Экспертиза и сертификационные испытания программных средств на соответствие требованиям по функциональной безопасности и качеству

Лозинин А. И.

Программные средства, применяемые на железнодорожном транспорте, особенно в системах, критичных по безопасности, имеют тенденцию к увеличению

сложности и объемов, при параллельно возрастающем росте ответственности выполняемых ими функций. Постоянно повышаются требования к качеству, надежности и безопасности применения программных средств.

В этой ситуации, ошибки или недостаточное качество программных средств (а также и данных), способны нанести ущерб, который значительно превысит эффект от их использования.

Нарушения в технологическом процессе создания программного обеспечения могут привести к нежелательным результатам:

удорожание программного продукта из-за увеличения сроков его разработки;

снижение безопасности систем, критичных по безопасности;

создание неудобства для пользователей, что приводит их к выбору более качественного продукта конкурента.

В связи с этим стратегической задачей в жизненном цикле современных программных средств является формализация требований к функциональной безопасности, надежности и другим характеристикам качества.

Во всех индустриально развитых странах стандартам, нацеленным на обеспечение качества программных средств, уделяется большое внимание. В первую очередь это относится к проблеме использования программных средств в критических приложениях, таких как оборона, космос, энергетика (особенно ядерная), производство (потенциально опасное для жизни и здоровья людей, окружающей среды), транспорт и коммуникации.

В зарубежной практике используется целый ряд стандартов, регламентирующих процессы и продукты жизненного цикла программных средств и баз данных. Следует отметить некоторое оживление в последние годы и в отечественной стандартизации, 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 15904-2003, ГОСТ Р ИСО/МЭК 15408-2002 и др.

Когда мы говорим о качестве, то подразумеваем, некоторый эталон для сравнения, соответствие которому мы и принимаем для данной продукции. Нормативные документы, соответствие требованиям которых мы принимаем за такой эталон, должны в полной мере отражать современный уровень развития технологии, поэтому пересмотр положений нормативных документов, регламентирующих процессы и продукты жизненного цикла программных средств и баз данных, должен происходить не реже одного раза в три года. Многие из нормативных документов, созданных ранее для применения на

железнодорожном транспорте, либо устарели, либо содержат требования, противоречащие положениям государственных стандартов.

Приступая к работе над нормативным документом необходимо четко представлять себе, что каждое слово, термин, каждое положение, должны содержать достоверный, всесторонне продуманный подход, основанный на проведенных исследованиях и анализе международного и отечественного опыта стандартизации.

Заканчиваться работа над документом должна только тогда, когда широкий круг специалистов выскажет свои замечания, будет составлена сводка отзывов, и проведено согласительное совещание. Короче говоря, работа над документами, определяющими на ближайшие годы требования по безопасности, надежности, а также организационные, технические, методические и другие требования к продукции и организации ее производства, должна вестись серьезно, профессионально, с участием экспертов-специалистов способных довести нормативные документы до высокого уровня профессиональной проработки.

Нормативные документы ОАО «РЖД», регламентирующие процессы и продукты жизненного цикла программных средств и баз данных, должны стать дополнением к специальным техническим регламентам по безопасности на железнодорожном транспорте.

Соответствие требованиям нормативных документов по функциональной безопасности, надежности и качеству программных средств должно быть оценено в результате испытаний, тестирования и экспертизы в процессе их жизненного цикла.

Все программные средства, разработка которых финансируется ОАО «РЖД», должны подлежать обязательному фондированию (эталонов на носителях данных и программных документов) и периодическому контролю работоспособности эталонов и правильного внесения изменений и других модификаций.

В целях обеспечения качества и надежности программных средств, обеспечения его безопасного функционирования, экспертиза должна начинаться на этапе заключения договора и согласования технического задания (формулирования требований к программному обеспечению). Особенно важно подключение экспертов на этапе формулирования требований к программному обеспечению. Независимое тестирование программного обеспечения также целесообразно проводить в ходе разработки проекта.

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

Испытания и экспертиза программных средств, программно-технических комплексов автоматизированных систем, устройств и оборудования систем железнодорожной автоматики и телемеханики (в части программного обеспечения) проводятся с целью определения их соответствия нормативным документам.

Проведение любых видов испытаний и экспертизы программных средств железнодорожного транспорта в Испытательном центре программных средств

железнодорожного транспорта осуществляется в соответствии с *типовыми* методиками испытаний и экспертизы, в которых устанавливаются:

правила отбора образцов программных средств;

общие подходы:

к определению состава документации;

к определяемым характеристикам и метрикам качества программного обеспечения;

к последовательности и видам испытаний, рекомендациям по тестированию (планы, протоколы, методы);

к методам обработки результатов испытаний;

а также требования к персоналу, проводящему испытания, и распределение ответственности за обеспечение и проведение испытаний.

