Стандартизация и сертификация

УДК 656.25:681.32

Д. С. Марков, канд. техн. наук,
О. А. Наседкин, канд. техн. наук,
Д. А. Васильев,
М. А. Бутузов
Кафедра «Автоматика и телемеханика на железных дорогах»,
Петербургский государственный университет путей сообщения
Императора Александра I

ПОНЯТИЙНЫЙ АППАРАТ ЭКСПЕРТИЗЫ И ИСПЫТАНИЙ НА БЕЗОПАСНОСТЬ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ

В статье показана необходимость развития понятийного аппарата в области инструментальных средств экспертизы и испытаний систем и устройств железнодорожной автоматики и телемеханики и его влияние на работоспособность и безопасность в соответствии с требованиями различных стадий жизненного цикла, в первую очередь тех, которые связаны с процессами разработки и доказательства безопасности. В существующих нормативных документах практически отсутствует терминология по нестандартным инструментальным средствам, что затрудняет взаимопонимание различных специалистов и коллективов, участвующих в процессах разработки и доказательства безопасности железнодорожной автоматики и телемеханики.

На основе анализа доказательства безопасности и свойств железнодорожной автоматики как объекта экспертизы и испытаний сформулированы требования и определен состав инструментальных средств. Показано, что имитаторы различного вида целесообразно разрабатывать на базе технологии гибридных экспертных систем, позволяющей эффективно использовать в одном испытательном средстве в качестве базы знаний эвристические экспертные алгоритмы и математические, как правило имитационные, модели объектов управления, устройств, подсистем и систем железнодорожной автоматики. В работе предложена совокупность терминов и определений по инструментальным средствам экспертизы и испытаний, являющаяся методологической основой дальнейшего развития нормативных документов в области доказательства работоспособности и безопасности железнодорожной автоматики и телемеханики.

железнодорожная автоматика и телемеханика; жизненный цикл; разработка и доказательство безопасности; безопасность функционирования; инструментальные средства экспертизы и испытаний; имитаторы; гибридные экспертные системы

Введение

Как показано в [1–4], изменение подходов к процессам разработки и проверки систем железнодорожной автоматики и телемеханики (ЖАТ) на базе со-

временных технических средств необходимо. Отмечается сложность технических средств, на базе которых разрабатываются такие системы. Показано, что оценить уровень безопасности этих систем возможно только путем поэтапного подтверждении правильности решаемой задачи от момента установления исходных требований к аппаратным и программным средствам до их интеграции в единую систему. Необходима также разработка средств экспертизы и испытаний с учетом возможности их применения на различных стадиях жизненного цикла ЖАТ. Такой класс средств получил название «нестандартные», так как он преимущественно разрабатывается под конкретный объект испытаний, ориентированный на проверку требований, сформулированных в соответствии с принятой последовательностью разработки системы. При этом принимается во внимание возможность разбиения системы на отдельные составляющие, требования к которым могут быть проверены только на стадии разработки. Состав таких средств, удельный объем проверок, а соответственно и общий объем испытаний на том или ином этапе разработки могут быть конкретизированы только с учетом специфических особенностей системы в каждом отдельном случае.

Принимая во внимание результаты исследований понятийного аппарата в [5], где рассмотрены известные и предложены новые понятия в области безопасности ЖАТ (функциональная безопасность – ГОСТ Р МЭК 61508-4–2012 [6], ГОСТ Р 54504–2011 [7], ГОСТ Р МЭК 61511-1–2011 [8], безопасность функционирования, безопасность железнодорожной автоматики – ГОСТ Р 53431–2009 [9]), можно утверждать, что испытания на безопасность должны проводиться с использованием в качестве методологической основы понятия «безопасность функционирования» ЖАТ. В [5] понятие безопасности функционирования ЖАТ определено как свойство системы (устройства) ЖАТ обеспечивать технологическую безопасность и безопасное поведение при систематических, случайных отказах аппаратных или аппаратно-программных средств и внешних воздействиях, включая ошибки операторов.

В данном случае понятие безопасности функционирования ЖАТ связано с понятием безопасности ЖАТ, т. е. является техническим и предполагает, в рамках общего процесса доказательства безопасности, выполнение следующих задач:

– подтверждение полноты и корректности технологических функций системы;

– подтверждение безопасного функционирования системы при ошибочных действиях оперативного и технического персонала;

– подтверждение режимов функционирования системы, связанных с ее реконфигурацией, обеспечением защитного состояния при отказах технических средств и восстановлением;

– подтверждение корректности и полноты реализации положений концепции обеспечения безопасности системы.

Выполнение указанных задач предполагает наличие методического обеспечения (программа и методика испытаний) и инструментальных средств экспертизы и проведение испытаний (ИСЭИ) устройств и систем ЖАТ на работоспособность и безопасность.

В данной работе развиваются идеи, изложенные в [5], она направлена на формирование понятийного аппарата в области ИСЭИ.

