытания СИ) и имеющие в своем штате специалистов в области программного обеспечения средств измерений.

Специалисты обязаны проходить процедуру повышения квалификации по указанной специализации не реже 1 раза в 5 лет.

4.2 В процессе проведения испытаний СИ в целях утверждения типа осуществляется проверка защиты ПО СИ от непреднамеренных и преднамеренных изменений и оценка ее уровня, декларированного разработчиком СИ (см. 4.4, 4.5 и 5.1.2), а также проверка идентификационных данных ПО СИ.

4.3 Для СИ, конструкция и/или особенности эксплуатации которых обеспечивает полное ограничение доступа к метрологически значимой части ПО и измерительной информации (наличие механической защиты и отсутствие программно-аппаратных интерфейсов связи) проверку защиты ПО СИ и оценку ее уровня допускается не проводить. В таких случаях, в описании типа СИ следует вносить запись: «Конструкция СИ исключает возможность несанкционированного влияния на ПО СИ и измерительную информацию».

4.4 Уровень защиты ПО СИ (низкий, средний, высокий) декларируется (назначается) разработчиком (изготовителем) СИ или заявителем испытаний при представлении СИ на испытания в целях утверждения типа (см. 4.5, 5.3.1).

The Guideline [2] provisions can provide a basis for such statement (assignment).

4.5 Paragraph 11 of the Guidelines [2] specifies the following protection levels for software and measurement data:

- low level: no special tools for the protection against deliberate changes are used;

medium level: software is protected against deliberate changes by simple software tools (for example, by text editor). Protection examples are passwords, user authorization, etc;

- high level: software is protected against deliberate changes by special software tools (debugging programmes and hard disk editors, software development tools). Protection examples are encryptic protection methods, electronical and mechanical sealing, etc.

Software for which it is permitted not to check its protection and not to evaluate the protection level as per 4.3, is related to software with high protection level.

4.6 Scope of MI software protection checks is specified by the developer or MI test applicant and is agreed upon with the MI testing company, if the MI is submitted for type approval testing, depending on the purpose and scope of MI application.

4.7 List of documents to be submitted for software protection check, scope and methods of checking the documentation and of functional tests are specified at the stage of developing the “Programme of MI type approval testing” as agreed between the test applicant and the MI testing company.

4.8 The result of the software protection check in the course of MI type approval testing is the authentication and integrity confirmation of the software which is set up in the MI, and of the software protection level stated by the developer or the applicant for MI testing.

За основу такого декларирования (назначения) могут быть взяты положения руководства [2].

4.5 Пунктом 11 руководства [2] предусмотрены следующие уровни защиты ПО и измерительной информации:

- низкий: не используются никакие специальные средства защиты от преднамеренных изменений;

- средний: программное обеспечение защищено от преднамеренных изменений с помощью простых программных средств (например, с помощью текстового редактора). Примерами защиты могут служить: пароли, авторизация пользователя и т. п.;

- высокий: программное обеспечение защищено от преднамеренных изменений с помощью специальных программных средств (программы-отладчики и редакторы жесткого диска, средства программной разработки). Примерами защиты могут служить: криптографические методы защиты, электронное и механическое опечатывание и т. д.

Программное обеспечение, для которого в соответствии с 4.3 проверку его защиты и оценку ее уровня допускается не проводить, относится к программному обеспечению с высоким уровнем защиты.

4.6 Объем проверок защиты ПО СИ определяется разработчиком или заявителем испытаний СИ и согласуется с организацией, проводящей испытания СИ, при представлении его на испытания в целях утверждения типа в зависимости от назначения и области применения СИ.

4.7 Перечень документов, представляемых для проверки защиты ПО, объем и методы проверки документации и функциональных проверок определяются на этапе разработки «Программы испытаний СИ в целях утверждения типа» по согласованию между заявителем испытаний и организацией, проводящей испытания СИ.

4.8 Результатом проверки защиты ПО в процессе проведения испытаний СИ в целях утверждения типа является подтверждение подлинности и це-

4.9 At checking the MI software it is permitted to use the test results complying with the requirements of the international document [1] and Guideline [2], regulatory documents and recommendations of the State System on Ensuring the Uniformity of Measurements, performance rules of voluntary MI software certification systems, industry documentation and documentation of the enterprises – MI manufacturers and developers.

5 Check of identification and protection of measuring instrument software

The identification and protection of MI software is carried out according to the test programme agreed upon with the applicant (developer, manufacturer) and involving:

- check of technical documentation as it pertains to the MI software;
- check of software identification;
- check of software protection against unintentional and deliberate changes.

Basing on the results of MI software identification and protection checks it is defined if the software protection level corresponds to the level stated by the developer or the applicant for MI testing. The protection level confirmed by the check is to be recorded in the MI type description.

The MI testing company shall execute a MI test report to the extent of the MI software protection check with the recommended report blank form being stipulated in the Appendix A.

лостности ПО, установленного в СИ, и уровня его защиты, декларированного разработчиком или заявителем испытаний СИ.

4.9 При проведении проверки защиты ПО СИ могут быть использованы результаты тестирования в соответствии с требованиями международного документа [1] и руководства [2], нормативными документами и рекомендациями Государственной системы обеспечения единства измерений, правилами функционирования систем добровольной сертификации ПО СИ, отраслевыми документами и документами предприятий - изготовителей и разработчиков СИ.

