Экспертиза качества и надежности программного обеспечения на федеральном железнодорожном транспорте

Лозинин А. И.,

Шубинский И. Б.

Журнал «Надежность» №3 2002 г.

В статье последовательно рассматриваются вопросы актуальности, цели и порядка проведения экспертизы программных средств информационных систем. Определяются требования к средствам обеспечения экспертизы программных средств реального времени, регламентируется перечень представляемых материалов и порядок передачи программного обеспечения в фонд алгоритмов и программ.

Введение

Железнодорожный транспорт, как и другие отрасли промышленности, находится в непрерывном развитии. Средства автоматики усложняются, оснащаются сложными технологическими комплексами и оборудованием с широким использованием информационных технологий. Системы контроля и управления объектами, выполняющие функции диагностики состояния оборудования и устройств, служат для предупреждения аварийных и нештатных ситуаций. Надежность и функциональная безопасность рассматриваются сейчас как важнейшие характеристики систем, относящихся к безопасности движения [1].

С ростом ответственности функций возрастают требования к качеству, надежности и безопасности применения программного обеспечения. Ошибки в программных средствах или данных, способны нанести ущерб, который значительно превысит эффект от их использования. К тому же, многие информационные системы, которые эксплуатируются на железнодорожном транспорте, не способны выполнять полностью требуемые функциональные задачи с гарантированным качеством, и их приходится долго и иногда безуспешно сопровождать (а точнее, дорабатывать) для достижения приемлемого качества и надежности функционирования, затрачивая дополнительно большие средства и время. Происходит это оттого, что в документации на информационные системы недостаточно формализуются значения характеристик качества программного продукта, как их следует измерять и сравнивать с требованиями, отраженными в договоре, техническом задании или спецификациях требований. Более того, некоторые из характеристик просто отсутствуют в требованиях на программные средства, что приводит к произвольному их учету или к пропуску при приемочных испытаниях.

Нечеткое декларирование в документах понятий и требуемых значений характеристик качества программных средств вызывает конфликты между заказчиками и разработчиками из-за разной трактовки одних и тех же характеристик [2]. Причем, даже положения, уже почти десятилетней давности, стандарта ГОСТ Р ИСО/МЭК 9126-93 не учитываются при формулировании требований к программному обеспечению в техническом

задании.

В связи с этим стратегической задачей в жизненном цикле современных информационных систем является формализация требований к характеристикам качества программных средств и баз данных. Как формулирование этих требований, так и их выполнение должны проверяться независимыми экспертами на всех стадиях жизненного цикла.

Назначение экспертизы

Определение. Основная и конечная цель экспертизы состоит в том, чтобы проверить насколько завершённость (полная укомплектованность прикладным программным обеспечением, работающим на плановых аппаратных средствах и инфраструктуре программного обеспечения) информационной системы удовлетворяет определенным требованиям (функциональность, эффективность, надёжность и др.) и в какой степени она приемлема для конечных пользователей.

Осуществление этой цели невозможно без регламентации процессов, требований, организационных и методических подходов к установлению однозначно понимаемых требований и характеристик качества программных средств.

За последние несколько лет создано множество международных стандартов, регламентирующих процессы и продукты жизненного цикла программных средств и баз данных. Однако их применение в России тормозится по ряду объективных и субъективных причин. Основная причина - недостаточное финансирование работ по корректировке, адаптации или исключению некоторых положений международных стандартов применительно к принципиальным особенностям технологий и характеристик программной продукции. Вместе с тем, следует отметить некоторое оживление в этой области в последние три года, когда были приняты стандарты ГОСТ Р ИСО/МЭК 12207-99, ГОСТ Р ИСО/МЭК 12119-2000, ГОСТ Р ИСО/МЭК 14764-2002, ГОСТ Р ИСО/МЭК ТО 16326-2002, ГОСТ Р ИСО/МЭК 15408 (3 части)-2002 и др.

В процессе разработки программного обеспечения в МПС России применяются различные виды испытаний и экспертиз, которые проводятся с использованием процессов верификации, аттестации, совместного анализа и аудита, определенных в ГОСТ Р ИСО/МЭК 12207-99.

Поскольку все программные средства, разработка которых финансируется МПС России, подлежат обязательному фондированию в отраслевом фонде алгоритмов и программ, экспертизе, испытаниям и периодическому контролю их работоспособности и правильного внесения изменений и других модификаций, экспертиза начинается на начальных процессах жизненного цикла программного обеспечения. В отраслевом фонде алгоритмов и программ фондируются эталоны на носителях данных с исходными текстами и документация (проектная, эксплуатационная и программная).

