Экспертиза и сертификационные испытания программных средств

Лозинин А.И.

Применяемые на железнодорожном транспорте программные средства в системах, критичных по безопасности, 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 и 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 продукта из-за увеличения сроков его разработки;
- снижению безопасности систем;
- неудобству для пользователей, из-за чего они выбирают более качественный продукт конкурента.

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

В зарубежной практике используется целый ряд стандартов, регламентирующих процессы и продукты жизненного цикла программных средств и баз данных. В последние годы в этой области были приняты и российские 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.

Современный уровень развития технологии должен в полной мере отражаться в требованиях нормативных документов. Положения нормативных документов, регламентирующих процессы и продукты жизненного цикла программных средств и баз данных, должны пересматриваться не реже одного раза в три года. Многие из созданных ранее нормативных документов для применения на железнодорожном транспорте, устарели или содержат требования, противоречащие положениям государственных стандартов.

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 профессионально с участием экспертов, способных довести нормативные документы до высокого уровня.

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

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.

Все программные средства, разработку которых финансирует ОАО «РЖД», подлежат обязательному фондированию (эталонов на носителях данных и программных документов) и периодическому контролю работоспособности эталонов и правильного внесения изменений.

Для достижения качества и надежности программных средств, обеспечения его безопасного функционирования экспертизу надо начинать на этапе заключения договора и согласования технического задания, т. е. формулирования требований к программному обеспечению. На этапе формулирования требований к программному обеспечению особенно важно подключить к работе экспертов. Независимое тестирование программного обеспечения также целесообразно проводить в ходе разработки проекта.

В процессе разработки программного обеспечения применяются различные виды контроля и испытаний, которые проводятся с использованием процессов сертификации, 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.

Любые виды испытаний и экспертизы программных средств железнодорожного транспорта осуществляются в Испытательном центре программных средств железнодорожного транспорта в соответствии с типовыми методиками испытаний и экспертизы. В них устанавливаются правила отбора образцов программных средств и общие подходы к определению состава документации, характеристикам и метрикам качества программного обеспечения, последовательности испытаний и их видам, а также к рекомендациям по тестированию, методам обработки результатов испытаний.

Кроме того, устанавливаются требования к персоналу, проводящему испытания, и распределяется ответственность за обеспечение и проведение испытаний.

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

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 др.), материал разработки, документы и материалы испытаний, эксплуатационную документацию.

Образцы, представленные разработчиком, отбирает и идентифицирует Регистр сертификации на федеральном железнодорожном транспорте (РС ФЖТ) совместно с Испытательным центром.

При испытаниях, тестировании и экспертизе 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 строго соблюдает последовательность испытаний, при которой прежде всего определяется выполнение требований по функциональной безопасности (при их нарушении, дальнейшие испытания теряют смысл), надежности программных средств и оценивается общее качество (функциональные возможности, практичность, эффективность, сопровождаемость, адаптируемость).

Испытательный центр программных средств железнодорожного транспорта имеет большой опыт проведения экспертиз и испытаний программного обеспечения. Центром проведено более 140 экспертиз и испытаний для приемки объектов в эксплуатацию, передачи в фонд алгоритмов и программ и для 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 являются экспертами Системы сертификации на федеральном железнодорожном транспорте и имеют высокую квалификацию в области нормативного обеспечения процессов жизненного цикла программных средств и испытаний. Они проводят консультации по вопросам экспертизы и сертификационных испытаний программных средств, 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, ГТСС, ПГУПС, РГУПС, НПП «Югпромавтоматизация», ЗАО «ИНФОТЭКС», НПЦ «Промавтоматика», ОАО «Радиоавионика», ООО «Бомбардье Транспортейшн (Сигнал)», ООО «Диалог-транс», ЗАО «Техтранс» и др.).

