Университет ИТМО

Факультет программной инженерии и компьютерной техники

Кафедра вычислительной техники

Реферат по дисциплине ”Метрология, стандартизация и сертификация”

Сертификация информационного и программного обеспечения

Выполнил:

Чебыкин И. Б.

Группа: P3401

Санкт-Петербург, 2018

ОГЛАВЛЕНИЕ

1 ВВЕДЕНИЕ **2**

2 ОБЩИЕ ПОЛОЖЕНИЯ **3**

3 ЭТАПЫ СЕРТИФИКАЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ **5**

3.1 Порядок проведения сертификации 5

3.2 Необходимая информация для прохождения процедуры сертификации . . 6

3.3 Требования к программному обеспечению 7

3.4 Проверка и тестирование программного обеспечения 9

3.5 Приемка и эксплуатация программного обеспечения 10

4 СТАНДАРТЫ ДЛЯ СЕРТИФИКАЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ **13**

4.1 Система государственных стандартов на программную продукцию . . . 13

4.2 Стандарты и нормативные документы, регламентирующие защищенность программного обеспечения 15

5 ЗАКЛЮЧЕНИЕ **18**

СПИСОК ЛИТЕРАТУРЫ **19**

1. ВВЕДЕНИЕ

Программное обеспечение – наряду с аппаратными средствами, важнейшая составляющая информационных технологий, включающая компьютерные программы и данные, предназначенные для решения определённого круга задач и хранящиеся на машинных носителях. Программное обеспечение представляет собой либо данные для использования в других программах, либо алгоритм, реализованный в виде последовательности инструкций для процессора. Программное обеспечение принято по назначению подразделять на системное и прикладное, а по способу распространения и использования на коммерческое, открытое и свободное.

Свободное программное обеспечение может распространяться, устанавливаться и использоваться на любых компьютерах дома, в офисах, школах, вузах, а также коммерческих и государственных учреждениях без ограничений. Применяемые программные средства в системах имеют тенденцию к увеличению сложности и объемов при параллельно возрастающем росте ответственности выполняемых ими функций. При этом постоянно повышаются требования к их качеству, надежности и безопасности. Ошибки или недостаточное качество программных средств, а также данных способны нанести ущерб, который значительно превысит эффект от их использования. Нарушения в технологическом процессе создания программного обеспечения могут привести к нежелательным результатам:

- удорожанию программного обеспечения;
- снижению безопасности систем;
- неудобству для пользователей, из-за чего они выбирают более качественный продукт.

2. ОБЩИЕ ПОЛОЖЕНИЯ

Использование сертификации программного обеспечения обусловлено тремя обстоятельствами – сертификация является единственным инструментом независимой оценки эффективности реализации механизмов защиты информации, решение с помощью встроенного СПО функциональных задач и обеспечение безопасности работы системы в целом, а также возможность реализации обязательных требований по обеспечению защиты информации различных уровней конфиденциальности.

В Законе “О техническом регулировании”[1] определены два вида сертификации: обязательная и добровольная.

Обязательной сертификации подлежит продукция, включенная в отраслевые перечни, определяемые соответствующими нормативными документами. В соответствии с законодательством обязательной сертификации подлежит используемое программное обеспечение и базы данных программно-аппаратных комплексов, обеспечивающее защиту государственных информационных ресурсов и конфиденциальность информации, составляющей государственную тайну.

Объектами, подлежащими добровольной сертификации, являются:

- сертификация программного обеспечения средств измерений как автономного, так и встроенного;
- сертификация программного обеспечения измерительных, информационно-измерительных и информационных систем;
- сертификация программного обеспечения контроллеров и вычислительных блоков;
- сертификация программного обеспечения систем управления, в том числе автоматизированных систем управления, функционирующих с использованием измерительного оборудования или элементов измерительных систем;
- сертификация программного обеспечения тренажеров и иных имитационных систем;

- сертификация программного обеспечения, используемого для моделирования технологических процессов, математического и иного моделирования;
- сертификация программного обеспечения для передачи, хранения, актуализации, защиты, обеспечения доступа и использования измерительной, вычислительной и иной информации;
- сертификация программного обеспечения баз данных;
- сертификация программного обеспечения устройств с измерительными функциями, в том числе игровых автоматов, включая аттракционы и игровые автоматы с денежным выигрышем, тотализаторов, виртуальных игр, платежных терминалов, а также лотерейного оборудования и т.п.;
- сертификация аппаратно-программных комплексов, представляющих собой нераздельную совокупность технических и программных средств, осуществляющих автоматизированное выполнение поставленных задач и/или обеспечивающих функционирование электронных информационных ресурсов информационных систем.