МПС России является правообладателем программной продукции, финансирование разработки которой он осуществлял. Сюда входят оригинальные прикладные программы и базы данных, которые соответствуют

алгоритмам функционирования и описанию конкретного объекта управления (станции, перегона, участка железной дороги).

Экспертиза осуществляется по методике экспертизы программного обеспечения, которая разработана в Центре надежности и информационной безопасности (ЦНИБ) ВНИИУП МПС России.

Стоимость работ по экспертизе программного обеспечения определяется по методике расчета стоимости испытаний и сертификации.

Что же определило столь жесткие условия контроля со стороны заказчика?

Людям свойственно ошибаться при любом виде деятельности, в том числе и при создании программ. Ошибки бывают разные - от опечаток, которые находятся при первом запуске программы, до скрытых ошибок алгоритма или, ошибок, которые найти особенно тяжело, например, неверного использования языковых конструкций.

Ошибки в документации, а чаще просто недостаточное понимание работы той или иной конструкции языка или назначения библиотеки, ведет к неправильной работе программы.

Чаще всего, "свежий" взгляд может значительно ускорить поиск ошибки.

Ошибки в программах и данных могут проявиться и в период эксплуатации системы. Зарегистрированные и обработанные сведения используются для *выявления отклонений* от требований заказчика или технического задания.

Средства накопления сообщений об отказах, ошибках, предложениях на изменения, выполненных корректировках и характеристиках версий являются основой для управления *развитием и сопровождением* комплекса программного обеспечения.

Порядок экспертизы

Программа и методика экспертизы и испытаний, разработанные, как правило, экспертами-специалистами и согласованные с разработчиком и заказчиком содержат уточнения требований технического задания и документации и гарантируют корректную проверку заданных характеристик.

В процессе экспертизы определяются характеристики программных средств, выявляется пригодность испытываемой информационной системы к эксплуатации в условиях, определенных технической документацией. Это, в частности, означает, что документация на программное средство должна полностью соответствовать испытываемым программам, обеспечивать познаваемость системы обслуживающим персоналом, а также обеспечивать возможность развития и модернизации программ.

В процессе экспертизы проверяются и корректируются инструкции по эксплуатации комплекса программ во всех заданных режимах.

Определение. Программа экспертизы является планом проведения ряда процедур (тестирование, верификация, аттестация и др.), а также включающих серии экспериментов, для оценки соответствия качества,

надежности и функциональной безопасности программного обеспечения заданным требованиям.

Разрабатывается программа с позиции минимизации объема тестирования для проверки выполнения всех требований документов. Это определяется тем, что процесс тестирования, затянутый во времени, значительно удорожает стоимость экспертизы.

Программа экспертизы, в общем виде, содержит следующие основные, четко сформулированные, разделы:

- объект, его назначение и перечень основных документов, определивших его разработку;
- цель, с указанием требований технического задания, параметров подлежащих проверке и ограничений на проведение испытаний;
- программа испытаний, содержащая проверку комплектности предъявленного программного средства в соответствии с технической документацией и план тестирования для проверки по всем разделам технического задания и дополнительным требованиям, формализованным отдельными совместными решениями заказчика и разработчика;
- все понятия проверяемых характеристик, условия тестирования, средства, используемые для автоматизации испытаний, методики обработки и оценки результатов тестирования по каждому разделу программы испытаний.

Важнейшим фактором при анализе является методика обработки и оценки результатов, а также содержание протоколов проверки по пунктам программы испытаний.

Определение. Методика обработки и оценки результатов призвана обеспечить единство взглядов заказчика, разработчика и испытателя программ на детальную технологию обработки и оценку результатов экспертизы, не допускать искажений при обработке результатов.

Средства автоматизации процессов экспертизы призваны обеспечить полноту проверок характеристик по каждому разделу методик. Поэтому целесообразно использовать набор таких средств, позволяющих оценить различные свойства программного продукта.

К необходимости тщательной формулировки всех условий испытаний и значений параметров, при которых должна производиться проверка по каждому разделу программы, нас подвели высокая сложность современных программных средств и сильная взаимосвязь между их характеристиками.

Результаты испытаний фиксируются в *протоколах,* которые обычно содержат обобщенные результаты испытаний с оценкой их на соответствие требованиям технического задания и нормативным документам, а также выводы о результатах испытаний и соответствии созданного программного средства определенному разделу требований технического задания и документации.

При выполнении всех требований технического задания заказчик юридически обязан принять комплекс программ, закрыть контракт и работа

считается завершенной.

