Обязательное подтверждение соответствия программных средств железнодорожного транспорта

А. А. КОРНИЕНКО, докт. техн. наук, профессор, проректор по информатизации
Петербургского государственного университета путей сообщения (ПГУПС),
В. И. САФОНОВ, докт. техн. наук, начальник отдела регистра сертификации на федеральном железнодорожном транспорте (РС ФЖТ)


В статье Рассмотрены общесистемные и специфичные проблемы и решения обязательного подтверждения соответствия программного обеспечения и программно-технических комплексов информационно-управляющих и автоматизированных систем, применяемых в критичных с точки зрения безопасности технологиях управления движением и перевозочным процессом. Предложены подходы к разработке норм безопасности и методик испытаний программных средств железнодорожного транспорта.

Программа научно-технического развития ОАО «РЖД» на период до 2015 г. — «Белая книга» ОАО «РЖД» — рассматривает совершенствование систем управления и обеспечения безопасности движения, управления перевозочным процессом и транспортной логистики как одно из приоритетных направлений достижения технологического паритета и инновационного развития железнодорожного транспорта.

Его реализация в значительной мере базируется на внедрении и использовании современных информационных и телекоммуникационных технологий и, в частности, предусматривает:

- переход к информационно-управляющим технологиям работы;
- управление движением поездов на основе принципов координатного управления и интервального регулирования с использованием спутниковых технологий и современной системы цифровой технологической радиосвязи;
- консолидацию вычислительных ресурсов;
- создание «интеллектуального» поезда и «интеллектуальной» грузовой станции и решение других задач.

ОАО «РЖД» приступило к реализации «Концепции повышения безопасности движения на основе применения на железных дорогах многофункциональных комплексных систем регулирования движения поездов», утвержденной президентом ОАО «РЖД» 12 мая 2006 года.

В условиях динамично нарастающей информатизации железнодорожного транспорта для поддержания высокого уровня безопасности движения, грузовых и пассажирских перевозок, корпоративного управления, других критичных технологических процессов и систем важное значение приобретают вопросы обеспечения функциональной и информационной безопасности информационно-управляющих и автоматизированных систем (ИУАС). Их основу составляют программируемые микропроцессорные устройства, программное обеспечение, программно-технические комплексы (далее программные средства — ПС).

Одной из важнейших организационно-правовых мер обеспечения функциональной и информационной безопасности ИУАС является подтверждение соответствия, сертификация и декларирование соответствия программных средств в обязательной и добровольной форме.

Отметим, что необходимость обязательной сертификации специальных программных средств, используемых для организации перевозочного процесса по установленным требованиям безопасности, заложена Федеральным законом «О железнодорожном транспорте Российской Федерации».

В настоящее время, в связи с комплексным характером требований к качеству и безопасности ИУАС, сертификация программных средств железнодорожного транспорта осуществляется на добровольной основе в двух основных системах сертификации — по требованиям качества (РС ФЖТ аккредитован в качестве органа по сертификации) и по требованиям безопасности информации. Отметим, что сертификация по требованиям качества ориентирована, в первую очередь, на пользователя ПС, без оценивания полной функциональной безопасности и качества разработки. Для проведения подтверждения соответствия действует Перечень программных средств, в отношении которых предусмотрена добровольная сертификация (2001 г.), и некоторые другие нормативные документы, которые разрабатывали, в основном, ВНИИАС (ныне ОАО «НИИАС») и ПГУПС. При этом отсутствуют Нормы безопасности для всех программных средств железнодорожного транспорта.

При проведении сертификации по требованиям безопасности информации проводятся, в основном, испытания программных средств на отсутствие недекларированных возможностей в соответствии с требованиями соответствующего руководящего документа ФСТЭК России.

Существующий порядок сертификации изделий (продукции), в том числе ПС, поставляемых для нужд железнодорожного транспорта, в целом обеспечивает необходимый уровень безопасности транспорта для жизни людей, здоровья потребителей и охраны окружающей среды, предотвращения вреда имуществу потребителей.

Однако в условиях повышения требований к безопасности железнодорожного транспорта при возрастании объемов и скоростей транспортных перевозок, повышении пропускной способности сети дорог, реализации координатного управления и интервального регулирования движения поездов приобрела остроту необходимость решения проблем обязательного

подтверждения соответствия и сертификации приобретаемой техники и программных средств по требованиям и нормам безопасности.