5 Проверка идентификации и защиты программного обеспечения средств измерений

Проверка идентификации и защиты ПО СИ проводится по согласованной с заявителем (разработчиком, изготовителем) программе испытаний, которая включает в себя:

- проверку технической документации в части, относящейся к ПО СИ;
- проверку идентификации ПО;
- проверку защиты ПО от непреднамеренных и преднамеренных изменений.

По результатам проверки идентификации и защиты ПО СИ устанавливается соответствие уровня защиты ПО уровню, декларированному разработчиком или заявителем испытаний СИ. Уровень защиты, подтвержденный в результате его проверки, документируется в описании типа СИ.

Организация, проводящая испытания СИ, оформляет протокол испытаний СИ в части проверки защиты ПО СИ, рекомендуемая форма которого приведена в приложении А.

5.1 Check of documentation

5.1.1 The aim of checking the documentation is to evaluate the completeness of description of the software important for the MI type approval and to confirm (set up) the software protection level.

5.1.2 The documentation on MI software shall include the data on programme functions, data structure and description of interfaces which are connected with the metrologically important software part. There shall be no hidden undocumented software functions.

The applicant for testing shall confirm the completeness of documenting the commands (p. 6.1 of the international document [1]) and absence of hidden undocumented functions.

The above data can be stated and executed in the form of a statement with its blank form being specified in the Appendix B.

5.1.3 The documentation on MI software shall include the information comprising the data from the list below to the extent applicable to this software:

- software designation including its name, designation of its version and/or versions of its modules;
- software purpose description, its structure and performed functions;
- description of the metrologically important software part;
- description of methods for software identification generation;
- description of methods for software identification visualization and instructions on identification presentation (if it is specified by the documentation);
- list of parameters being protected and description of tools for their protection and unauthorized access to them (if it is specified by the documentation);
- description of user interfaces, menu and dialogues;

5.1 Проверка документации

5.1.1 Целью проверки документации является оценка полноты описания ПО, существенного для утверждения типа СИ, и подтверждения (установления) уровня защиты ПО.

5.1.2 В документации на ПО СИ должны быть указаны программные функции, структура данных, и описаны интерфейсы, связанные с метрологически значимой частью ПО. Скрытые недокументированные функции ПО должны отсутствовать.

Заявитель испытаний должен подтвердить полноту документирования команд (пункт 6.1 международного документа [1]) и отсутствие скрытых недокументированных функций.

Данная информация может быть указана и оформлена в виде декларации, форма которой приведена в приложении Б.

5.1.3 В документации на ПО СИ следует представить информацию, которая должна содержать сведения из приведенного ниже перечня в той части, которая применима к данному СИ:

- обозначение ПО, включающее в себя его наименование, обозначение его версии и/или версий его модулей;
- описание назначения ПО, его структуры и выполняемых функций;
- описание метрологически значимой части ПО;
- описание методов генерации идентификации ПО;
- описание способов визуализации идентификации ПО и инструкция о представлении идентификации (если это предусмотрено документацией);
- список (перечень) защищаемых параметров и описание средств их защиты и несанкционированного доступа к ним (если это предусмотрено документацией);
- описание интерфейсов пользователя, меню и диалогов;
- описание интерфейсов связи ПО для передачи, обработки и хранения данных (в т.ч. посредством открытых или закрытых сетей связи);

- description of software communication interfaces for data transfer, processing and storage (including those by open or closed communication networks);
- description of implemented protection methods for software and measurement results;
- description of methods for measurement result storage on integrated, remote or portable media;
- description of systems and hardware required for MI operation.

The software protection level as per 4.5 shall also be stated in the documentation on MI software.

5.1.4 The information mentioned in 5.1.3 can be presented as programme documents (for example, programme description, explanatory note, application description, guidelines for system programmer, operator's manual etc.) or other programme documentation which the applicant has, herewith the recommendations of the unified system for programme documentation (USPD), etc. can be followed at executing the documents.

5.1.5 Graphic and text information in technical documentation shall be presented in such a way as to be suitable for complete and unambiguous interpretation.

5.1.6 The developer or the applicant for MI testing can present original programme texts or their fragments in technical documentation or separately, in case it appears to be required in the course of tests. A contract on confidentiality compliance can be concluded herewith.

5.2 Check of software identification

The MI testing company shall check the software identification data assigned by the MI developer (manufacturer) by the analysis of the documentation and functional (experimental) tests of MI samples submitted for testing.

- описание реализованных методов защиты ПО и результатов измерений;
- описание способов хранения результатов измерений на встроенном, удаленном или съемном носителях;
- описание требуемых для работы СИ системных и аппаратных средств.

Кроме того, в документации на ПО СИ следует декларировать уровень защиты ПО в соответствии с 4.5;

5.1.4 Указанная в 5.1.3 информация может быть представлена в виде программных документов (например, описания программы, пояснительной записки, описания применения, руководства системного программиста, руководства оператора и т. д.) или иной программной документации, имеющейся у заявителя, при этом при ее составлении можно руководствоваться рекомендациями единой системы программной документации (ЕСПД) и т. п.