1 Основные положения

Сложность процесса доказательства безопасности современных систем ЖАТ, базирующихся на микроэлектронной и программируемой технике, определяется рядом особенностей [10–12], которые должны быть учтены в процессе их разработки:

– сложность и функциональная замкнутость микроэлектронных элементов;

– преобладание программной составляющей при реализации функций, связанных с безопасностью;

– разнообразие микроэлектронной и программируемой техники;

– высокая чувствительность микроэлектронной элементной базы к влияниям внешней среды;

– многообразие интерфейсов, определяющих взаимодействие подсистем и систем между собой и с эксплуатационно-техническим персоналом;

– наличие нескольких подсистем, объединенных иерархической структурой;

– многообразие подходов к реализации технологических задач и методов обеспечения безопасности;

– распределенность процесса разработки и сопутствующих процессов во времени и по месту выполнения и соответственно неодновременность готовности к экспертизе и испытаниям различных устройств, подсистем, прежде всего программных и аппаратных средств разрабатываемых ЖАТ.

Указанные особенности микропроцессорных ЖАТ определяют специфику процесса их разработки, которая заключается в последовательном подтверждении правильности решаемой задачи – от постановки исходных требований до интеграции составных частей (программ и аппаратных средств) в систему. Процесс доказательства безопасности имеет вид итеративного процесса, охватывающего все стадии разработки системы, начиная со стадии формирования технических требований и заканчивая эксплуатационными испытаниями. Таким образом, возможно обоснование требований безопасности по результатам интегральной оценки результатов разработки на отдельных стадиях создания системы. Это, естественно, означает дополнительные требования к разработчику, обязывая его, параллельно разработке, осуществлять деятельность по подтверждению безопасности:

– формулировать требования с учетом принятой последовательности разработки системы;

– выделять фазы разработки с учетом возможности разбиения системы на отдельные составляющие, разработка и контроль которых могут осуществляться параллельно;

– разрабатывать методики испытаний с учетом специфики требований;

– разрабатывать средства экспертизы и испытаний для соответствующей стадии разработки системы.

Выполнение этих требования позволяет:

– оценивать, с поэтапным повышением полноты и достоверности, достигнутый уровень безопасности системы, начиная с экспертных и расчетных методов и заканчивая экспериментальными проверками;

– упростить процесс доказательства за счет разбиения общей задачи по стадиям разработки системы, с учетом степени готовности ее составляющих;

– определять степень соответствия установленным требованиям на ранних стадиях разработки и тем самым сократить затраты, связанные с корректировкой схемотехнических и программных решений;

– формировать доказательную базу для последующих процедур, связанных с подтверждением соответствия.

2 Требования к средствам экспертизы и испытаний

Анализ понятий безопасности, особенностей процессов разработки и свойств ЖАТ как объекта экспертизы и испытаний позволяет сформулировать следующие основные требования к ИСЭИ:

1. Концепция синтеза ИСЭИ должна базироваться на основе технологии экспертных систем, позволяющей концентрировать в одном испытательном средстве знания экспертов; требования нормативной и конструкторско-технической документации; различные концепции, методы и средства реализации ЖАТ, защищенных от опасных отказов; математические (чаще всего имитационные [13, 14]) модели объектов управления, устройств и систем ЖАТ.

2. ИСЭИ должны обеспечивать функциональную полноту испытаний относительно создания технологических и технических ситуаций, обеспечивающих проверку полноты и корректности выполнения технологических функций, технологической безопасности и безопасного поведения.

3. ИСЭИ должны обеспечивать возможность эмуляции испытываемого устройства с целью изучения поведения данного устройства и (или) его программного обеспечения при возникновении отказов или в режимах, переход в которые реального (физического) устройства невозможен или труднодостижим.

4. Возможность автоматической генерации тестовых воздействий на испытываемую систему (устройство) с целью проведения экспериментов в соответствии с программой и методикой испытаний в автоматическом режиме.

5. Наличие в ИСЭИ информационных, программных и аппаратных интерфейсов; некоторые (незначительные) изменения программного обеспечения – преобразование в контрольно-испытательное программное обеспечение.

6. Возможность отображения в ИСЭИ в зависимости от целей испытаний и свойств ЖАТ:

6.1. Состояний испытываемой системы (устройства) для обеспечения возможности визуального контроля состояния ЖАТ в процессе экспериментов.

6.2. Объектов управления и контроля.

6.3. Неразработанных на момент испытаний программ, устройств и (или) подсистем испытуемой ЖАТ.

6.4. Отказов аппаратных средств и ошибок программ (например, методом программных закладок в контрольно-испытательное программное обеспечение).

8. Наличие в ИСЭИ средств взаимодействия (диалоговая подсистема ИСЭИ) с персоналом (экспертами, инженерами по знаниям, пользователями), обеспечивающих удобство и в то же время контроль действий операторов в процессе подготовки и проведения испытаний.