При этом необходимо решить две группы проблем: системного — нормативного правового и организационного — характера, связанных с совершенствованием корпоративной системы управления качеством, сферы технического регулирования и подтверждения соответствия, и ряд проблем методического и инструментального плана с учетом особенностей ПС как объектов подтверждения соответствия.

Общесистемное решение этих проблем требует радикального пересмотра нормативной правовой и методической базы в рамках закона «О техническом регулировании». Создание необходимых условий для решения этой группы проблем предусматривается также в проекте постановления Правительства Российской Федерации «Об утверждении единого перечня продукции, подлежащей обязательной сертификации, и единого перечня продукции, подлежащей декларированию соответствия», в который введен ряд программных средств автоматизированных систем, применяемых на железнодорожном транспорте.

При решении проблем методического и инструментального плана необходимо учитывать следующие особенности сертификации ПО:

- программный продукт — сложный, динамично развивающийся объект;
- существует большое количество качественных характеристик с высокой сложностью практического оценивания качества, при этом отсутствуют нормы безопасности для всех программных средств железнодорожного транспорта;
- сложность проведения сертификационных испытаний на этапе динамического анализа;
- при сертификации часто доминирует этап экспертизы документации;
- ограниченные возможности существующих инструментальных средств оценки качества и распознавания недекларированных возможностей.

Сначала проанализируем уровень решения основных проблем системного плана. Коренной перелом решения этой группы проблем связан с существенной коррекцией в 2007 г. Федерального закона «О техническом регулировании» и, как следствие, радикальным изменением концепции технического регулирования на железнодорожном транспорте.

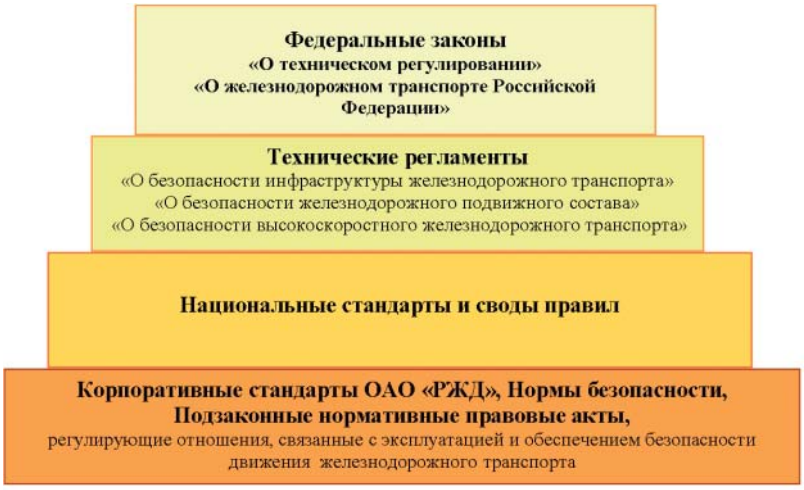

Рис. 1. Нормативная правовая база сферы технического регулирования на железнодорожном транспорте

С учетом скорректированной концепции и на основании утвержденной распоряжением Правительства Российской Федерации от 28 декабря 2007 г. № 1930-р Программы разработки технических регламентов вместо тяжеловесной системы из 16 технических регламентов (ТР) принято решение о создании трех основополагающих ТР. Один из основных разработчиков новых технических регламентов — ОАО «ВНИИЖТ».

В результате создана многоуровневая нормативная правовая система технического регулирования на железнодорожном транспорте (*рис. 1*), включающая в себя наряду с соответствующими федеральными законами:

- технические регламенты:

— «О безопасности инфраструктуры железнодорожного транспорта»;

— «О безопасности железнодорожного подвижного состава»;

— «О безопасности высокоскоростного железнодорожного транспорта»;

- национальные стандарты и своды правил;
- корпоративные стандарты ОАО «РЖД» (СТО ОАО «РЖД»), нормы безопасности и подзаконные нормативные правовые акты, регулирующие отношения, связанные с эксплуатацией и обеспечением безопасности движения железнодорожного транспорта.