Однако, как уже отмечалось выше, для сложных программных средств трудно на начальных этапах проектирования предусмотреть и корректно сформулировать все требования технического задания. Поэтому при испытаниях часто выявляется, что некоторые требования технического задания оказываются невыполненными, и иногда не могут быть выполнены разработчиком даже при очень добросовестном отношении.

В этом случае необходима совместная работа специалистов-экспертов, заказчика и разработчика в поисках компромиссного решения при завершении испытаний и составлении заключения.

Если невыполненные требования являются второстепенными и слабо влияют на решение основных целевых задач программного средства, то может быть допустима корректировка технического задания или сертификация комплекса программ с отклонениями от первоначальных требований.

При выявлении отклонений от основных требований технического задания, существенно влияющих на целевые задачи функционирования, программное средство возвращается на доработку и затем, на повторные испытания.

Определение. Экспертное заключение должно содержать оценку степени выполнения требований технического задания и соответствия документации, а также вывод о возможности передачи программ в эксплуатацию и для серийного производства.

Сложность программных средств обычно адекватна сложности поведения объектов внешней среды, в которой функционирует соответствующее программное средство. Внешнюю среду для некоторых типов информационных систем и программных средств формируют специалисты-эксперты, которые непосредственно вручную создают (моделируют) тестовые ситуации при испытаниях соответствующих программных средств.

Иногда автоматизация генерации тестов может быть не рентабельна, так как трудно формализовать поведение человека при его взаимодействии с программным средством и такая замена вряд ли может быть достаточно адекватной. Эксперт может изобретать хитроумные логические ситуации и реализовать их в качестве тестов более эффективно, чем программные имитаторы, отражающие повеление человека.

Однако при генерации таких тестов следует соблюдать ряд общих правил, обеспечивающих регламентированность и контролируемость процессов тестирования программного средства [3]. Необходимо регистрировать эталонные, исходные и результирующие данные, обеспечить их точную повторяемость и полноту охвата реальных условий эксплуатации программного средства.

Требования к средствам обеспечения экспертизы программных средств реального времени

При наличии во внешней среде испытываемого программного средства

большого числа технических объектов, характеристики функционирования которых достаточно сложны, но могут быть формализованы, целесообразно создавать автоматизированные программно-аппаратные имитаторы тестов.

В сложных случаях испытаний программных средств для систем управления движением поездов требования к средствам обеспечения экспертизы программных средств сводятся к следующим:

- диапазоны изменения исходных данных, генерируемых в имитаторах, должны обеспечивать перекрытие всех характеристик современных реальных объектов внешней среды, а также предусматривать возможность их расширения с учетом прогресса в соответствующих областях техники;
- необходимо обеспечить регистрацию, контроль и обобщение характеристик генерируемых тестовых данных, эталонных данных и всех видов искажений и аномалий, поступающих на программное средство в любой момент времени и на любом заданном шаге обработки информации;
- для всех тестовых данных должны быть подготовлены эталонные реакции программного средства, с которыми следует сравнивать результаты, получаемые в процессе экспертизы программ;
- следует обеспечить максимально возможную повторяемость сеансов испытаний и генерируемых тестов после обнаружения аномалий в функционировании программного средства;
- все данные от реальных объектов и имитаторов внешней среды должны поступать в соответствии с естественным ходом процессов в объектах реального времени;
- необходимо иметь возможность совмещать данные от реальных объектов внешней среды и от имитаторов, заменяющих некоторые из них, которые нерационально или невозможно применять в натуральном виде.

Перечисленные требования определяют необходимость разработки соответствующих проблемно-ориентированных интегрированных систем имитаторов, способных достаточно полно заменить проверку программ с реальными объектами внешней среды.

Высокая стоимость и риск испытаний с реальными объектами практически всегда оправдывает значительные затраты на интегрированные системы имитации тестов, если предстоит экспертиза критических программных средств с высокими требованиями к корректности и надежности функционирования программ и их длительным жизненным циклом с множеством развивающихся версий [4].

Проверка системы во всех режимах и со всеми параметрами трудно реализуема, но к этому надо стремиться. Во многом успеху такой проверки для готовых и адаптируемых проектов программного обеспечения может послужить эталон, который должен храниться в отраслевом фонде алгоритмов и программ.

Отсутствие эталона программы, с которым можно было бы сравнить нечто

уже созданное, создает трудность определения момента, когда наступает уверенность, что необходимое качество программы достигнуто.

Эталоном в этом случае выступает проектная документация, которая приводит разницу взглядов различных людей на качество программы к одному знаменателю.