9. Наличие средств приобретения знаний для развития ИСЭИ по мере накопления опыта в процессе выполнения реальных испытаний по видам систем и устройств ЖАТ.

10. Наличие в ИСЭИ средств протоколирования и анализа результатов испытаний.

Анализ задач экспертизы и испытаний, свойств ЖАТ и сформулированных выше требований к ИСЭИ позволяет определить базовый перечень инструментальных средств, необходимых для выполнения процессов доказательства безопасности ЖАТ:

1. Средства экспертизы.

1.1. Базы знаний для начальных этапов доказательства безопасности систем ЖАТ (в частности, для получения экспертами информации о возможных безопасных структурах, нормативных документах, системах-аналогах и т. п.).

1.2. Эвристические методы экспертного анализа концептуальных, технических и программных решений на соответствие требованиям функциональной безопасности ЖАТ, безопасности функционирования ЖАТ и безопасности ЖАТ, основой которых является анализ нормативной и конструкторско-технической документации (эксплуатационно-технические требования, программа обеспечения безопасности, техническое задание на устройство или систему и т. п.).

1.3. Средства получения расчетных оценок уровня безопасности и надежности систем ЖАТ (ориентированы на расчетные методы доказательства

безопасности, а также на оценку уровня безопасности на основе статистической информации результатов имитационных и эксплуатационных испытаний).

1.4. Методы и средства статических испытаний и анализа программных средств ЖАТ.

2. Средства испытаний.

2.1. Имитаторы внешней среды программных средств испытываемой ЖАТ.

2.2. Аппаратно-программные имитаторы внешней среды испытуемой ЖАТ (объекты контроля и управления, устройств и подсистем данной ЖАТ, смежных ЖАТ).

2.3. Эмуляторы аппаратно-программных устройств ЖАТ.

2.4. Инструментальные программные средства моделирования релейных и электронных устройств ЖАТ.

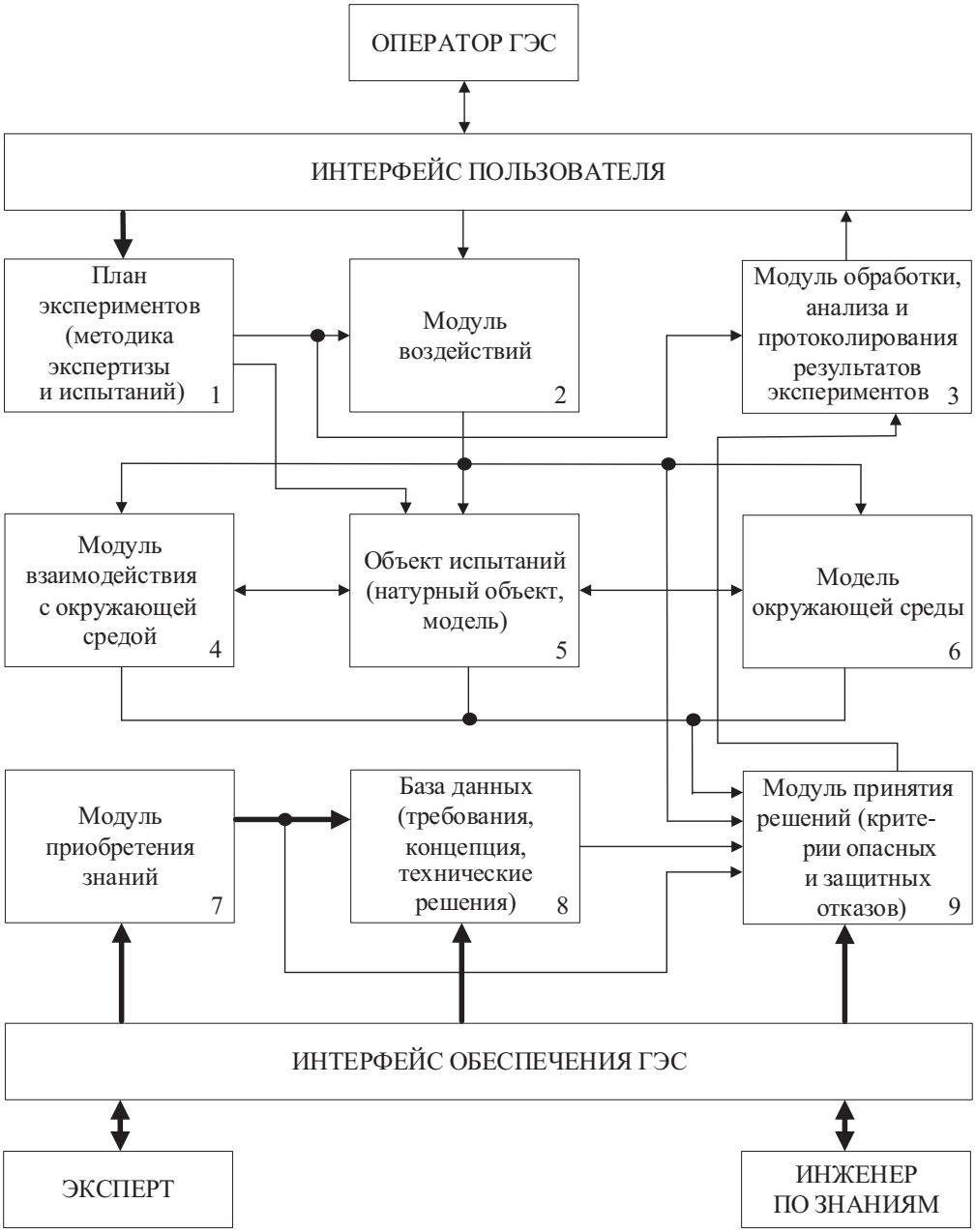
2.5. Инструментальное обеспечение испытаний системы (устройства) ЖАТ на безопасность при воздействии внешних факторов (электромагнитные помехи, климатические и механические воздействия).