Основными принципами формирования ТР являлись:

- поддержание существующего высокого уровня безопасности на железнодорожном транспорте;
- преемственность по отношению к действующей системе технического регулирования на железнодорожном транспорте;
- гармонизация с требованиями, установленными в международных и европейских стандартах.

Методологической основой системы устанавливаемых в ТР требований является реализация «нового подхода» — обеспечение приемлемого риска, сущность которого схематически иллюстрируется *рис. 2*. Техническими регламентами задаются обязательные для выполнения существенные требования безопасности с учетом оценки степени риска в виде функциональных требований, качественно определяющих необходимый уровень безопасности.

Выполнение требований ТР обеспечивается путем реализации положений национальных стандартов и сводов правил, применение которых является добровольным. Для подтверждения выполнения требований каждого ТР подготовлены два перечня: перечень национальных стандартов, в результате применения которых на добровольной основе обеспечивается соблюдение требований технического регламента; перечень национальных стандартов, содержащих правила и методы исследований (испытаний) и измерений, в том числе правила отбора образцов, необходимых для применения и исполнения принятого технического регламента.

Для инновационной продукции подтверждение соответствия требованиям безопасности технического регламента допускается проводить в форме обязательной сертификации путем выполнения отдельных положений национальных стандартов и/или сводов правил, а также на основании заключений, полученных от экспертного совета.

Отношения, связанные с эксплуатацией железнодорожного транспорта как единой системы, а также отношения, связанные с обеспечением безопасности движения, должны регламентироваться также на уровне подзаконных нормативных правовых актов и нормативных документов федераль-

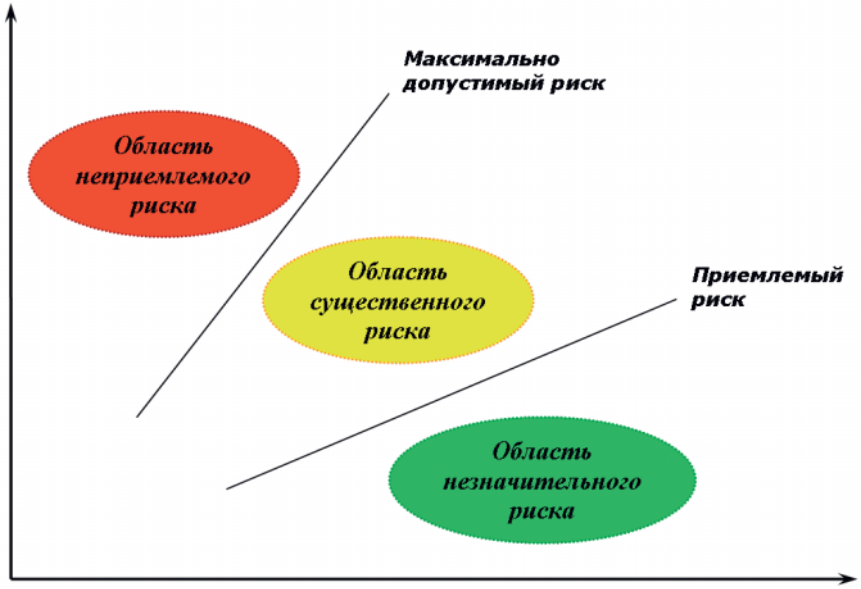

Рис. 2. Риск-ориентированный подход к обеспечению безопасности

ных органов исполнительной власти, таких, например, как правила технической эксплуатации и другие.

Таким образом, образована единая система обеспечения безопасности на железнодорожном транспорте, объединяющая привычные и, главное, обязательные для всех основные инструкции, корпоративные и национальные стандарты и технические регламенты. Такая структура легко гармонизируется с аналогичными европейскими документами и позволяет создать единое нормативное пространство, снимающее многие искусственно созданные барьеры на пути повышения безопасности и развития новой железнодорожной техники.

Техническими регламентами заданы обязательные требования безопасности к ПС как элементам функциональных подсистем и составных частей объектов технического регулирования.

Для программируемых устройств железнодорожных подсистем электроснабжения, автоматики и телемеханики, электросвязи и их составных частей и автоматических бортовых систем подвижного состава производят анализ информационной и функциональной безопасности. Для программируемых устройств и систем высокоскоростного подвижного состава и его составных частей при его проектировании и изготовлении и для программируемых устройств и систем железнодорожной линии, ее подсистем и их составных частей при их проектировании и строительстве обеспечивают информационную и функциональную безопасность.