Отсутствие такой документации делает возможность качественной экспертизы программ весьма призрачной, поскольку взгляд на объем и качество выполняемых функций не совпадает не только у разных людей, но и может различаться у одного человека в разные промежутки времени.

Можно выделить три уровня достижения необходимого качества программ:

- отсутствие синтаксических ошибок и аварийных остановок в программе, что достигается прогоном программы с различными данными по максимальному числу ветвей;
- выполняемые функции программ соответствуют технической документации;
- расчетные значения, полученные при помощи процедур расчета, соответствуют эталонным.

Первый этап тестирования можно прекращать, когда есть уверенность, что большая часть синтаксических ошибок и аварийных остановов устранена. Остальные постепенно будут устраняться в процессе других этапов тестирования.

Второй этап тестирования можно прекращать, когда большая часть функциональности проверена и работает в соответствии с проектной документацией. Остальные несоответствия будут устраняться в процессе написания сопроводительной документации.

И, наконец, третий этап тестирования можно прекращать, когда основные расчетные тесты дают правильные результаты.

Общее качество программного обеспечения служит основным гарантом надежности и функциональной безопасности автоматизированных систем.

Однако существуют и особенности в экспертизе надежности и функциональной безопасности автоматизированных систем и их составляющих - программных средств.

Для программных средств реального времени, функционирующих в критических и важных системах управления и обработки информации, одним из важнейших показателей качества является надежность решения задач.

Для определения количественных значений показателей надежности создан и широко применяется ряд методов испытаний сложных систем, которые в той или иной мере могут использоваться для определения характеристик надежности программных средств реального времени [5]. Эти методы можно свести к трем основным группам:

- прямые экспериментальные методы определения показателей надежности систем в условиях нормального функционирования;
- форсированные (ускоренные) методы испытаний реальных систем на

надежность;

- расчетно-экспериментальные методы, при использовании которых ряд исходных данных для компонент получается экспериментально, а окончательные показатели надежности систем рассчитываются с использованием этих данных.

Для оценки надежности программного обеспечения нами разработана методика расчета надежности и функциональной безопасности критичных систем. Если, например, экспериментальным путем определены характеристики возможного искажения массива данных при функционировании программного средства, то аналитически можно рассчитывать надежность хранения данных при типовых схемах их дублированного хранения и оперативного восстановления при искажениях.

Порядок передачи программного обеспечения в фонд алгоритмов и программ

Определенный для указанных выше целей порядок проведения работ по экспертизе, тестированию, испытаниям (для целей экспертизы) и передачи программного обеспечения в отраслевой фонд алгоритмов и программ (ОФАП) предписывает, что эксперты ОФАП и испытательных центров обязаны принимать участие в работе ведомственных комиссий по приемке программных средств, разработанных организациями отрасли.

Программные средства передаются в ОФАП *с программными, информационными и сопроводительными документами* по договорам, заключенным между разработчиком и фондом. ОФАП, по желанию разработчика, может по договору об оказании научно-технических услуг провести работы по техническому редактированию и доработке документации в соответствии со стандартами.

В состав ОФАП МПС России включаются программные средства (программный фонд) и информационные материалы (информационный фонд), предназначенные для использования на железных дорогах, предприятиях и в организациях Министерства путей сообщения.

Обязательной передаче в ОФАП МПС России подлежат программные средства, разработка которых проводилась по планам НИОКР, финансируемым МПС России[1], а также программные средства, разработанные по прямым договорам, если техническим заданием или договором на разработку предусмотрено представление в ОФАП МПС России.

Передача в *программный фонд* (фондирование программных средств) - это передача разработчиком и (или) держателем авторских (имущественных) прав на программные средства в ОФАП МПС России эталонного образца программного средства и технической документации. Передача может осуществляться с правом (или без права) его изготовления (тиражирования), что определяется соответствующим договором между сторонами или в обязательном порядке на основании соответствующих указаний МПС России.

---

[1] В этом случае имущественные права на программное средство получает МПС России через отраслевой фонд алгоритмов и программ

Передача в *информационный фонд* алгоритмов, типовых проектных решений - это передача разработчиком или заказчиком программных средств информации о программных средствах в ОФАП МПС России. Передача может осуществляться в виде анкет, проектной документации, описаний, демонстрационных роликов и рекламно-технического описания для учета, распространения, публикации, маркетинга согласно договору между сторонами или в обязательном порядке на основании указаний МПС России.

Цель фондирования:

- накопление научно-технического потенциала отрасли;
- ведение эталонов разработок отраслевого применения с целью предупреждения утраты программных средств, разработка которых проводилась по планам НИОКР, финансируемым МПС России, из-за ликвидации предприятий, увольнения разработчиков и других форс-мажорных обстоятельств;
- повышение качества программных средств путем экспертизы соответствия программного и информационного обеспечения соглашениям, установленным в отрасли и требованиям нормативных документов.