5.1.5 Графическая и текстовая информация в технической документации должна быть представлена таким образом, чтобы она была пригодна для полного и однозначного понимания.

5.1.6 В случаях, когда в процессе испытаний возникает в этом необходимость, разработчиком или заявителем испытаний СИ в технической документации или отдельно могут быть дополнительно представлены исходные тексты программ или их фрагменты. При этом может быть заключен договор о соблюдении конфиденциальности.

5.2 Проверка идентификации ПО

Идентификационные данные ПО, присвоенные разработчиком (изготовителем) СИ, проверяются организацией, проводящей испытания СИ, путем анализа документации и функциональными (экспериментальными) проверками на образцах СИ, представленных для тестирования.

5.2.1 Analysis of documentation

5.2.1.1 The following data are referred to the software identification data (features) that can be stated in documentation and recorded in the MI type description (their content and type of a record entry can vary depending on the MI type):

- software identification name;
- software version number (identification number);
- digital software identifier (control totals of executable code of metrologically important software parts calculated as per the algorithms CRC32, md5, SHA1, etc. or as per specially developed algorithms with their calculation method being stated);

In particular cases such data as software name, developer's name, MI serial number, number of conformity certificate etc. can also be considered as software identification data (features), if they are directly related with the software (for example for MI as stated in p. 4.3).

The identification data (features) shall have the structure being unambiguously connected with the metrologically important software part.

It is permitted to present the software version number as a record entry "from version ..." or replacement of some elements in its designation related to metrologically unimportant part by special symbols (for example, «X» or «-»).

For instance, software version "Photogrammetric single-camera system PSCS" v.3.5.7.2 can be presented as v.3.5.x.x, herewith only part of the software version "v.3.5" is related to the metrologically important part, and the record entry "software version from v.3.5.7.2" can mean that versions v.3.5.7.2, v.3.5.7.3, v.3.5.8.1, etc. are allowed.

5.2.1 Анализ документации

5.2.1.1 К идентификационным данным (признакам) ПО, которые могут быть представлены в документации и зафиксированы в описании типа СИ, относятся следующие данные (их содержание и вид записи может зависеть от типа СИ):

- идентификационное наименование программного обеспечения;
- номер версии (идентификационный номер) программного обеспечения;
- цифровой идентификатор программного обеспечения (контрольные суммы исполняемого кода метрологически значимых частей ПО, рассчитанные по алгоритмам CRC32, md5, SHA1 и т. п. или специально разработанным алгоритмам с указанием способа их вычисления);

В особых случаях к идентификационным данным (признакам) ПО можно отнести также наименования ПО, имя разработчика, серийный номер СИ, номер свидетельства или сертификата соответствия и т. д., если эти данные непосредственно связаны с ПО (например, для СИ, как указано в пункте 4.3).

Идентификационные данные (признаки) должны иметь структуру, однозначно связанную с метрологически значимой частью программного обеспечения.

Допускается представление номера версии ПО в форме записи «номер версии не ниже ...» или замены некоторых элементов в его обозначении, отвечающих за метрологически незначимую часть, специальными символами (например, «X» или «-»).

Например, версия программного обеспечения «Система фотограмметрическая однокамерная СФО» v.3.5.7.2 может быть представлена в виде v.3.5.x.x, при этом только часть версии ПО «v.3.5» отвечает за метрологически значимую часть, а запись «версия ПО не ниже v.3.5.7.2» может означать, что допускаются версии v.3.5.7.2, v.3.5.7.3, v.3.5.8.1 и т. д.

5.2.1.2 The changes to MI software shall be reported by the manufacturer (developer or applicant) to the MI testing company which shall decide upon new software identification with the respective introduction of amendments to the MI type description, or on new tests of the said MI with updated software, in case the updated software can influence the metrological characteristics of MI and the MI verification operations specified at the type approval.

The above notification shall be sent as a letter to the MI testing company in which the nature of change in the metrologically important software part is described and a request for the introduction of amendments to the type description according to p. 5.1 of the Order [5], if necessary, is given.

5.2.2 Functional tests

5.2.2.1 MI software identification performed by the user (test operator) can be carried out either under his command or be executed during the normal MI operation.

Should the MI be not fitted by any indicators, the identification data can be sent via a communication interface and be displayed (printed) on another electronic device.

The test in question shall not be carried out for the MI design of which provides for complete software access restriction (see 4.3).

5.2.2.2 Functional tests involve the following:

- check of identification methods stated in the technical documentation on the software;
- check of implemented software identification methods;
- check that identification data (features) are independent of the identification methods;

Note – In case two alternative methods to obtain the same digital software identifier are described in the technical documentation on software, the digital identifiers obtained by the above methods shall be identical.

5.2.1.2 Изменения в ПО СИ требуют информирования изготовителем (разработчиком или заявителем) об этом организации, проводящей испытания СИ, которая должна принять решение о новой идентификации ПО с соответствующим внесением изменений в описание типа СИ, или о новых испытаниях данного СИ с обновленным ПО в случаях, когда обновленное ПО может влиять на метрологические характеристики СИ, а также на установленные при утверждении типа операции поверки СИ.

Информирование осуществляется письмом в организацию, проводящую испытания СИ, в котором описывается характер изменения метрологически значимой части ПО и содержится просьба, если это необходимо, о внесении изменений в описание типа, в соответствии с пунктом 5.1 приказа [5].