3.1. Порядок проведения сертификации

Процедуры и вся технология проведения работ по сертификации определяются схемой сертификации, которая устанавливает четкую совокупность действий, по результатам которых принимается решение о соответствии или несоответствии продукции заданным требованиям. Согласно идеологии Международной организации по стандартизации (ISO)[2] общепризнанными являются восемь основных схем сертификации.[3] Они используются и в комплекте основополагающих документов системы сертификации ГОСТ Р. При этом число схем сертификации, принятых Госстандартом России, в два раза больше, чем принято в зарубежной и международной практике.

Для каждой схемы сертификации продукции приводятся условия ее применения с учетом степени опасности продукции.

Порядок проведения сертификации программного обеспечения средств измерений, информационно-измерительных систем и аппаратно-программных комплексов определен такими методиками как МИ 2891-2004 “ГСИ. Общие требования к программному обеспечению средств измерений”[4] и МИ 2955-2005 “Типовая методика аттестации программного обеспечения средств измерений и порядок ее проведения”.[5]

Порядок проведения сертификации программного обеспечения включает:

- подачу заявки на сертификацию;
- принятие решения по заявке на сертификацию, в том числе назначение экспертов на проведение основных работ по сертификации из числа экспертов органа по сертификации;
- оформление договора на проведение работ по сертификации;
- проведение сертификационной проверки ПО, в том числе при необходимости проведение испытаний/контроля ПО по согласованным с заказчиком методикам;
- принятие решения о выдаче Сертификата соответствия и разрешения использова-

ния знака соответствия либо об отказе в выдаче Сертификата соответствия;

- выдача Сертификата соответствия и разрешения использования знака соответствия;
- занесение заявителя/изготовителя ПО и перечня сертифицированных ПО в Реестр СДС ПО;
- проведение инспекционного контроля сертифицированных ПО.

Результатом сертификации является возможность приобрести программный продукт в Российской Федерации с соответствующей поддержкой от производителя или его официального представителя.

3.2. Необходимая информация для прохождения процедуры сертификации

Для прохождения процедуры сертификации требуется:

- описание структуры сертифицируемого программного обеспечения, выполняемых функций, в том числе последовательность обработки данных;
- описание функций сертифицируемого ПО и параметров программного обеспечения, существенных для их работы;
- описание реализованных в сертифицируемом программном обеспечении алгоритмов функционирования, в том числе вычислительных алгоритмов, а также их блок-схемы;
- описание модулей программного обеспечения;
- перечень интерфейсов и перечень команд для каждого интерфейса, включая заявление об их полноте;
- список, значение и действие всех команд, получаемых от устройств ввода (клавиатуры, мыши, сенсорных устройств и т.п.);

- описание реализованных методов идентификации сертифицируемого программного обеспечения;
- описание реализованных методов защиты сертифицируемого программного обеспечения и данных от влияющих факторов;
- описание интерфейсов пользователя, всех меню и диалогов;
- описание хранимых или передаваемых наборов данных;
- руководство пользователя на сертифицируемое программное обеспечение;
- характеристики необходимых системных и аппаратных средств, если эта информация не приведена в руководстве пользователя.

Перечень документов, сопровождающих программное обеспечение, может корректироваться соглашением между исполнителем и заказчиком сертификации ПО.

3.3. Требования к программному обеспечению

Анализ требований к программному обеспечению предполагает определение следующих характеристик для каждого компонента ПО:

- функциональных возможностей, включая характеристики производительности и среды функционирования компонента;
- внешних интерфейсов;
- спецификаций надежности и безопасности;
- эргономических требований;
- требований к используемым данным;
- требований к установке и приемке;
- требований к пользовательской документации;
- требований к эксплуатации и сопровождению.

Требования к ПО оцениваются исходя из критериев соответствия требованиям к системе, реализуемости и возможности проверки при тестировании. Проектирование архитектуры ПО включает задачи (для каждого компонента ПО):

- трансформацию требований к ПО в архитектуру, определяющую на высоком уровне структуру ПО и состав ее компонентов;
- разработку и документирование программных интерфейсов ПО и баз данных;
- разработку предварительной версии пользовательской документации;
- разработку и документирование предварительных требований к тестам и планам интеграции ПО.

Архитектура компонентов ПО должна соответствовать требованиям, предъявляемым к ним, а также принятым проектным стандартам и методам.

Детальное проектирование ПО включает следующие задачи:

- описание компонентов и интерфейсов между ними на более низком уровне, достаточном для их последующего самостоятельного тестирования;
- разработку и документирование детального проекта базы данных;
- обновление (при необходимости) пользовательской документации;
- разработку и документирование требований к тестам и плана тестирования компонентов ПО;
- обновление плана интеграции ПО.