Опыт создания и практического применения ряда ИСЭИ в испытательном центре ПГУПС позволяет подтвердить актуальность первого требования, т. е. выполнения разработки ИСЭИ по технологии гибридных экспертных систем (ГЭС). Для испытаний программного обеспечения следует использовать идеологию статических, а для стендовых испытаний аппаратно-программных средств – динамических экспертных систем.

На рисунке приведена обобщенная структура ИСЭИ, синтезированная на основе технологии экспертных систем. Жирными линиями показаны потоки информации, обеспечивающие настройку модулей *1*, *7*, *8*, *9* ИСЭИ на испытываемую систему ЖАТ и конкретные серии экспериментов в соответствии с методикой и программой испытаний. Потоки информации, соединяющие модули *2*, *3*, *4*, *5*, *6*, *9*, обеспечивают выполнение ими указанных функций непосредственно в процессе испытаний. Следует отметить, что предложение использовать технологию экспертных систем не означает необходимость построения всех указанных видов ИСЭИ для всех видов устройств и систем ЖАТ как законченных ГЭС. Применение такой технологии позволяет формализовать процедуры разработки, четко регламентировать состав и структуру ИСЭИ, состав и форму представления исходных данных для выполнения экспериментов, методы и правила принятия решений по результатам в процессе выполнения экспериментов с использованием информации из нормативной, конструкторско-технической документации, а также знаний и эвристических алгоритмов экспертов. Однако для традиционных ЖАТ, таких как электрическая централизация стрелок и сигналов, автоматическая и полуавтоматическая блокировка, автоматическая переездная сигнализация и т. п., безусловно, целесообразно разрабатывать ИСЭИ как экспертные системы. То же самое

относится к отдельным устройствам ЖАТ: схемам управления стрелочными электроприводами, светофорам, рельсовым цепям и т. п.

Следует отметить, что процессы разработки ИСЭИ и взаимопонимание заказчиков и разработчиков ЖАТ, экспертов, аналитиков, инженеров и программистов, создающих ИСЭИ, специалистов сертификационных центров, затруднены недостаточно развитым понятийным аппаратом в области инструментальных средств доказательства безопасности ЖАТ. Нами предложена система терминов и определений, направленная на устранение данного пробела и сформулированная на основе приведенных выше требований и состава ИСЭИ.



Обобщенная структура ИСЭИ

3 Термины и определения

3.1 Характеристики объекта испытаний

Объект испытаний – аппаратные, программные и аппаратно-программные средства ЖАТ, которые подвергаются испытаниям.

Примечание. Под средствами ЖАТ понимаются отдельные устройства, оборудование, система ЖАТ в целом и (или) средства защиты от электромагнитных и других внешних воздействий.

Жизненный цикл ЖАТ – совокупность взаимосвязанных, последовательно выполняемых процессов – от формирования концепции безопасности и исходных требований к системе ЖАТ до вывода ее из эксплуатации и утилизации.

Примечание. Этапы разработки, тиражирования, изготовления и эксплуатации сопровождаются процедурами экспертизы и испытаний ЖАТ на работоспособность и безопасность.

Техническое средство ЖАТ – аппаратная или аппаратно-программная составляющая системы или устройства ЖАТ.

Системное программное обеспечение системы (устройства) ЖАТ – программное обеспечение системы (устройства) ЖАТ, реализующее управление аппаратным обеспечением и предоставляющее прикладной интерфейс программирования для взаимодействия с прикладным программным обеспечением.

Прикладное программное обеспечение системы (устройства) ЖАТ – программное обеспечение системы (устройства) ЖАТ, взаимодействующее с системным программным обеспечением и выполняющее прикладную задачу.