5.2.2 Функциональные проверки

5.2.2.1 Идентификация ПО СИ, проводимая пользователем (испытателем), может быть осуществлена либо по его команде, либо выполнена в процессе штатного функционирования СИ.

Если у СИ отсутствуют средства индикации, идентификационные данные могут направляться через интерфейс связи и отображаться (печататься) на другом электронном устройстве.

Для СИ, устройство которых обеспечивает полное ограничение доступа к программному обеспечению (см. 4.3), данная проверка не проводится.

5.2.2.2 При проведении функциональных проверок осуществляется:

- проверка способов идентификации, заявленных в технической документации на ПО;
- проверка реализованных способов идентификации ПО;
- проверка независимости идентификационных данных (признаков) от способов идентификации;

Примечание — Если в документации на программное обеспечение изложены два альтернативных способа получения одного и того же цифрового идентификатора ПО, то цифровые идентификаторы, полученные такими способами, должны быть идентичны.

- check of identification data (features) sufficiency.

It shall be verified that the stated software identification data (features) include such data (features) that identify the software unambiguously, i.e. change their value at the modification of the metrological software part.

For example, chromatograph software has the following identification features: software identification name: “testlab”, software version number: 1.2.4 and digital software identifier: 29657126aeb388d757e501b19ebe58e5. Change of the metrologically important software part shall prove that it had no impact on the software name and version number, but the digital software identifier has changed. Consequently, the digital identifier is sufficient for the unambiguous identification of the software and other identification features can be considered redundant.

5.2.2.3 The functional test of software identification shall prove:

- correctness of the software identification described in the documentation;
- compliance of the identification methods with the methods stated in the documentation.

5.3 Check of software protection against unintentional and deliberate changes

The protection level is checked by the MI testing company by the analysis of the documentation and functional (experimental) tests of MI samples submitted for testing.

5.3.1 Analysis of documentation

5.3.1.1 The software protection level is stated by the applicant/manufacture in a statement with the form of the latter being specified in the Appendix B.

- проверка достаточности идентификационных данных (признаков).

Убеждаются, что среди заявленных идентификационных данные (признаков) ПО имеются такие, которые однозначно идентифицируют ПО, т.е. меняют свое значение при модификации метрологической части ПО.

Например, ПО хроматографа имеет следующие идентификационные признаки: идентификационное наименование ПО: «testlab», номер версии ПО: 1.2.4 и цифровой идентификатор ПО: 29657126aeb388d757e501b19ebe58e5. Путем внесения изменений в метрологически значимую часть ПО убеждаемся, что они никак не повлияла на наименование и номер версии ПО, но при этом цифровой идентификатор ПО изменил свое значение. Таким образом, для однозначной идентификации ПО достаточно только цифрового идентификатора, а остальные идентификационные признаки можно считать избыточными.

5.2.2.3 В результате функциональной проверки идентификации ПО должны быть установлены:

- правильность идентификации ПО, описанной в документации;
- соответствие методов идентификации, методам, заявленным в документации.

5.3 Проверка защиты ПО от непреднамеренных и преднамеренных изменений

Проверка уровня защиты выполняется организацией, проводящей испытания СИ, путем анализа документации и функциональных (экспериментальных) проверок на образцах СИ, представленных для тестирования.

5.3.1 Анализ документации

5.3.1.1 Уровень защиты ПО декларируется заявителем/изготовителем и указывается в декларации, форма, которой приведена в приложении Б.

5.3.1.2 At stating the protection level (low, medium, high) the applicant shall compile probative materials verifying the stated level by himself. Technical documentation, software test results and/or other documents required to justify the chosen protection level can be used as the probative materials.

5.3.2 Functional tests

5.3.2.1 Correctness of the entered commands and display of the respective modes and settings of MI concerned with the measurement result displaying or MI metrology characteristics reproducing shall be proved by the check of user interfaces.

5.3.2.2 It shall be proved that the user interface gates through only those commands and/or data that are specified in the documentation on software.

5.3.2.3 The following shall be checked at functional tests of the software and measurement data protection against occasional or unintentional changes:

- availability of tools for the protection of software and measurement data against change or deletion in case of accidental actions (for example, power outages and voltage jumps);
- availability of tools for reporting on the change or deletion of metrologically important software files and measurement data;
- availability and proper functioning of the error recording logs (if it is provided by the documentation on MI);
- availability of measures to prevent unauthorized logging on into calibration mode allowing for the change of calibration constant values in the MI memory.

5.3.2.4 The following shall be checked at functional tests of the software and measurement data protection against deliberate changes:

5.3.1.2 При декларировании уровня защиты (низкий, средний, высокий) Заявитель самостоятельно формирует доказательные материалы, подтверждающие декларируемый уровень. В качестве доказательных материалов могут использоваться техническая документация, результаты испытаний ПО и/или другие документы, необходимые для обоснования выбранного уровня защиты.

5.3.2 Функциональные проверки

5.3.2.1 Путем проверки интерфейсов пользователя следует убедиться в правильности вводимых команд, и отображения соответствующих режимов и установок СИ, связанных с отображением результатов измерений или воспроизведением метрологических характеристик СИ.