Должно проверяться наличие у технических и программных средств, предназначенных для комплектования составных частей подсистем, документов об их соответствии предъявляемым требованиям безопасности настоящего технического регламента с не истекшим сроком действия.

Ошибочные действия персонала эксплуатирующей организации подсистемы и/или отказы (сбои) ее технических и программных средств не должны приводить к опасным состояниям.

Программные средства как встраиваемые в технические средства, так и поставляемые на материальных носителях должны удовлетворять следующим требованиям:

- обеспечивать возможность настройки и самодиагностики без прерывания своего функционирования;
- сохранять работоспособность после перезагрузок, вызванных сбоями/отказами технических средств, и целостность при собственных сбоях;
- не должны иметь свойств и характеристик, не описанных в своей документации (недекларированных возможностей);
- должны быть защищены от компьютерных вирусов, от несанкционированного доступа, от потерь и искажений при хранении, вводе, выводе, возникновении сбоев при обработке информации и от возможности случайных изменений

На каждой единице высокоскоростного подвижного состава проверяют соответствие версии установленного на ней программного обеспечения версии, указанной в документе о соответствии программного обеспечения предъявляемым к нему требованиям безопасности.

Система управления высокоскоростного подвижного состава, работа тягового привода и другого оборудования при любых неисправностях, ошибках и сбоях программного обеспечения не должна разрешать изменения характеристик и режимов работы, которые могут привести к нарушению безопасного состояния железнодорожного подвижного состава.

Номенклатура продукции, подлежащей обязательной сертификации, претерпела существенные изменения в сторону проведения декларирования соответствия. В перечень элементов составных частей и функциональных подсистем инфраструктуры железнодорожной линии, подлежащих декларированию соответствия, в том числе и для высокоскоростного железнодорожного транспорта, включены программные средства для систем управления движущимися объектами. В перечень составных частей железнодорожного подвижного состава, в том числе и высокоскоростного, подлежащих декларированию соответствия на основании собственных доказательств и доказательств с участием третьей стороны, включены системы управления электроподвижного состава, в том числе ПС.

В настоящее время в Правительство Российской Федерации переданы проекты технических регламентов и единых перечней продукции железнодорожного транспорта, подлежащих обязательному подтверждению соответствия. Это требует безотлагательной разработки норм безопасности для программной продукции, приведенной в утверждаемых перечнях:

- программно-технических комплексов для автоматизации управления организационно-экономическими процессами железнодорожного транспорта в части автоматизированных систем управления актово-претензионной работой; корпоративных автоматизированных систем управления финансами, материальными и трудовыми ресурсами; систем сетевого документооборота и делопроизводства; автоматизированных систем управления организационно-экономическими процессами железнодорожного транспорта;
- программно-технических комплексов для автоматизации управления технологическими процессами производства;
- программно-технических комплексов для автоматизации обмена данными (в интегрированных системах) в части информационно-управляющих систем, осуществляющих информаци-

онный обмен в сети передачи данных железнодорожного транспорта.

К основным проблемам разработки норм безопасности, прежде всего, относятся:

- отсутствие критериального аппарата определения безопасности применения ПС на железнодорожном транспорте;
- отсутствие необходимого методического аппарата оценки соответствия и расчета сертификационных показателей ПС.

Возможно использовать несколько подходов к разработке норм безопасности и методического обеспечения оценки соответствия по требованиям функциональной безопасности ПС.

Один из них заключается в подтверждении соответствия ПС на основе определения функций безопасности и уровней полноты безопасности программного обеспечения и использовании системы качественных показателей для их оценки в соответствии с серией стандартов ГОСТ Р МЭК 61508, в частности ГОСТ Р МЭК 61508-3-2007 «Функциональная безопасность систем электрических, электронных, программируемых, связанных с безопасностью. Часть 3. Требования к программному обеспечению».

Второй подход заключается в использовании иерархической системы показателей качества ПС, устанавливаемых ГОСТ 28195-89 и ГОСТ Р ИСО/МЭК 9126-93, с выделением на первом иерархическом уровне показателей безопасности и введением схем расчета оценочных элементов качества ПС.

Третий подход предполагает их комбинирование.

