УДК 656.25

И. И. АКСЮТИК, начальник службы сигнализации и связи Белорусской железной дороги; К. А. БОЧКОВ, доктор технических наук, проректор по учебной работе; С. Н. ХАРЛАП, кандидат технических наук, доцент; Белорусский государственный университет транспорта, г. Гомель

МЕТОДЫ ПРОВЕДЕНИЯ ИСПЫТАНИЙ НА БЕЗОПАСНОСТЬ ФУНКЦИОНИРОВАНИЯ И ЭМС МИКРОЭЛЕКТРОННЫХ СИСТЕМ УПРАВЛЕНИЯ ОТВЕТСТВЕННЫМИ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ

Изложены основные методы проведения испытаний на безопасность функционирования и электромагнитную совместимость микроэлектронных систем управления ответственными технологическими процессами. Раскрыты вопросы построения моделей микроэлектронных систем и проведения имитационных испытаний на безопасность. Обоснована необходимость проведения комплексных испытаний на безопасность и электромагнитную совместимость.

Начиная с 80-х годов XX века во всем мире при автоматизации ответственных технологических процессов, связанных с угрозой жизни людей, значительными материальными потерями и негативным воздействием на окружающую среду, все большее применение находят микроэлектронные системы обеспечения безопасности (СОБ). К таким системам относятся устройства и системы управления движением поездов, системы лифтовой и газовой автоматики, системы управления химическими производствами, системы управления транспортными средствами, технические средства контроля состояния опасных технологических процессов и т.п. Отказы СОБ, приводящие к нарушению условий безопасности функционирования, называют опасными.

Дальнейшее развитие систем обеспечения безопасности связано, в первую очередь, с повышением требований к их эксплуатационным и информационным функциям, к безотказности и отказоустойчивости систем, т.к. передача все большего числа функций от человека устройствам автоматики увеличивает экономические затраты в связи с отказом [1]. Недостатками релейных систем обеспечения безопасности являются незначительные размеры, высокая материалоемкость и наличие дефицитных материалов. Поэтому развитие средств автоматики и телемеханики в ближайшем будущем будет связано с совершенствованием микроэлектронной, микропроцессорной и компьютерной техники.

Проблема перехода на новую элементную базу очень остро стоит на Белорусской железной дороге. Большинство эксплуатируемых релейных систем либо уже выработало свой ресурс, либо выработает его в ближайшее время. В наиболее критичном состоянии находятся системы автоматической и полуавтоматической блокировки, где в настоящее время эксплуатируется с истекшим сроком эксплуатации 25 % систем, а при существующих темпах реконструкции и замены к 2003 году таких систем будет уже 50 %.

Последние годы на Белорусской железной дороге характеризуются началом опытной эксплуатации нового поколения систем железнодорожной автоматики и телемеханики с использованием микроэлектронной и микропроцессорной элементной базы, таких как ДЦ «Неман», КТСМ и др.

Однако, несмотря на преимущества этих систем: малая материало- и энергоемкость, большие функциональные возможности, высокие расчетные показатели надежности, малые габаритные размеры – их широкое внедрение и практическое использование сдерживаются по нескольким причинам:

- неочевидность достаточного уровня безопасности систем на микроэлектронной и программируемой элементной базе;
- наличие психологического барьера у эксплуатационного и обслуживающего персонала при вводе в эксплуатацию систем нового поколения;
- сложность процедур доказательства и подтверждения безопасности таких систем;
- отсутствие достаточного опыта сопровождения и эксплуатации таких систем;
- высокая чувствительность к воздействию электромагнитных помех различного вида.

Одной из причин сравнительно медленного внедрения бесконтактной техники в устройствах СЖАТ также являлось отсутствие достоверных методов определения уровня безопасности микроэлектронных и микропроцессорных систем и устройств. Вместе с тем, за последние 10 лет в МПС РФ накоплен определенный опыт решения этих проблем. В начале 90-х годов были разработаны и введены в действие в России нормативные документы «Безопасность железнодорожной автоматики и телемеханики», составляющие методическую основу для проведения сертификации СЖАТ на безопасность. Созданы орган по сертификации и три испытательные лаборатории в Москве и Санкт-Петербурге, обладающие статусом технической компетентности и независимости и имеющие

следующие области аккредитации [2]:

- программные и аппаратные средства микроэлектронных систем ЖАТ, электромагнитная совместимость устройств ЖАТ (Петербургский государственный университет путей сообщения);
- средства измерения и контроля устройств технического обеспечения движения поездов, программные средства автоматизированных систем управления движением поездов (Всероссийский научно-исследовательский институт управления МПС РФ),
- электромагнитная совместимость устройств ЖАТ (Московский государственный университет путей сообщения).