5.3.2.2 Следует убедиться в том, что интерфейс связи пропускает только те команды и/или данные, которые отражены в документации на ПО.

5.3.2.3 При проведении функциональных проверок защиты ПО и измерительной информации от случайных или непреднамеренных изменений необходимо проверить:

- наличие средств защиты ПО и измерительной информации от изменения или удаления в случае возникновения случайных воздействий (например, отключение питания и скачки напряжения);
- наличие средств, информирующих об изменении или удалении метрологически значимых файлов ПО и измерительной информации;
- наличие и правильность функционирования журналов регистрации ошибок (если это предусмотрено документацией на СИ);
- наличие мер от несанкционированного входа в калибровочный режим, позволяющих изменять значения калибровочных констант в памяти СИ.

5.3.2.4 При проведении функциональных проверок защиты ПО и измерительной информации от преднамеренных изменений необходимо проверить:

- наличие средств защиты, исключающих возможность несанкциониро-

- availability of protection tools eliminating the risk of unauthorized modification, downloading, memory reading, deletion or other deliberate changes of metrologically important software part and measurement data;

- availability and implementation of measures to assure software integrity that are applied to the metrologically important software part and measured data.

As per the documentation on software, availability and proper functioning of the stated measures to assure software integrity shall be checked by making changes in the metrologically important software part, its structure and measurement data:

- availability of the procedure (for example, autotesting at MI switch-on / start-up) to check the software integrity and absence of errors;

- compliance of the algorithm used to calculate control totals and of the number of digits in control totals with the description provided in the documentation, in case the calculation of software control totals is stipulated;

- proper functioning of event detection and recording tools;

- compliance of authorities (access techniques) of the users having different rights of access to the software and measured data, with those stated in the technical documentation on MI software;

- correct and proper implementation of management of user's access to software functions and measured data.

6 Measuring instrument software validation at verification

6.1 Identification of software of every MI item used in the field of the state regulation for ensuring the uniformity of measurements, shall conform to that one stated in the MI type description. Provided with positive results, the MI software identification features are stated in the verification certificate.

ванных модификации, загрузки, считывания из памяти, удаления или иных преднамеренных изменений метрологически значимой части ПО и измерительной информации;

- наличие и реализацию мер по обеспечению целостности ПО, распространяющиеся на метрологически значимую часть ПО и измеренные данные;

В соответствии с документацией на ПО проверяют наличие и правильность функционирования заявленных мер по обеспечению целостности ПО путем внесения изменений в метрологически значимую часть ПО, его структуру и измерительную информацию.

- наличие процедуры проверки (например, автоматического тестирования при включении / запуске СИ) целостности ПО и отсутствия ошибок;

- соответствие алгоритма, используемого для расчета контрольных сумм, и количества разрядов контрольных сумм описанию в документации в случаях, если предусмотрен расчет контрольных сумм ПО;

- правильность функционирования средств обнаружения и фиксации событий;

- соответствие полномочий (способов доступа) пользователей, имеющих различные права доступа к ПО и измеренным данным, заявленным в технической документации на ПО СИ;

- корректность и правильность реализации управления доступом пользователя к функциям ПО и измеренным данным.

6 Подтверждение соответствия программного обеспечения средств измерений при поверке

6.1 Идентификация ПО каждого экземпляра СИ, используемого в сфере государственного регулирования в области обеспечения единства измерений, должна соответствовать той, что указана в описании типа СИ. При положительных результатах идентификационные признаки ПО СИ вносят в свидетельство о поверке.

6.2 Conformity of the software identification to the approved MI type shall be validated according to the procedure which shall be stipulated as a separate paragraph in the Section “Testing” of the MI verification procedure approved in the course of MI type approval testing. Software identification checking procedure shall comply with the procedure described in technical documentation on MI and approved in the course of MI testing to approve the MI type.

6.2 Подтверждение идентификации ПО утвержденному типу СИ проводят по методике, которая должна входить отдельным пунктом в раздел «Опробование» методики поверки СИ, апробированной в процессе испытаний СИ в целях утверждения типа. Методика проверки идентификации ПО должна соответствовать процедуре, описанной в технической документации на СИ, и подтвержденной в процессе испытаний СИ в целях утверждения типа СИ.

Appendix A
(recommended)

**Blank form of report on measuring instrument testing as to the
check of measuring instrument software protection**

Note – The test report shall be executed on the blank form of the MI testing company, page number and their total number in the report shall be provided on each page. Section “Test results” is an integral part of the report.

Blank form of the MI testing company	
TYPE APPROVAL TEST REPORT	
Software protection check	
Test operator	_____ name, mailing and legal address (if differ)
Applicant	_____ name, mailing and legal address (if differ)
MI name	_____ MI name and designation as in test programme and report
Manufacturer	_____ name, mailing and legal address (if differ)
Test carried out on	_____ the date on which the tests were carried out
Place of testing	_____ name, actual address where tests were carried out
Testing procedure	_____ name of testing programme or procedure and title of the section where MI software testing procedure is specified
Test carried out by	_____ signature _____ initials, surname
	_____ signature _____ initials, surname

Приложение А
(рекомендуемое)

**Форма протокола испытаний средств измерений в части проверки
защиты программного обеспечения средств измерений**

Примечание — Протокол испытаний оформляется на бланке организации, проводящей испытания СИ, на каждой странице указывается ее номер и общее количество страниц в протоколе. Раздел «Результаты испытаний» является неотъемлемой частью протокола.