По адаптациям программного обеспечения для конкретных станций и участков проведено более 120 экспертиз. Четыре проекта по подсистемам логического обнаружения несоответствия зависимостей электрической централизации и автоблокировки (системы «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 Ebilock-950 («Бомбардье Транспортейшн (Сигнал)»), УВК РА («Радиоавионика») и АРМ ЛПК («ИНФОТЭКС») и др. Идут сертификационные испытания программных средств ДЦ «Сетунь» (АРМ ДНЦ, программное обеспечение радиостанций «Связь», «Шлюз» и блоков БКПМ), ДЦ «Юг» с КП «Круг», ПО САУТ-ЦМ/485, АДК СЦБ и др.

Вот конкретный пример. После схода вагонов поезда № 2707 15 марта 2004 г. на станции Буранная Южно-Уральской дороги проведены экспертиза программного обеспечения и анализ целостности и достоверности данных АРМ ЛПК станции Гумбейка. Была оценена правильность функционирования программного обеспечения при прохождении поезда № 2707. В результате установлено, что нарушений целостности данных не было, некорректной работы ПО не выявлено.

Проведенные экспертизы и испытания показали общие для большинства проектов недостатки. Среди них – низкий технический уровень документов, отсутствие требуемой для нормальной эксплуатации программной документации, выполненной в соответствии с российскими стандартами. Технические проблемы запуска программ показывают недостатки конфигурирования операционной среды для программного обеспечения. Документация недоукомплектована и некорректно определяет состав программного обеспечения. Это не позволяет идентифицировать и определить его конфигурацию как объекта экспертизы. В некоторых проектах создается большое количество документации, которая не информативна и 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. Типовое программное обеспечение не выделено, в результате сам продукт не определен и не идентифицирован.

Большую роль в повышении функциональной безопасности, надежности и качества программного обеспечения играет сертификация. Она осуществляется в порядке, соответствующем требованиям П ССФЖТ 41–2000 «Порядок проведения сертификации программных средств железнодорожного транспорта».

Программные средства систем, критичных по функциональной и информационной безопасности, подлежат добровольной сертификации согласно перечню, утвержденному МПС России 19.03.2000 г.

Сертификация проводится в следующем порядке. На первом этапе изготовитель (поставщик, разработчик) подает заявку в РС ФЖТ на сертификацию программного средства. На втором этапе в Регистре принимают решение по заявке. Срок ответа по заявке должен быть не более одного месяца. При положительном решении РС ФЖТ заключает договор с заявителем и определяет испытательный центр для проведения сертификационных испытаний.

На третьем этапе проводят отбор, идентификацию и испытания образцов. Образец программного средства отбирает РС ФЖТ совместно с Испытательным центром и представителем заявителя. Заявитель предоставляет необходимую для испытаний документацию, заключает договор на их проведение с Испытательным центром. Центр проводит сертификационные испытания и составляет протокол, который предоставляется в Регистр сертификации и заявителю.

На четвертом этапе проводят (в зависимости от выбранной схемы сертификации) оценку производства программных средств. Его состояние может анализироваться заочно на основе анкеты и дополнительных документов. Информация в представленных документах и анкете является конфиденциальной. Сведения о состоянии производства периодически уточняются специалистами РС ФЖТ.

На пятом этапе на основе результатов испытаний и анализа состояния производства принимают 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.

На шестом этапе проводят инспекционный контроль за сертифицированными программными средствами. По его результатам 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 его возобновлении и восстановлении лицензии.

На седьмом этапе в информационных сборниках распространяется информация о получении сертификата. Другие результаты сертификации и испытаний являются конфиденциальными, 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.

Сертификация программных средств осуществляется по трем схемам. Первая схема применяется при сертификации опытных образцов сложных автоматизированных систем для допуска их к эксплуатации на железных дорогах России.

Вторая используется при сертификации программных средств, изготовитель которых находится в отдаленных районах России или за рубежом, а также если на стабильность характеристик влияют условия транспортирования и хранения или возможен отбор образцов у продавца (потребителя).

Третья схема применяется при сертификации следующей продукции: стабильность ее серийного производства не вызывает сомнений, отбор образцов у продавца (потребителя) затруднен или не может быть осуществлен.

Благодаря тестированию, экспертизам, различным видам испытаний и соответствующим доработкам программного обеспечения по многим проектам 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 может быть уверен, 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.