Кодирование и тестирование ПО охватывает задачи:

- разработку и документирование каждого компонента ПО и базы данных а также совокупности тестовых процедур и данных для их тестирования;
- тестирование каждого компонента ПО и базы данных на соответствие предъявляемых к ним требованиям. Результаты тестирования компонентов должны быть документированы;
- обновление (при необходимости) пользовательской документации;

- обновление плана интеграции ПО.

3.4. Проверка и тестирование программного обеспечения

Необходимость проведения тестирования программного обеспечения средств измерений на соответствие требованиям настоятельно подчеркивается в таких международных WELMEC 7.2 “Руководство по программному обеспечению”, и в ГОСТ Р 8.596 “ГСИ. Метрологическое обеспечение измерительных систем. Основные положения”.[6]

Сертификация программного обеспечения предназначена для производителей программного обеспечения и представляет собой проверку ПО с целью оценки степени пригодности к автоматизации процессов управления информационными ресурсами и включает следующие работы:[7]

- Проверка по функциональным критериям функциональных возможностей ПО (не проверяются: удобство использования, быстродействие, надежность защитных механизмов, и т.п.)
- Оценка состава документации;
- Оценка объема программирования, необходимого для настройки продукта по требованиям технологических процессов;
- Конфигурирование продукта для его проверки выполняется производителем ПО, за счет настройки профессионалом для обеспечения объективности проверки.
- Проверка по любому количеству процессов;
- Подробный отчет, включая детали реализации.

3.5. Приемка и эксплуатация программного обеспечения

Установка ПО осуществляется разработчиком в соответствии с планом в той среде и на том оборудовании, которые предусмотрены договором. В процессе установки проверяется работоспособность ПО и баз данных. Если устанавливаемое программное обеспечение заменяет существующую систему, разработчик должен обеспечить их параллельное функционирование в соответствии с договором.

Приемка ПО предусматривает оценку результатов квалификационного тестирования ПО и системы и документирование результатов оценки, которые проводятся заказчиком с помощью разработчика. Разработчик выполняет окончательную передачу ПО заказчику в соответствии с договором, обеспечивая при этом необходимое обучение и поддержку.

Процесс эксплуатации охватывает действия и задачи оператора – организации, эксплуатирующей систему и включает действия:

- Процесс обеспечения качества обеспечивает соответствующие гарантии того, что ПО и процессы его жизненные циклы соответствуют заданным требованиям и утвержденным планам. Под качеством ПО понимается совокупность свойств, которые характеризуют способность ПО удовлетворять заданным требованиям. Для получения достоверных оценок создаваемого ПО процесс обеспечения его качества должен происходить независимо от субъектов, непосредственно связанных с разработкой ПО. При этом могут использоваться результаты других вспомогательных процессов, таких, как верификация, аттестация, совместная оценка, аудит и разрешение проблем.

Процесс обеспечения качества программного обеспечения включает:

- подготовительная работа (заключается в координации с другими вспомогательными процессами и планировании самого процесса обеспечения качества с учетом используемых стандартов, методов, процедур и средств);
- обеспечение качества продукта подразумевает гарантирование полного соответствия программных продуктов и их документации требованиям заказчика, преду-

смотренным в договоре;

- обеспечение качества процесса предполагает гарантирование соответствия процессов жизненного цикла ПО, методов разработки, среды разработки и квалификации персонала условиям договора, установленным стандартам и процедурам;
- обеспечение прочих показателей качества системы осуществляется в соответствии с условиями договора и стандартом ISO 9001.

Процесс верификации состоит в определении того, что программные продукты, являющиеся результатами некоторого действия, полностью удовлетворяют требованиям или условиям, обусловленным предшествующими действиями (верификация в узком смысле означает формальное доказательство правильности ПО). В процесс верификации проверяются следующие условия:[8]

- непротиворечивость требований к системе и степень учета потребностей пользователей;
- возможности поставщика выполнять заданные требования;
- соответствие выбранных процессов жизненного цикла программного обеспечения условиям договора;
- адекватность стандартов, процедур и среды разработки процесса ПО;
- соответствие проектных спецификаций ПО заданным требованиям;
- корректность описания в проектных спецификациях входных и выходных данных, последовательности событий, интерфейсов, логики;
- соответствие кода проектным спецификациям и требованиям;
- тестируемость и корректность кода, его соответствие принятым стандартам кодирования;
- корректность описания в проектных спецификациях входных и выходных данных, последовательности событий, интерфейсов, логики;
- адекватность, полнота и непротиворечивость документации.