В методиках содержатся также формы документов, таблицы показателей качества, условия проведения испытаний и пр. Для проведения сертификационных испытаний, на основании требований к программному обеспечению и типовых методик испытаний, испытателем разрабатывается Программа и методика сертификационных испытаний.

На независимые испытания, тестирование, экспертизу разработчик (поставщик, изготовитель) должен представить:

образец программного средства с сопроводительными документами;

документацию требований (технические задания, технические условия, спецификацию требований и пр.);

материалы разработки;

документы и материалы по испытаниям;

эксплуатационную документацию.

Отбор и идентификацию образцов, представленных разработчиком, производит Регистр сертификации на федеральном железнодорожном транспорте (РС ФЖТ) совместно с испытательным центром.

При выполнении испытаний, тестирования и экспертиз Испытательный центр программных средств железнодорожного транспорта использует инструментальные программные средства: тестирования и моделирования; расчета надежности; анализа исходных текстов программ, фиксации эталонного образца; методики, основанные на современных методах испытаний. При этом Испытательный центр соблюдает строгую последовательность при проведении испытаний, при которой, прежде всего, определяется соблюдение требований по функциональной безопасности (при их нарушении, дальнейшие испытания теряют смысл), определяется надежность программных средств и производится общее оценивание качества (функциональные возможности, практичность, эффективность, сопровождаемость, адаптируемость).

Испытательный центр программных средств железнодорожного транспорта имеет большой опыт проведения экспертиз и испытаний программного обеспечения. Испытательным центром проведено более 140 экспертиз и испытаний в целях приемки объектов в эксплуатацию, передачи в фонд алгоритмов и программ и других целей по большому спектру программного обеспечения, представленного различными организациями, а также филиалами и подразделениями ОАО «РЖД».

Испытательный центр также участвует в экспертизах при возникновении нештатных и аварийных ситуаций; технических заданий на программное обеспечение; технических решений; программ и доказательств безопасности; нормативных документов и др.

Сотрудники Испытательного центра программных средств железнодорожного транспорта являются экспертами Системы сертификации на федеральном железнодорожном транспорте, имеют высокую квалификацию в области нормативного обеспечения процессов жизненного цикла программных средств и испытаний. Сотрудники Испытательного центра проводят консультации по вопросам экспертизы и сертификационных испытаний программных средств, по составу и содержанию программных документов и другим вопросам, связанным с качеством программных средств.

Услугами Испытательного центра пользуются различные организации, а также подразделения и филиалы ОАО «РЖД» (ВНИИАС МПС России, ГТСС, ПГУ ПС, РГУ ПС, НПП «Югпромавтоматизация», ЗАО «ИНФОТЭКС-АТ», НПЦ «Промавтоматика», ОАО «Радиоавионика», ООО «Бомбардье транспортейшн», ООО «Диалог-транс», ЗАО «Техтранс» и другие):

по адаптациям программного обеспечения по конкретные станции и участки проведено более 120 экспертиз;

по подсистемам логического обнаружения несоответствия зависимостей электрической централизации и автоблокировки 4 проекта (по системам «СЕТУНЬ», «ЮГ», «ДИАЛОГ» и «Тракт») доведены до состояния продукта с хорошей конфигурацией и полным комплектом программных документов;

проведены экспертизы при передаче в фонд алгоритмов и программ программных продуктов ЭБИЛОК-950 (Бомбардье), УВК РА (Радиоавионика) и АРМ ЛПК (ИНФОТЭКС АТ) и другие;

проводятся сертификационные испытания программных средств ДЦ «Сетунь» (АРМ ДНЦ, ПО РС «Связь», ПО РС «Шлюз» и ПО блоков БКПМ), ДЦ «ЮГ» с КП «КРУГ», ПО САУТ-ЦМ/485, АДК (диагностики и контроля) СЦБ и другие;

проведена экспертиза по случаю схода вагонов поезда №2707 на ст. Буранная Челябинского отд. Южно-Уральской ж.д. 15.03.2004 в части программного обеспечения (при экспертизе проведен анализ целостности и достоверности данных АРМ ЛПК ст. Гумбейка, проведена оценка правильности функционирования программного обеспечения при прохождении поезда №2707. Установлено, что нарушений целостности данных не было, некорректностей работы ПО не выявлено).