Базовое программное обеспечение системы (устройства) ЖАТ – вид прикладного программного обеспечения системы (устройства) ЖАТ, в котором реализуются алгоритмы, обеспечивающие выполнение требований безопасности программно-аппаратного комплекса независимо от специфики решаемых задач.

Технологическое программное обеспечение системы (устройства) ЖАТ – вид прикладного программного обеспечения системы (устройства) ЖАТ, в котором реализуются технологические функции системы (устройства).

Электромагнитная обстановка ЖАТ – совокупность электромагнитных воздействий на систему (устройство) ЖАТ в местах установки.

Примечание. Местами установки систем (устройства) ЖАТ являются посты электрической централизации, релейные и батарейные шкафы, устройства, устанавливаемые непосредственно на поле.

Электромагнитная совместимость технических средств ЖАТ – способность технического средства ЖАТ функционировать с заданным каче-

ством в заданной электромагнитной обстановке и не создавать недопустимых электромагнитных помех другим техническим средствам.

3.2 Инструментальные средства

Средства расчета показателей безопасности ЖАТ – методы и (или) машинные программы проектной оценки вероятностных показателей безопасности устройств (систем) ЖАТ на основе математических моделей.

Примечание. Математические модели в зависимости от этапа жизненного цикла ЖАТ разработаны или разрабатываются с использованием теории вероятности, математической статистики, байесовских решений, массового обслуживания и рассчитываются по справочным и (или) статистическим данным и результатам имитационного моделирования устройств и систем ЖАТ.

Гибридные экспертные системы ЖАТ – экспертные системы, основу базы знаний которых составляют как эвристические знания экспертов, так и математические модели объектов ЖАТ.

Примечание. База знаний имитаторов ЖАТ, реализованных по технологии ГЭС, формируется на основе имитационных моделей объектов управления, устройств и систем ЖАТ.

Динамические гибридные экспертные системы ЖАТ – гибридные экспертные системы в реальном масштабе времени, непосредственно взаимодействующие на аппаратном, информационном и программном уровне с испытываемой системой (устройством) ЖАТ.

Имитационная модель ЖАТ – программный или программно-аппаратный аналог устройства, системы или объекта управления и контроля ЖАТ, имитирующий набор функций устройства, системы или объекта управления и контроля, определяемый целью моделирования.

Адекватность имитационной модели ЖАТ – степень соответствия имитационной модели объекту моделирования относительно цели моделирования.

Доказательство адекватности имитационной модели ЖАТ – процедура выполнения статических и контрольных динамических экспериментов с имитационной моделью по специальному плану с последующей экспертной оценкой полученных результатов.

Примечания:

1. При положительном результате экспертной оценки имитационная модель признается пригодной для дальнейшего применения.

2. При отрицательном результате экспертной оценки выполняется процедура калибровки имитационной модели, а процедуры доказательства адекватности повторяются.

Испытания имитационных моделей ЖАТ – испытания имитационных моделей с целью оценки работоспособности и безопасности моделируемой системы ЖАТ.

Имитатор системы (устройства) ЖАТ – аппаратный, программный или аппаратно-программный комплекс, предназначенный для имитации системы (устройства) ЖАТ с целью испытания системы (устройства) на работоспособность и безопасность.

Примечание. Основой программных или аппаратно-программных имитаторов системы или устройства являются имитационные модели.

Имитатор внешней среды системы (устройства) ЖАТ – аппаратный, программный или аппаратно-программный комплекс, предназначенный для имитации объекта управления и контроля, подсистемы или смежной системы с целью генерации входных воздействий и восприятия ответных реакций системой (устройством) ЖАТ, проведения испытаний на работоспособность и безопасность.

Эмулятор вычислительных устройств ЖАТ – аппаратно-программный комплекс, предназначенный для имитации и реализация программного кода другого компьютера или системы с целью испытаний модели устройства ЖАТ на работоспособность и безопасность.

Имитаторы электромагнитной обстановки ЖАТ – электротехнические устройства, имитирующие электромагнитную обстановку и соответствующие воздействия на системы (устройства) ЖАТ.

Анализатор программного обеспечения ЖАТ – программное средство, предназначенное для сбора и анализа информации о свойствах программного обеспечения испытываемой системы (устройства) ЖАТ.

Виртуальная машина – программный комплекс, в среде которого функционирует контрольно-испытательное программное обеспечение системы (устройства) ЖАТ.

Примечание. Контрольно-испытательное программное обеспечание доступно для манипуляций с любыми искажениями при обеспечении контроля требуемых показателей программного обеспечения ЖАТ.

Информационное обеспечение испытаний ЖАТ – информационные интерфейсы с операторами ИСЭИ и испытуемой ЖАТ, базы данных, способы получения всех видов информации в соответствии с программой испытаний об объекте и ходе испытаний, ее хранение и систематизация.

Математическое обеспечение испытаний ЖАТ – методы, математические модели, алгоритмы, базы знаний и программы выполнения испытаний в соответствии с программой и методикой испытаний, обработки и анализа информации, полученной в результате испытаний.