Бланк организации, проводящей испытания СИ	
ПРОТОКОЛ ИСПЫТАНИЙ В ЦЕЛЯХ УТВЕРЖДЕНИЯ ТИПА	
Проверка защиты программного обеспечения	
Испытатель	_____ наименование, почтовый и юридический адрес (если не совпадают)
Заявитель	_____ наименование, почтовый и юридический адрес (если не совпадают)
Наименование СИ	_____ наименование и обозначение СИ, как в программе и акте испытаний
Изготовитель	_____ наименование, почтовый и юридический адрес (если не совпадают)
Дата проведения испытаний	_____ указывается дата проведения испытаний
Место проведения испытаний	_____ наименование, фактический адрес организации, где проводились испытания
Методика проведения испытаний	_____ наименование программы или методики испытаний, и номер раздела, в котором установлены методы испытаний ПО СИ)
Испытания провели	_____ личная подпись _____ инициалы, фамилия
	_____ личная подпись _____ инициалы, фамилия
	...

Test results

Note – It is recommended to execute the test results as tables, forms and content of the tables depend on the type, MI kind and protection level.

1 Check of documentation

1.1 List of documents submitted for checking

Note – It is presented according to the programme and/or procedure of testing.

No.	Title	Designation

1.2 Check of documentation as to software

Note – The following check results are to be stated: sufficiency and completeness of technical documentation on MI as related to software for the determination of software identification data, software structure, definition of metrologically important software part and level of software protection against unintentional and deliberate changes.

Requirements	Check results	Notes*
1	2	3
Software name, designation of its version and/or versions of its modules		
Software purpose description, its structure and performed functions		
Description of the metrologically important software part		
Description of methods for software identification generation		
Description of methods for software identification visualization and identification guidelines		
List of parameters being protected and description of tools for their protection and unauthorized access to them		
Description of user interfaces, menu and dialogues		
Description of software communication interfaces for data transfer, processing and storage		
Description of implemented protection methods for software and measurement results		
Description of methods for measurement result storage on integrated, remote or portable media		
Description of systems and hardware required for MI operation		
Availability of initial software		

* The document section providing the basis on which the fulfillment of the requirement can be judged, shall be specified

Результаты испытаний

Примечание — Результаты испытаний рекомендуется оформлять в виде таблиц; формы и содержание таблиц зависят от типа, вида СИ и уровня защиты.

1 Проверка документации

1.1 Перечень документации, предъявленной для проверки

Примечание — Представляют в соответствии с программой и/или методикой испытаний.

№	Наименование	Обозначение

1.2 Проверка документации в части программного обеспечения

Примечание — Указываются результаты проверки: достаточность и полнота технической документации на СИ в части ПО для определения идентификационных данных ПО, структуры ПО, выделения метрологически значимой части ПО и уровня защиты ПО от непреднамеренных и преднамеренных изменений.

Требования	Результаты проверки	Примечания*
1	2	3
Наименование ПО, обозначение его версии и/или версий его модулей		
Описание назначения ПО, его структуры и выполняемых функций		
Описание метрологически значимой части ПО		
Описание методов генерации идентификации ПО		
Описание способов визуализации идентификации ПО и инструкции по идентификации		
Список (перечень) защищаемых параметров и описание средств их защиты и несанкционированного доступа к ним		
Описание интерфейсов пользователя, меню и диалогов		
Описание интерфейсов связи ПО для передачи, обработки и хранения данных		
Описание реализованных методов защиты ПО и результатов измерений		
Описание способов хранения результатов измерений на встроенном, удаленном или съемном носителях		
Описание требуемых для работы СИ системных и аппаратных средств		
Наличие исходного ПО		

* Указывается раздел документа, на основе которого можно судить о выполнении требования

2 Check of software identification

Note – The data of the following operations shall be stipulated: check of implemented software identification methods, check of identification methods stated in technical documentation on software, check that identification data (features) are independent of the identification methods, check of availability and sufficiency of identification data.

2.1 Software identification data

Identification data (features)	Value
1	2
Software identification name	
Software version number (identification number)	
Digital software identifier	
Other identification data, if any	

2.2 Functional tests of software

Check scope	Check results	Description of procedure
1	2	3
Check of identification methods stated in technical documentation on software		
Check of implemented software identification methods		
Check that identification data (features) are independent of identification methods		
Check of sufficiency and availability of identification data (features)		

3 Check of software protection against unintentional and deliberate changes

3.1 Functional tests of software protection against unintentional changes

Note – The following check results shall be stated: availability and proper functioning of the tools to protect the metrologically important software part and measurement results against change or deletion in case of unforeseen physical impacts, availability of tools to inform the software user on the change or deletion of the metrologically important software part and measurement results, availability and proper functioning of logs to record errors and occasional or unintentional changes.

2 Проверка идентификации ПО

Примечание — Приводятся данные: проверки реализованных способов идентификации ПО, проверки способов идентификации, заявленных в технической документации на ПО, проверки независимости идентификационных признаков от способов идентификации, проверки наличия и достаточности идентификационных данных.