Необходимо обратить внимание на то, что проведенные экспертизы и испытания показали общие для большинства проектов недостатки:

низкий технический уровень документов;

почти на все объекты отсутствует требуемая для нормальной эксплуатации программная документация, выполненная в соответствии с российскими стандартами;

технические проблемы запуска программ показывают недостатки конфигурирования операционной среды для программного обеспечения;

комплект документации неполон, некорректно определяет состав программного обеспечения, не позволяет его идентифицировать и определить конфигурацию представленного программного обеспечения как объекта экспертизы;

в некоторых проектах создается большое количество документации, которая не информативна, дублирует целые разделы других документов;

в документации много противоречий, в том числе между документами в твердой копии и на диске;

для нештатных ситуаций программное обеспечение имеет недостаточно средств диагностики и поддержки пользователя;

во многих случаях дистрибутив программного средства некорректен, неполон или не может быть идентифицирован;

в большинстве разработок нет технического задания на программное обеспечение;

не выделено типовое программное обеспечение, в результате сам продукт не определен и не идентифицирован.

Большую роль в повышении функциональной безопасности, надежности и качества программного обеспечения играет сертификация в Системе сертификации на Федеральном железнодорожном транспорте. Сертификация осуществляется в порядке, соответствующем требованиям П ССФЖТ 41-2000 «Порядок проведения сертификации программных средств железнодорожного транспорта».

Согласно перечню, утвержденному МПС России 19.03.2000 г., сертификации (по форме добровольной сертификации) подлежат программные средства систем, критичных по функциональной и информационной безопасности.

Сертификация проводится в следующем порядке:

1 этап. Подача заявки изготовителем (поставщиком, разработчиком) в Регистр сертификации (РС ФЖТ) на сертификацию программного средства.

2 этап. Принятие решения РС ФЖТ по заявке. Срок ответа по заявке – не более 1 месяца. При положительном решении заключается договор РС ФЖТ с заявителем и определяется Испытательный центр для проведения сертификационных испытаний.

3 этап. Проводится отбор, идентификация и испытания образцов. Отбор образца программного средства проводит РС ФЖТ совместно с Испытательным центром и представителем заявителя. Заявитель предоставляет необходимую для испытаний документацию, заключает договор на проведение испытаний с Испытательным центром. Испытательный центр проводит сертификационные испытания и составляет протокол испытаний, который предоставляется в Регистр сертификации и заявителю.

4 этап. Проводится (в зависимости от выбранной схемы сертификации) оценка производства программных средств. Анализ состояния производства может проводиться заочно на основе анкеты и дополнительных документов.

Информация в представленных документах и анкете является конфиденциальной. Информация о состоянии производства периодически уточняется специалистами РС ФЖТ.

5 этап. Принятие, на основе результатов испытаний и анализа состояния производства, решения о выдаче сертификата соответствия.

При положительном решении – оформляется сертификат соответствия и лицензия на применения знака соответствия. Программный продукт вносится в Государственный Реестр Системы сертификации на федеральном железнодорожном транспорте.

При отрицательном решении – материалы возвращаются заявителю с указанием причин отказа.

6 этап. Проведение инспекционного контроля за сертифицированными программными средствами. По результатам инспекционного контроля РС ФЖТ может приостановить или аннулировать действие сертификата соответствия и лицензии на применение знака соответствия.

При устранении заявителем причин, приведших к приостановке действия сертификата, РС ФЖТ принимает решение о возобновлении действия сертификата и лицензии.

7 этап. О получении сертификата в информационных сборниках распространяется информация. Информация о других результатах сертификации и испытаний является конфиденциальной, что определяется договором с заявителем. Документы и материалы, подтверждающие сертификацию, передаются на хранение в РС ФЖТ. Образцы и результаты испытаний хранятся в архиве Испытательного центра.

При сертификации программных средств применяются следующие схемы:

Схема 1 Применяется для сертификации опытных образцов сложных автоматизированных систем для допуска их к эксплуатации на железных дорогах России.

Схема 2 Применяется при сертификации программных средств, для которых: изготовитель находится в отдаленных районах России или за рубежом; на стабильность характеристик влияют условия транспортирования и хранения; возможен отбор образцов у продавца (потребителя).

Схема 3 Применяется при сертификации продукции: стабильность серийного производства которой не вызывает сомнений; для которой отбор образцов у продавца (потребителя) затруднен или не может быть осуществлен.

В результате проведения тестирования, экспертиз, различные видов испытаний и соответствующих доработок программного обеспечения удалось добиться по многим проектам того, что:

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.

В результате заказчик получает уверенность в том, что он получает в свое распоряжение продукт, который соответствует его потребностям, сопровождается и может в случае форс-мажорных обстоятельств легко быть восстановлен без дополнительных материальных затрат.