Техническое обеспечение испытаний ЖАТ – аппаратные интерфейсы с испытываемой ЖАТ, совокупность устройств получения и обработки ин-

формации (измерительные приборы, датчики, преобразователи, сигнализаторы и т. п.), включая соответствующие имитаторы и эмуляторы ЖАТ.

Протокол испытаний ЖАТ – документ, содержащий необходимые сведения об испытываемой системе (устройстве) ЖАТ, методах, средствах, условиях испытаний, а также результаты испытаний и выводы по ним.

Заключение

Важнейшей задачей решения сложных научно-технических проблем является поддержание коммуникативности участников этого процесса. Особенное значение однозначность взаимопонимания приобретает при разработке и доказательстве безопасности ЖАТ, участниками процесса являются специалисты разных профилей и организации: заказчики, разработчики, эксперты, испытательные и сертификационные центры; предприятия – изготовители аппаратно-программных средств, организации – проектировщики ЖАТ и т. д. Неоднозначность трактовки понятий в области безопасности ЖАТ и практически отсутствие таковых в сфере ИСЭИ в существующих нормативных документах затрудняет взаимодействие участников процессов создания современных ЖАТ и свидетельствует о необходимости развития понятийного аппарата, касающегося безопасности ЖАТ и ИСЭИ. В [5] предложена взаимосвязанная совокупность понятий по безопасности для этапов разработки и доказательства безопасности ЖАТ. Данная работа является продолжением исследований, представленных в [2, 3, 5], и направлена на разработку понятийного аппарата по ИСЭИ.

Получены следующие результаты:

1) сформулированы задачи доказательства безопасности ЖАТ;

2) определены свойства ЖАТ как объекта испытаний;

3) на основе анализа задач и свойств ЖАТ сформулированы требования к ИСЭИ;

4) показана целесообразность разработки ИСЭИ с использованием технологии ГЭС;

5) определен перечень ИСЭИ, необходимых для выполнения работ по доказательству безопасности ЖАТ;

6) предложена совокупность взаимосвязанных понятий по ИСЭИ ЖАТ на безопасность.

Перспективы:

1) совершенствование понятийного аппарата для процессов разработки и аттестации нестандартных ИСЭИ;

2) определение этапов жизненного цикла и терминологии для всех этапов – от формирования концепции синтеза и исходных требований к ИСЭИ до их аттестации как средств экспертизы и испытаний ЖАТ на безопасность.

Следует отметить, что разработка и эксплуатация ИСЭИ должны сопровождаться (на всех этапах жизненного цикла) процедурами верификации и валидации – от формирования концепции и исходных требований до применения ИСЭИ для экспертизы и испытаний конкретной ЖАТ. Сущность верификации заключается в доказательстве соответствия результатов выполнения данного этапа синтеза ИСЭИ исходным требованиям (например, оценка полноты и корректности концепции и требований к ИСЭИ). Процедуры валидации направлены на убеждение в том, что результаты данного этапа пригодны для выполнения следующего. Конечным результатом выполнения процедур верификации и валидации является аттестация ИСЭИ. Процессы верификации и валидации особенно важны для обеспечения качества разработки и применения ИСЭИ и, следовательно, требуют особенно тщательной разработки соответствующего понятийного аппарата, что является одной из основных перспективных задач исследований в данной области.

Библиографический список

1. Сапожников Вал. В. Методы и средства оценки и обеспечения безопасности систем железнодорожной автоматики / Вал. В. Сапожников, Вл. В. Сапожников, Д. В. Гавзов, Д. С. Марков // Автоматика, телемеханика и связь. – 1992. – № 1. – С. 4–7.
2. Наседкин О. А. Особенности испытания МПУ ЖАТ / О. А. Наседкин, Е. В. Ледяев // Автоматика, связь, информатика. – 2012. – № 7. – С. 30–32.
3. Наседкин О. А. Методическое и техническое обеспечение испытаний микропроцессорных систем / О. А. Наседкин, Д. А. Васильев, А. М. Белоус // Автоматика, связь, информатика. – 2013. – № 12. – С. 23–27.
4. Белишкина Т. А. Особенности подтверждения соответствия требованиям безопасности железнодорожной автоматики в переходный период после принятия технических регламентов таможенного союза / Т. А. Белишкина // Автоматика на транспорте. – 2016. – Т. 2. – № 2. – С. 208–227.
5. Марков Д. С. Терминологические особенности этапов разработки и доказательства безопасности железнодорожной автоматики и телемеханики / Д. С. Марков, О. А. Наседкин, Д. А. Васильев, М. А. Бутузов // Автоматика на транспорте. – 2017. – Т. 3. – № 3. – С. 368–379.
6. ГОСТ Р МЭК 61508-4–2012. Функциональная безопасность систем электрических, электронных программируемых электронных, связанных с безопасностью. Ч. 4. Термины и определения. – М. : Стандартинформ, 2014. – 20 с.
7. ГОСТ Р 54504–2011. Безопасность функциональная. Политика, программа обеспечения безопасности. Доказательство безопасности объектов железнодорожного транспорта. – М. : Стандартинформ, 2013. – 24 с.
8. ГОСТ Р МЭК 61511-1–2011. Безопасность функциональная. Системы безопасности приборные промышленных процессов. Ч. 1. Термины, определения и технические требования. – М. : Стандартинформ, 2013. – 65 с.