В 1998–1999 гг. Белорусский государственный университет при активной поддержке Белорусской железной дороги начал работы по созданию и аккредитации испытательной лаборатории для проведения испытаний на безопасность и электромагнитную совместимость (ЭМС) микроэлектронных, микропроцессорных и компьютерных технических средств железнодорожной автоматики и телемеханики. За два года коллективом лаборатории и службой сигнализации и связи Белорусской железной дороги был разработан ряд руководящих документов Республики Беларусь, определяющих необходимую нормативную базу для проведения испытаний на безопасность и ЭМС современных систем железнодорожной автоматики. К этим документам относятся:

1 РД РБ БЧ 19.048-98. Безопасность железнодорожной автоматики и телемеханики. Основные понятия. Термины и определения.

2 РД РБ БЧ 19.049-98. Безопасность железнодорожной автоматики и телемеханики. Выбор, общие правила нормирования и методы расчета показателей безопасности.

3 РД РБ БЧ 19.050-98. Безопасность железнодорожной автоматики и телемеханики. Безопасность программного обеспечения.

4 РД РБ БЧ 19.055-99. Безопасность железнодорожной автоматики и телемеханики. Общие положения, порядок и методы проведения испытаний на безопасность.

5 РД РБ БЧ 19.057-99. Безопасность железнодорожной автоматики и телемеханики. Общие положения, порядок и методы доказательства безопасности систем и устройств железнодорожной автоматики и телемеханики.

6 РД РБ БЧ 19.058-99. Методика испытаний на электромагнитную совместимость систем диспетчерской централизации. Общие положения. Порядок и методы проведения испытаний.

7 РД РБ БЧ 19.059-99. Методика испытаний блоков и узлов технических средств железнодорожной автоматики и телемеханики на устойчивость к внешним электромагнитным помехам. Общие положения. Порядок и методы проведения испытаний.

8 РД РБ БЧ 19.062-99. Безопасность железнодорожной автоматики и телемеханики. Порядок разработки и общие требования к содержанию программ обеспечения безопасности.

В 1998 году коллективом лаборатории во главе с руководителем доктором технических наук, профессором К. А. Бочковым был выигран гранд Министерства образования Республики Беларусь на приобретение уникального испытательного оборудования фирмы “Schaffner” – мирового лидера по производству испытательного оборудования на ЭМС. При финансовой поддержке Белорусской железной дороги была открыта и аккредитована на техническую компетентность и независимость (аттестат аккредитации № BY/112 02.1.0.0364) научно-исследовательская и испытательная лаборатория «Безопасность и ЭМС технических средств».

За время работы в лаборатории проведено свыше 70 испытаний на безопасность и ЭМС различных устройств, в том числе технических средств центрального поста и линейного пункта диспетчерской централизации (ДЦ) «Неман», а также экспертиза технической документации и доказательства безопасности ДЦ «Неман». Разработаны и утверждены программы обеспечения безопасности, программы и методики проведения испытаний на безопасность и электромагнитную совместимость различных технических средств.

Коллективом лаборатории проводятся научные исследования, результаты которых постоянно докладываются на самых престижных международных симпозиумах в Японии (1994 г.), Франции (1994 г.), Италии (1994, 1996 и 1998 гг.), Польше (1992, 1994, 1996 и 2000 гг.) и Югославии (2000 г.).

В сентябре 2001 года в Белорусском государственном университете транспорта при содействии Белорусской железной дороги прошел Международный семинар «Испытания систем железнодорожной автоматики и телемеханики на безопасность и электромагнитную совместимость». В работе семинара приняли участие ведущие ученые и специалисты из России, Беларуси, Украины, Польши, Молдовы и Литвы, представляющие следующие организации и учреждения: Департамент СЦБ МПС РФ, ВНИИУП МПС РФ, ВНИИЖТ, Регистр по сертификации МПС РФ, ГТСС, МГУ ПС, ПГУ ПС, Белорусскую железную дорогу, БелГУТ, Центр сертификационных испытаний на ЭМС и безопасность Харьковской государственной академии железнодорожного транспорта, Научно-технический Центр польских железных дорог, Молдавскую железную дорогу, литовские железные дороги.