Аттестация, так же как и верификация, может осуществляться с различными степенями независимости. Если процесс аттестации выполняется организацией, не зависящей от поставщика, разработчика, оператора или службы сопровождения, то он называется процессом независимой аттестации. Процесс аттестации предусматривает определение полноты соответствия заданных требований и созданной системы или программного продукта их конечному функциональному назначению. Под аттестацией обычно понимается подтверждение и оценка достоверности проеденного тестирования. Аттестация должно гарантировать полное соответствие ПО спецификациям, требованиям и документации, а также возможность его безопасного и надежного применения пользователем. Аттестацию рекомендуется выполнять путем тестирования во всех возможных ситуациях и использовать при этом независимых специалистов. Аттестация может проводиться на начальных стадиях жизненного цикла ПО или как часть работы по приемке ПО.

Процесс совместной оценки предназначен для оценки состояния работ по проекту и ПО. Он сосредоточен в основном на контроле планирования и управления ресурсами, персоналом, аппаратурой и инструментальными средствами проекта. Оценка применяется как на уровне управления проектом, так и на уровне технической реализации проекта и проводится в течение всего срока договора. Данный процесс может выполняться двумя любыми сторонами, участвующими в договоре, при этом одна сторона проверяет другую. Процесс совместной оценки включает действия:

- подготовительную работу;
- оценку управления проектом;
- техническую оценку.

Процесс разрешения проблем предусматривает анализ и решение проблем (включая обнаруженные несоответствия) независимо от их происхождения или источника, которые обнаружены в ходе разработки, эксплуатации, сопровождения или других процессов. Каждая обнаруженная проблема должна быть идентифицирована, описана, проанализирована и разрешена.

4.1. Система государственных стандартов на программную продукцию

При проведении сертификации программного обеспечения используются методы оценки соответствия, основанные на международных правилах и нормах, которые позволяют с достаточной степенью достоверности определить соответствие программного обеспечения (программных продуктов) и аппаратно-программных комплексов требованиям нормативных документов программного обеспечения (программных продуктов) и аппаратно-программных комплексов.[9]

При сертификации программного обеспечения в системе ГОСТ Р, могут быть подтверждены требования, установленные следующими государственными стандартами на программную продукцию:

- ГОСТ 19.101-77 Единая система программной документации. Виды программ и программных документов
- ГОСТ 19.106-78 Единая система программной документации. Требования к программным документам, выполненным печатным способом
- ГОСТ 19.001-77 Единая система программной документации. Общие положения
- ГОСТ 19.401-78 Единая система программной документации. Текст программы. Требования к содержанию и оформлению
- ГОСТ 19.404-79 Единая система программной документации. Пояснительная записка. Требования к содержанию и оформлению
- ГОСТ 19.501-78 Единая система программной документации. Формуляр. Требования к содержанию и оформлению
- ГОСТ 19.508-79 Единая система программной документации. Руководство по техническому обслуживанию. Требования к содержанию и оформлению

- ГОСТ 19.601-78 Единая система программной документации. Общие правила дублирования, учета и хранения
- ГОСТ 19.604-78 Единая система программной документации. Правила внесения изменений в программные
- ГОСТ Р ИСО/МЭК 12207-99 Информационная технология. Процессы жизненного цикла программных средств
- ГОСТ Р ИСО/МЭК ТО 16326-2002 Программная инженерия. Руководство по применению
- ГОСТ Р ИСО/МЭК 12207 при управлении проектом
- ГОСТ Р ИСО/МЭК 12119-2000 Информационная технология. Пакеты программ. Требования к качеству и тестирование
- ГОСТ Р ИСО/МЭК 15408-2-2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
- ГОСТ Р ИСО/МЭК 15408-1-2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
- ГОСТ Р ИСО/МЭК 15408-3-2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
- ГОСТ 28195-89 Оценка качества программных средств. Общие положения
- ГОСТ 19.005-85 Единая система программной документации. Р-схемы алгоритмов и программ. Обозначения условные графические и правила выполнения
- ГОСТ 19.201-78 Единая система программной документации. Техническое задание. Требования к содержанию и оформлению
- ГОСТ 19.202-78 Единая система программной документации. Спецификация. Требования к содержанию и оформлению

- ГОСТ 19.301-79 Единая система программной документации. Программа и методика испытаний. Требования к содержанию и оформлению
- ГОСТ 7.70-96 Система стандартов по информации, библиотечному и издательскому делу. Описание баз данных и машиночитаемых информационных массивов. Состав и обозначение характеристик
- ГОСТ 7.70-2003 Система стандартов по информации, библиотечному и издательскому делу. Описание баз данных и машиночитаемых информационных массивов. Состав и обозначение характеристик