9. ГОСТ Р 53431–2009. Автоматика и телемеханика железнодорожная. Термины и определения. – М. : Стандартинформ, 2010. – 19 с.
10. Никитин А. Б. Анализ компьютерных систем оперативного управления устройствами ЭЦ / А. Б. Никитин, Вал. В. Сапожников // Автоматика, связь, информатика. – 2006. – № 6. – С. 6–8.
11. Никитин А. Б. Комплекс технических средств управления и контроля / А. Б. Никитин, С. В. Ракчеев, М. В. Сидоров, М. Г. Максимов // Автоматика, связь, информатика. – 2007. – № 2. – С. 7–12.
12. Никитин А. Б. Повышение эффективности систем электрической централизации / А. Б. Никитин // Автоматика связь, информатика. – 2010. – № 4. – С. 4–7.
13. Марков Д. С. Матричный метод формализации имитационных моделей сложных систем массового обслуживания / Д. С. Марков, П. Е. Булавский // Известия Петербургского университета путей сообщения. – 2010. – № 4. – С. 186–196.
14. Марков Д. С. Метод формализации имитационных моделей технологических процессов в хозяйстве автоматики и телемеханики на железнодорожном транспорте / Д. С. Марков, А. А. Лыков // Известия Петербургского государственного университета путей сообщения. – 2012. – № 1.– С. 23– 28.

Dmitry S. Markov,
Oleg A. Nasedkin,
Denis A. Vasil'ev,
Maxim A. Butuzov
«Automation and remote control on railways» department
Emperor Alexander I St. Petersburg state transport university

Definitions and terminology of expertise and testing of railway automation for safety

The necessity of a conceptual apparatus development in the area of expertise and testing tools of railway automation and remote control systems and devices for working capacity and safety is demonstrated in accordance with the requirements of different stages of the lifecycle, foremost for those that are connected with processes of safety development and proving. This is determined by the fact that there is practically no terminology on non-standard instrumental means in existing regulatory documents, and it makes understanding between different specialists and teams, which are involved in the processes of safety development and proving of railway automation and remote control, difficult. The requirements are formulated and the composition of instrumental means is determined based on the analysis of the problem of safety proving and the characteristics of railway automation as an object of expertise and testing. It is proved that it is expedient to develop simula-

tors of various types on the basis of the hybrid expert systems technology, which makes it possible to use effectively heuristic expert algorithms and mathematical, as a rule, simulation models of control objects, devices, subsystems and systems of railway automation as a knowledge base in one test facility. On this basis, this paper offers the complex of terms and definitions for instrumental means of expertise and testing, which is a the methodological basis for further development of regulatory documentation in the area of safety and working capacity proving of railway automation and remote control.

railway automation and remote control; lifecycle; safety development and proving; safety of functioning; instrumental means of expertise and testing; simulators; hybrid expert systems

References

1. Sapozhnikov Val. V., Sapozhnikov Vl. V., Gavzov D. V., Markov D. S. (1992). Methods and means of assessing and ensuring the safety of railway automation systems [Metody i sredstva ocenki i obespecheniya bezopasnosti sistem zheleznodorozhnoj avtomatiki]. Automation, remote control and communication [Avtomatika, telemekhanika i svyaz’], issue 1. – Pp. 4–7.
2. Nasedkin O. A., Ledyaev E. V. (2012). Features of testing of microprocessor devices of railway automatics and telemechanics [Osobennosti ispytaniya MPU ZHAT]. Automation, communication, information science [Avtomatika, svyaz’, informatika], issue 7. – Pp. 30–32.
3. Nasedkin O. A., Vasil’ev D. A., Belous A. M. (2013). Methodical and technical support of tests of microprocessor systems [Metodicheskoe i tekhnicheskoe obespechenie ispytanij mikroprocessornyh sistem]. Automation, communication, information science [Avtomatika, svyaz’, informatika], issue 12. – Pp. 23–27.
4. Belishkina T. A. (2016). Features of Confirmation of Conformity to the Requirements of Railway Automation and Remote Control Safety During The Transition Period after Acceptance Of Technical Regulations Of The Customs Union [Osobennosti podtverzhdeniya sootvetstviya trebovaniyam bezopasnosti zheleznodorozhnoj avtomatiki v perekhodnyj period posle prinyatiya tekhnicheskih reglamentov tamozhennogo soyuza]. Automation on Transport [Avtomatika na transporte], vol. 2, issue 2. – Pp. 208–227.
5. Markov D. S., Nasedkin O. A., Vasil’ev D. A., Butuzov M. A. (2017). Terminological peculiarities of stages of railway automatics and telemechanics safety development and proving [Terminologicheskie osobennosti ehtapov razrabotki i dokazatel’stva bezopasnosti zheleznodorozhnoj avtomatiki i telemekhaniki]. Automation on transport [Avtomatika na transporte], vol. 3, issue 3. – Pp. 368–379.
6. GOST R MEK 61508-4–2012. Functional safety of electrical, electronic programmable electronic systems related to safety. Part 4: Terms and Definitions [GOST R MEHK 61508-4–2012 Funkcional’naya bezopasnost’ sistem ehlektricheskih,