Участники семинара отметили, что БелГУТ обладает высококвалифицированными кадрами, имеет современную базу и необходимое оборудование в области испытаний на безопасность и электро-

магнитную совместимость (ЭМС), и рекомендовали провести аккредитацию испытательной лаборатории «Безопасность и ЭМС ТС» БелГУТа в системе Регистра по сертификации МПС РФ. Это необходимо для проведения совместных исследований и испытаний на безопасность функционирования и ЭМС микроэлектронных ТС ЖАТ и более полного использования возможностей уникального оборудования лаборатории.

Лаборатория располагает современным оборудованием швейцарской фирмы “Schaffner” – мирового лидера испытательной техники в области ЭМС, оборудованием давно известной и хорошо зарекомендовавшей себя немецкой фирмы “RFT”, современным компьютерным оборудованием (как стационарным, так и переносным) для проведения испытаний на ЭМС и имитационных испытаний на безопасность (рисунок 1). Данное оборудование по своим характеристикам значительно превосходит оборудование, применяемое для испытаний в других лабораториях, например, в аналогичной по области аккредитации ИЛ ПГУ ПС.

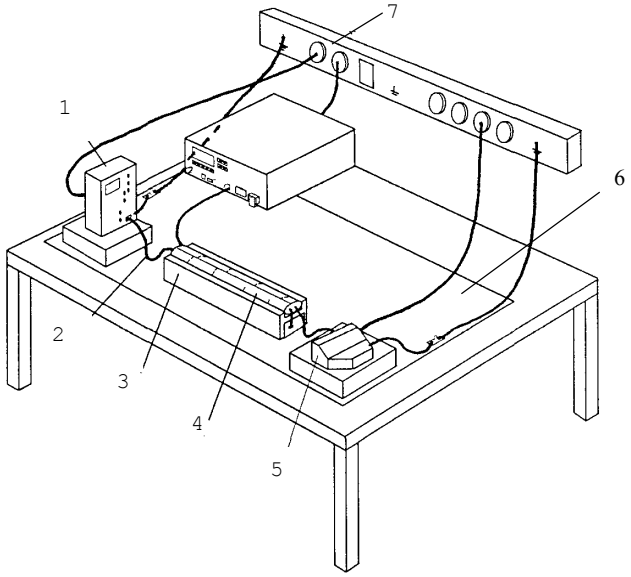

Рисунок 1 – Рабочее место для испытаний технических средств на устойчивость к пачкам помех с использованием испытательного оборудования «*Shaffner*»:
1- периферия; 2 – кабель между испытуемым объектом и периферией; 3 – опора клещей связи; 4 – емкостные клещи связи; 5 – испытуемый объект; 6 – плоскость заземления; 7 – розетки электропитания

Опыт использования этого оборудования при испытаниях и научных исследованиях показал, что испытания на безопасность функционирования и ЭМС необходимо проводить в комплексе, а не раздельно, как предусмотрено в действующих методиках. Это связано с тем, что под воздействием электромагнитных помех могут формироваться сигналы управления, влияющие на безопасность движения поездов. Уровень помех, при котором наблюдается формирование сигналов управления, зависит от большого числа факторов (типа аппаратуры, взаимного расположения, температуры и т.д.) и часто значительно ниже нормативного значения. Воздействие же помехами нормативного уровня не приводит к формированию команд управления из-за сбоев аппаратуры. Поэтому для определения необходимого уровня помех, вызывающих сбои в аппаратуре, необходимо проводить исследования уровня помехозащищенности устройств и систем железнодорожной автоматики. Выполнить такие исследования на другом оборудовании не представляется возможным из-за отсутствия средств плавного регулирования уровня электромагнитной помехи.

Современные микроэлектронные системы состоят из десятков миллионов элементарных структур, отказ каждой из которых может привести к нарушению условий безопасности функционирования всей системы. Поэтому основным способом анализа и доказательства безопасности являются имитационные испытания моделей аппаратных и программных средств. Наиболее сложной проблемой при проведении имитационных испытаний является разработка математических моделей микроэлектронных систем, методов анализа и доказательство их адекватности. Для проведения экспериментов модель должна позволять вносить разнообразные отказы и сбои аппаратных средств во время обработки входных воздействий. В существующих системах автоматизированного проектирования микроэлектронных систем имитация отказов затруднена из-за отсутствия доступа к внутренним элементам имитационной модели и возможна только в ручном режиме, что исключает возможность полного анализа последствий даже отдельных видов отказов.