В данной статье рассматривается второй подход к разработке норм безопасности ПС. При этом в качестве основного критерия качества ПС, от которого зависит безопасность применения ПС на федеральном железнодорожном транспорте, выбирается критерий применимости. Критерий применимости определяет, что показатели качества-безопасности должны лежать в областях значений, которые позволяют безопасно применить данное ПС на железнодорожном транспорте. Сужая (делая более жесткими) границы области значений, определяющих безопасное применение ПС на федеральном железнодорожном транспорте, строится следующая четырехуровневая структура системы показателей качества-безопасности.

Первый уровень — это факторы качества-безопасности, которые определяются интегральными оценками по пяти группам показателей качества и безопасности, таких как функциональные возможности и корректность, надежность, удобство применения и безошибочность действий, безопасность и развертываемость. Второй уровень составляют комплексные показатели качества, третий уровень — метрики качества и метрики сложности, четвертый уровень — оценочные элементы.

Далее необходимо решать проблемы методического и инструментального обеспечения оценки соответствия ПС разработанным и утвержденным нормам безопасности.

Для оценки и расчета показателей качества ПС целесообразно разработать следующие типовые методики сертификационных испытаний:

- проверки функциональных возможностей ПС;
- оценки своевременности и надежности представления выходной информации ПС;
- оценки безошибочности действий должностных лиц при применении ПС;
- оценки безопасности ПС;
- оценки возможности развертывания ПС.

Каждая типовая методика сертификационных испытаний программных средств должна включать следующие основные положения:

- область применения;
- объект испытаний;
- виды и последовательность проведения испытаний, определяемые характеристики;
- условия проведения испытаний; методы и средства проведения испытаний;
- порядок проведения испытаний; обработка данных и оформление результатов испытаний;
- требования безопасности и охраны окружающей среды;
- требования к персоналу; распределение ответственности за обеспечение и проведение испытаний.

Основными методами испытаний выступают: экспертный, специальное тестирование и расчетный в различных соотношениях.

Одним из важных направлений по созданию средств испытаний является разработка инструментальных средств автоматизации оценки соответствия ПС по требованиям качества и безопасности, которые позволят повысить достоверность результатов и существенно сократить временные затраты на проведение сертификационных испытаний.

Важную роль в области подтверждения соответствия, сертификации и декларирования соответствия ПС могут играть вузы по следующим направлениям:

1. Создание и аккредитация на базе вузов испытательных лабораторий (ИЛ) или испытательных центров (ИЦ), а также экспертных центров (ЭЦ) в системах сертификации РС ФЖТ и других системах сертификации и организация их эффективной практической работы.

Представляется полезным опыт ПГУПС по организации работы аккредитованных в различных системах сертификации ИЛ и ИЦ по принципу «в одно окно», что позволяет сократить время на предварительную экспертизу документов и уменьшить стоимость сертификационных испытаний для заявителя. Например, по этому принципу строится работа «испытательного холдинга» ПГУПС в составе трех аккредитованных структур (ИЛ и ИЦ), проводящих сертификационные испытания по требованиям безопасности информации и качества программного обеспечения, а также по требованиям безопасности функционирования, ЭМС, надежности.

2. Подготовка специалистов в рамках информационных специальностей за счет введения в учебные планы соответствующих дисциплин, участие в подготовке экспертов РС ФЖТ (подобный опыт имеет МИИТ) и других систем сертификации.

3. Разработка нормативных правовых и методических документов и инструментальных средств, автоматизирующих работу эксперта.

В частности, ПГУПС ведет разработку нормативных правовых и методических документов и имеет почти двадцатилетний научно-методический и практический опыт в области подтверждения соответствия и сертификации средств железнодорожной автоматики и телемеханики. Сотрудниками ПГУПС ведется научная работа в направлении использования и разработки системы метрик сложности для оценки качества разработки и безопасности программного обеспечения, выявления недекларированных возможностей и создания на этой основе автоматизированных инструментальных средств нового поколения (с интеллектуальными свойствами).

Предлагаемые решения проблем подтверждения соответствия и сертификации программных средств нормативного правового, методического и инструментального плана повысят качество и безопасность поставляемой программной продукции и обеспечат выполнение возрастающих требований к безопасности и надежности железнодорожного транспорта.