2.1 Идентификационные данные ПО

Идентификационные данные (признаки)	Значение
1	2
Идентификационное наименование ПО	
Номер версии (идентификационный номер) ПО	
Цифровой идентификатор ПО	
Другие идентификационные данные, если имеются	

2.2 Функциональные проверки ПО

Содержание проверки	Результаты проверки	Описание процедуры
1	2	3
Проверка способов идентификации, заявленных в технической документации на ПО		
Проверка реализованных способов идентификации ПО		
Проверка независимости идентификационных данных (признаков) от способов идентификации		
Проверка наличия и достаточности идентификационных данных (признаков)		

3 Проверка защиты ПО от непреднамеренных и преднамеренных изменений

3.1 Функциональные проверки защиты ПО от непреднамеренных изменений

Примечание — Приводятся результаты проверки: наличия и правильности функционирования средств защиты метрологически значимой части ПО и результатов измерений от изменения или удаления в случае возникновения непредсказуемых физических воздействий, наличия средств, информирующих пользователя ПО об изменении или удалении метрологически значимой части ПО и результатов измерений, наличия и правильности функционирования журналов фиксации ошибок и изменений случайного или непреднамеренного характера.

Check scope	Check results	Description of procedure
1	2	3
Check of the availability of tools for the protection of software and measurement data against change or deletion in case of accidental actions		
Check of the availability of tools for informing about the change or deletion of metrologically important software files and measurement data		
Check of the availability and proper functioning of error recording logs		
Check of the availability of measures to prevent unauthorized logging on into calibration mode allowing for the change of calibration constant values in the MI memory		

3.2 Functional tests of software protection against deliberate changes

Note – Results of the following checks shall be stated: availability of special protection tools eliminating the risk of unauthorized modification, downloading, MI memory reading, deletion or other deliberate changes of metrologically important software part and measurement results; check that application scope of the tools to check the software integrity covers the metrologically important software part and measurement results, check of conformity of software integrity checking algorithm to the sufficient level of protection against deliberate changes, check of a set of events subject to detection and recording in an event log, check of proper functioning of event detection and recording tools and their compliance with the sufficient level of protection of metrologically important software part and measurement results.

Содержание проверки	Результаты проверки	Описание процедуры
1	2	3
Проверка наличия средств защиты ПО и измерительной информации от изменения или удаления в случае возникновения случайных воздействий		
Проверка наличия средств, информирующих об изменении или удалении метрологически значимых файлов ПО и измерительной информации		
Проверка наличия и правильность функционирования журналов регистрации ошибок		
Проверка наличия мер от несанкционированного входа в калибровочный режим, позволяющим изменить значения калибровочных констант в памяти СИ		

3.2 Функциональные проверки защиты ПО от преднамеренных изменений

Примечание — Приводятся результаты проверки: наличия специальных средств защиты, исключающих возможность несанкционированных модификации, загрузки, считывания из памяти СИ, удаления или иных преднамеренных изменений метрологически значимой части ПО и результатов измерений, проверки сферы распространения действия средств проверки целостности ПО на метрологически значимую часть ПО и результаты измерений, проверки соответствия алгоритма проверки целостности ПО достаточному уровню защиты от преднамеренных изменений, проверки набора событий, подлежащих обнаружению и фиксации в журнале событий, проверки правильности функционирования средств обнаружения и фиксации событий и их соответствия достаточному уровню защиты метрологически значимой части ПО и результатов измерений.

Check scope	Check results	Description of procedure
1	2	3
Check of the availability of protection tools eliminating the risk of unauthorized modification, downloading, memory reading, deletion or other deliberate changes of metrologically important software part and measurement data		
Check of the availability of procedures to check the software integrity and absence of errors		
In case the calculation of software control totals is stipulated, it shall be checked that the algorithm used to calculate the control totals and the number of digits in the control totals comply with the procedures described in the documentation		
Check of proper functioning of event detection and recording tools		
Check of the compliance of authorities (access techniques) of the users having different rights of access to the software and measured data, with those stated in technical documentation on MI software		
Check of correct and proper implementation of management of user's access to software functions and measured data		

4 Conclusions as per check results

Conclusion on the MI software protection level shall be stipulated in the findings as per the check results.

Note – Additional sections can be included in the MI test report as to software protection check, if provided with well-grounded reasons.

Содержание проверки	Результаты проверки	Описание процедуры
1	2	3
Проверка наличия средств защиты, исключающих возможность несанкционированных модификации, загрузки, считывания из памяти, удаления или иных преднамеренных изменений метрологически значимой части ПО и измерительной информации		
Проверка наличия процедур проверки целостности ПО и отсутствия ошибок		
В случаях, если предусмотрен расчет контрольных сумм ПО, убедиться в том, что алгоритм, используемый для расчета контрольных сумм, и количество разрядов контрольных сумм, соответствуют описанным в документации процедурам		
Проверка правильность функционирования средств обнаружения и фиксации событий		
Проверка соответствие полномочий (способов доступа) пользователей, имеющих различные права доступа к ПО и измеренным данным, заявленным в технической документации на ПО СИ		
Проверка корректность и правильность реализации управления доступом пользователя к функциям ПО и измеренным данным		

4 Выводы по результатам проверки.

В выводах по результатам проверки делается заключение об уровне защиты ПО СИ.