При передаче программного средства в ОФАП должна быть произведена идентификация представленного опытного (эталонного) образца.

Идентификаторами образцов программного средства служат:

- Структура директорий;
- Файловая структура;
- Файлы исполняемые;
- Файлы данных;
- Контрольное число.

Комплект документации должен быть оговорен в техническом задании, и в этом же комплекте должен передаваться в ОФАП.

Программные средства, включаемые в программную часть фонда, должны соответствовать техническому заданию на разработку и отвечать следующим основным требованиям:

- работоспособность и актуальность;
- типовость (возможность широкого распространения);
- наличие комплекта программных и технических документов в соответствии с техническим заданием, необходимого для внедрения программных, аппаратно-программных средств и автоматизированных систем и ее компонентов на предприятиях и в организациях отрасли;
- соответствие документации стандартам;
- наличие лицензионных соглашений на право использования применяемых в разработке инструментальных программных средств;
- наличие сертификата соответствия (декларации о соответствии) или экспертного заключения о качестве, надежности и функциональной

безопасности;

- наличие акта о приемке в постоянную эксплуатацию на головном объекте и решения приемочной комиссии о тиражировании.

ОФАП МПС России формирует (совместно с организациями-разработчиками отрасли) единую программно-технологическую и информационную среду разработки и функционирования программных, аппаратно-программных средств и автоматизированных систем и их компонентов отраслевого применения, которая включает:

- операционные системы и компиляторы;
- интегрированные оболочки;
- системы телеобработки;
- сетевое программное обеспечение;
- системы управления базами данных;
- инструментальные средства (интегрированные пакеты прикладных программ, экспертные системы);
- издательские системы и редакторы текстов и прочие.

Хранение образцов и инспекционный контроль

Образцы программных средств, программные средства тестирования и их поставляемые дистрибутивы, базы данных испытаний в электронном представлении хранятся на сервере Испытательного центра (в защищенном от несанкционированного копирования варианте) с еженедельным резервным копированием.

Испытательный центр программных средств должен обеспечивать официальный инспекционный контроль выпуска и поставки программных продуктов и документации, включая изготовление копий с образца, маркировку и упаковку.

Обязательно проверяется комплектация и маркировка в соответствии с формуляром на программный продукт (документом, хранящимся, например, в ОФАП МПС России и у пользователя).

По результатам испытаний и экспертизы составляется перечень ошибок для единичных характеристик (затем этот перечень пополняет каталог ошибок программного обеспечения):

обобщенные статистические данные для повторяющихся ошибок, где это возможно и целесообразно;

сводная итоговая таблица ошибок, где полученные данные об ошибках группируются в соответствии с их взаимосвязями с единичными характеристиками.

Исходными данными для расчетов являются:

результаты регистрации времени реакции, выполнения функций, задач, запросов;

сводная итоговая таблица ошибок, где полученные данные об ошибках группируют в соответствии с их взаимосвязями с единичными показателями надежности.

Потенциальная польза от экспертизы

Итак, какова же потенциальная польза от независимой экспертизы на начальных этапах жизненного цикла программного обеспечения:

- разработчик может использовать результаты экспертизы для определения корректирующих воздействий по улучшению качества, повышению надежности или для выработки решений по изменению стратегии разработки;
- для заказчика - это уверенность в том, что финансирование работ можно осуществлять (продолжать) или прекращать, а также, поможет использовать качество как аргумент при выборе разработчика по данной тематике;
- для отрасли в целом, экспертиза дает уверенность в определенном уровне качества, надежности и функциональной безопасности конечного продукта.

Литература

1. Мишарин А.С. Концепция функциональной надежности информационных систем на федеральном железнодорожном транспорте // Надежность. 2002. №1, с.15-20
2. Липаев В.В. Системное проектирование сложных программных средств для информационных систем. Серия «Информатизация России на пороге XXI века». – М.: СИНТЕГ, 1999, 224с.
3. ГОСТ Р ИСО/МЭК 12119-2000. Информационная технология – Пакеты программ – Требования к качеству и тестирование.
4. ГОСТ Р ИСО/МЭК 12207-99. Информационная технология – Процессы жизненного цикла программного обеспечения.
5. Уткин Л.В., Шубинский И.Б. Нетрадиционные методы оценки надежности информационных систем //Под ред. И. Б. Шубинского – СПб.: Любавич, 2000, 173 с.: ил.