4.2. Стандарты и нормативные документы, регламентирующие защищенность программного обеспечения

К основным стандартам и нормативным техническим документам по безопасности информации, в первую очередь, относятся:[10]

- в области защиты информации от несанкционированного доступа комплект руководящих документов Гостехкомиссии России (1998 г), которые в соответствии с Законом “О стандартизации” можно отнести к отраслевым стандартам, в том числе “Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности средств вычислительной техники”“,”Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации“,”Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники“,”Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации“, ГОСТ Р 50739-95”Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования“;

- в области защиты информации от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН) “Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки за счет ПЭМИН” (СТР), ГОСТ 29339-92 “Информационная технология. Защита информации от утечки за счет ПЭМИН при ее обработке средствами вычислительной техники. Общие технические требования”, ГОСТ Р 50752-95 “Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники. Методы испытаний”, методики контроля защищенности объектов ЭВТ и другие.

Особенности защиты программ нашли свое отражение в следующих документах Гостехкомиссии России: “Программное обеспечение автоматизированных систем и средств вычислительной техники. Классификация по уровню гарантированности отсутствия недекларированных возможностей” и “Антивирусные средства. Показатели защищенности и требования по защите от вирусов”.

В первом документе устанавливается классификация программного обеспечения автоматизированных систем и средств вычислительной техники по уровню гарантированности отсутствия в нем недекларированных возможностей, где уровень гарантированности определяется набором требований, предъявляемых к составу, объему и содержанию документации представляемой заявителем для проведения испытаний программ и к содержанию испытаний.

Во втором документе устанавливается классификация средств антивирусной защиты по уровню обеспечения защиты от воздействия программ-вирусов на базе перечня показателей защищенности и совокупности описывающих их требований. Кроме того, следующие нормативные документы так или иначе косвенно регламентируют отдельные вопросы обеспечения безопасности ПО:

- ГОСТ 28195-89. Оценка качества программных средств. Общие положения;
- ГОСТ 21552-84. Средства вычислительной техники. ОТТ, приемка методы испытаний, маркировка, упаковка, транспортировка и хранение;
- ГОСТ ВД 21552-84. Средства вычислительной техники. ОТТ, приемка методы

испытаний, маркировка, упаковка, транспортировка и хранение;

- ТУ на конкретный вид продукции (ПО).

5. ЗАКЛЮЧЕНИЕ

Благодаря тестированию, экспертизам, различным видам испытаний и соответствующим доработкам программного обеспечения пользователь получает программный продукт, а не полуфабрикат. По эксплуатационной документации пользователь легко может установить программное обеспечение и быстро освоить приемы работы с ним. Ошибки, выявленные испытательным центром при тестировании и испытаниях, позволяют разработчику повысить надежность и качество программного обеспечения.

Таким образом, заказчик получает уверенность в том, что в его распоряжении находится качественный, законченный программный продукт, который соответствует потребностям, уверенно сопровождается и в случае необходимости может быть легко и без потерь восстановлен.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 27.12.2002 N 184-ФЗ (ред. от 29.07.2017) О техническом регулировании.

2. ISO 9000 — Википедия [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/ISO_9000 (дата обращения: 13.04.2018).

3. Схемы сертификации [Электронный ресурс]. URL: https://www.cert-group.ru/informatsiya/skhemy-sertifikatsii/ (дата обращения: 13.04.2018).

4. МИ 2891-2004 ГСИ. Общие требования к программному обеспечению средств измерений.

5. МИ 2955-2005 Типовая методика аттестации программного обеспечения средств измерений и порядок ее проведения.

6. ГОСТ Р 8.596-2002 Государственная система обеспечения единства измерений (ГСИ). Метрологическое обеспечение измерительных систем. Основные положения.

7. WELMEC 7.2 Software Guide (Measuring Instruments Directive 2004/22/EC).

8. ГОСТ Р 51904-2002 Программное обеспечение встроенных систем. Общие требования к разработке и документированию, гл. 8. Процесс верификации ПО.

9. Сертификация программного обеспечения [Электронный ресурс]. URL: http://gametest.ru/index.php?option=com_content&view=article&id=32:2011-11-21-10-28-10&catid=16:2011-09-22-13-44-43&Itemid=24 (дата обращения: 13.04.2018).

10. Казарин О.В. Безопасность программного обеспечения компьютерных систем. Монография. М.: МГУЛ, 2003. 212 с.