ehlektronnyh programmiruemyh ehlektronnyh, svyazannyh s bezopasnost'yu. Chast' 4: Terminy i opredeleniya]. Moscow, Standartinform [Standartinform]. – 20 p.
7. GOST R 54504–2011. Functional safety. Policy, safety program. Proof of the safety of railway transport facilities [GOST R 54504–2011. Bezopasnost' funkcional'naya. Politika, programma obespecheniya bezopasnosti. Dokazatel'stvo bezopasnosti ob'ektov zheleznodorozhnogo transporta]. Moscow, Standartinform [Standartinform]. – 24 p.
8. GOST R MEC 61511-1–2011. Functional safety. Safety systems instrument industrial processes. Part 1: Terms, definitions and technical requirements [GOST R MEHK 61511-1–2011. Bezopasnost' funkcional'naya. Sistemy bezopasnosti pribornye promyshlennyh processov. Chast' 1: Terminy, opredeleniya i tekhnicheskie trebovaniya]. Moscow, Standartinform [Standartinform]. – 65 p.
9. GOST R 53431–2009. Railway automation and remote control. Terms and Definitions [GOST R 53431–2009.Avtomatika i telemekhanika zheleznodorozhnaya. Terminy i opredeleniya]. Moscow, Standartinform [Standartinform]. – 19 p.
10. Nikitin A. B., Sapozhnikov Val. V. (2006). Analysis of computer-based systems of operational control of electric centralization devices [Analiz komp'yuternykh sistem operativnogo upravleniya ustroystvami ETs]. Automation, communication, information science (Avtomatika, svyaz', informatika), issue 6. – Pp. 6–8.
11. Nikitin A. B., Rakcheev S. V., Sidorov M. V., Maksimov M. G. (2007). Complex of technical facilities for control and management [Kompleks tekhnicheskikh sredstv upravleniya i kontrolya]. Automation, communication, information science (Avtomatika, svyaz', informatika), issue 2. – Pp. 7–12.
12. Nikitin A. B. (2010). Improving of electrical interlocking systems efficiency [Povysheniye effektivnosti sistem elektricheskoy tsentralizatsii]. Automation, communication, information science (Avtomatika, svyaz', informatika), issue 4. – Pp. 4–7.
13. Markov D. S., Bulavsky P. E. (2010). Matrix method of formalization of simulation models of complex mass service systems. Proceedings of Petersburg Transport University, issue 4. – Pp. 186–196.
14. Markov D. S., Lykov A. A. (2012). Method for formalization of simulation models of technological processes within railway transport automation and remote control facilities [Metod formalizatsii imitatsionnykh modeley tekhnologicheskikh protsessov v khozyaystve avtomatiki i telemekhaniki na zheleznodorozhnom transporte]. Proceedings of PSTU (Izvestiya PGUPS), issue 1. – Pp. 23–28.

Статья представлена к публикации членом редколлегии Вал. В. Сапожниковым
Поступила в редакцию 15.11.2017, принята к публикации 08.12.2017

МАРКОВ Дмитрий Спиридонович – кандидат технических наук, доцент кафедры «Автоматика и телемеханика на железных дорогах» Петербургского государственного университета путей сообщения Императора Александра I.
e-mail: MDS1945@yandex.ru

НАСЕДКИН Олег Андреевич – кандидат технических наук, доцент кафедры «Автоматика и телемеханика на железных дорогах» Петербургского государственного университета путей сообщения Императора Александра I.
e-mail: nasedkin@crtc.spb.com

ВАСИЛЬЕВ Денис Анатольевич – старший научный сотрудник Центра компьютерных железнодорожных технологий кафедры «Автоматика и телемеханика на железных дорогах» Петербургского государственного университета путей сообщения Императора Александра I.
e-mail: denvas@crtc.spb.com

БУТУЗОВ Максим Алексеевич – старший научный сотрудник Центра компьютерных железнодорожных технологий кафедры «Автоматика и телемеханика на железных дорогах» Петербургского государственного университета путей сообщения Императора Александра I.
e-mail: max@crtc.spb.com