Примечание — В обоснованных случаях в протокол испытаний СИ в части проверки защиты ПО могут быть включены дополнительные разделы.

Appendix B
(recommended)

**Statement of documentation completeness, protection level and
absence of undocumented capabilities of measuring instrument
software**

Note – The statement shall be executed on the blank form of the applicant for measuring instrument testing to approve its type.

Applicant _____
name, mailing and legal address (if differ)

Manufacturer _____
name, mailing and legal address (if differ)

MI name _____
MI name and designation

The applicant confirms that:

1 For the purpose of type approval testing of _____
MI name
the following programme documentation on _____
MI software name
was submitted _____;
list of the submitted programme documentation

2 Programme functions, important data structures and interfaces of the metrologically important software part are presented in full and are described in the documents submitted for testing;

3 Level of protection for _____
MI software name
complies with the level _____;
MI software protection level according to 4.5

4 There are no undocumented capabilities of _____.
MI software name

Приложение Б
(рекомендуемое)

**Декларация полноты документации, уровня защиты и отсутствия
недокументированных возможностей программного обеспечения средств
измерений**

Примечание — Декларация оформляется на бланке заявителя испытаний средств измерений в целях утверждения типа.

Заявитель _____
наименование, почтовый и юридический адрес (если не совпадают)

Изготовитель _____
наименование, почтовый и юридический адрес (если не совпадают)

Наименование СИ _____
наименование и обозначение СИ

Заявитель подтверждает, что:

1 для проведения испытаний _____
наименование СИ

в целях утверждения была предоставлена следующая программная документация на _____;
наименование ПО СИ

_____;
перечень предоставленной программной документации

2 программные функции, значимые структуры данных и интерфейсы метрологически значимой части ПО представлены полностью и описаны в предоставленной на испытаний документации;

3 уровень защиты _____
наименование ПО СИ

соответствует уровню _____;
уровень защиты ПО СИ в соответствии с 4.5

4 недокументированные возможности _____
наименование ПО СИ

отсутствуют.

References

- [1] OIML D 31:2008 (E) General requirements for software controlled measuring instruments
- [2] WELMEC 7.2, Issue 5 Software Guide (Measuring Instruments Directive 2004/22/EC), March 2012
- [3] Procedure for type approval testing of standard samples or measuring instruments (approved by the Order of the RF Ministry of Industry and Trade No. 1081 dd. November 30, 2009)
- [4] Procedure for issuing certificates of standard sample or measuring instrument type approval, setting and altering the validity term of the above certificates and verification intervals for measuring instruments (approved by the Order of the RF Ministry of Industry and Trade No. 1081 dd. November 30, 2009)
- [5] Order of the RF Ministry of Industry and Trade (Minpromtorg of Russia) No. 1326 dd. September 30, 2011) “On the introduction of amendments to the Procedure for standard sample or measuring instrument type approval, Procedure for issuing certificates of standard sample or measuring instrument type approval, setting and altering the validity term of the above certificates and verification intervals for measuring instruments approved by the Order of the RF Ministry of Industry and Trade No. 1081 dd. November 30, 2009”

Библиография

- [1] OIML D 31:2008 (E) General requirements for software controlled measuring instruments (Общие требования к программно контролируемым средствам измерений)
- [2] WELMEC 7.2, Issue 5 Software Guide (Measuring Instruments Directive 2004/22/EC), March 2012 (Руководство по программному обеспечению (Директива по измерительным приборам 2004/22/EC), март 2012)
- [3] Порядок проведения испытаний стандартных образцов или средств измерений в целях утверждения типа (Утвержден Приказом Министерства промышленности и торговли Российской Федерации от 30 ноября 2009 г. № 1081)
- [4] Порядок выдачи свидетельств об утверждении типа стандартных образцов или типа средств измерений, установления и изменения срока действия указанных свидетельств и интервала между поверками средств измерений (Утвержден Приказом Министерства промышленности и торговли Российской Федерации от 30 ноября 2009 г. № 1081)
- [5] Приказ Министерства промышленности и торговли Российской Федерации (Минпромторг России) от 30 сентября 2011 г. № 1326 «О внесении изменений в Порядок утверждения типа стандартных образцов или типа средств измерений, Порядок выдачи свидетельств об утверждении типа стандартных образцов или типа средств измерений, установления и изменения срока действия указанных свидетельств и интервала между поверками средств измерений, утвержденные приказом Минпромторга России от 30 ноября 2009 г. № 1081»

UDK 389.14:006.354

OKS 17.020

Key words: measuring instrument testing, approval of measuring instrument type, measuring instrument software, check of measuring instrument software protection

УДК 389.14:006.354

ОКС 17.020

Ключевые слова: испытания средств измерений, утверждение типа средств измерений, программное обеспечение средств измерений, проверка защиты программного обеспечения средств измерений

Руководитель разработки

Главный научный сотрудник ФГУП «ВНИИМС»

Ю.А. Кудяров

Исполнитель

Научный сотрудник ФГУП «ВНИИМС»

А.Н. Паньков

Head of development

Chief Scientific Officer of FGUP "VNIIMS"

Yu.A. Kudyarov

Executed by

Scientific Officer of FGUP "VNIIMS"

A.N. Pankov