Кроме того, к нарушениям условий безопасности могут привести не только отказы элементов микроэлектронных систем управления, но и сбои, вызванные действием электромагнитных помех. Сбои в работе микроэлектронных систем – явления на порядок, а то и выше более частые, чем отказы, а последствия от влияния помех в конечном итоге проявляются так же, как отказы аппаратных средств или ошибки программного обеспечения. Вследствие этого имитационная модель должна учитывать влияние электромагнитных помех, проявляющееся в виде сбоев аппаратных и программных средств.

Авторами предлагается новый подход к проведению испытаний на безопасность на основе результатов математического моделирования. Разработана обобщенная формализованная модель функционирования микроэлектронных систем, которая отличается от известных моделей учетом особенностей работы системы при отказах и сбоях ее элементов. Построение модели осуществляется на базе обобщенной переходной системы [3] с использованием современного аппарата теории автоматов, теории алгоритмов и имитационного моделирования.

Моделирование отказов дискретных объектов предлагается выполнять следующим образом [4]. Отказ элемента предполагает искажение выходной информации по сравнению с выходной информацией исправного элемента. Искажение может произойти в результате искажения входных сигналов, искажения функции, реализуемой элементом, или искажения выходных сигналов. Искажения входных и выходных сигналов легко реализуются наложением «маски» на определенные входы или выходы элемента. Описать искажение функционирования сложных элементов (например, микропроцессоров) из-за большого разнообразия отказов и их влияния на алгоритм работы очень сложно. Однако всегда можно подобрать такие входные и выходные искажения информации, которые по своим проявлениям будут эквивалентны отказам во внутренней структуре элемента.

Поведение дискретных объектов с памятью зависит не только от значений входов, но также от его состояний. При этом один и тот же объект в ответ на одну и ту же входную последовательность может выдавать различные выходные последовательности в зависимости от того, в каком начальном состоянии находился объект. В этом случае недостаточно искажать только значения выходов элемента. Требуется дополнительное искажение внутренних состояний объекта (рисунок 2).

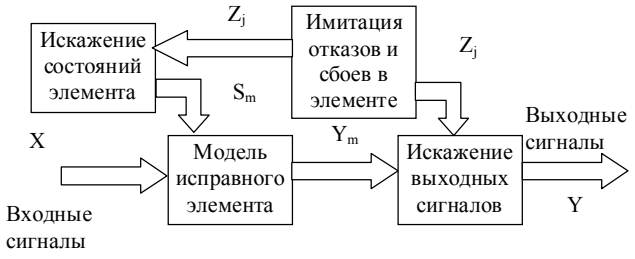

Рисунок 2 – Структура модели дискретного объекта с памятью

Рассмотрим в качестве примера модель D-триггера, учитывающую константные неисправности «1→0». Элемент описывается конечным автоматом вида

$$V_{dtr}^{*} = (A_{dtr}^{*}, S_{dtr}^{*}, B_{dtr}^{*}, \varphi_{dtr}^{*}, \psi_{dtr}^{*}), \qquad (1)$$

где $A_{dtr}^{*} = \{a_1, a_2, a_3, a_4, a_5\}$ – входной алфавит D-триггера, a_1 и a_2 – входы установки и сброса триггера, a_3 – вход синхронизации, a_4 – информационный вход, a_5 – внешний сигнал неисправности (a_5 =0 – элемент неисправен, a_5 =1 – элемент исправен); $S_{dtr}^{*} = \{s_1, s_2, s_3, s_4\}$ – множество состояний элемента, s_1 и s_2 – соответствуют значениям “0” и “1” в памяти элемента, s_3 – неопределенное состояние, s_4 – неисправное состояние; $B_{dtr}^{*} = \{0, 1\}$ – выходной алфавит элемента; φ_{dtr}^{*} и ψ_{dtr}^{*} – функции переходов и функции выходов элемента, учитывающие его отказ и восстановление.

Получив описание элементов схемы в виде абстрактных конечных автоматов, выполняют построение модели. Модель представляет собой структурный автомат, схема взаимосвязей которого задается обобщенной переходной системой согласно [3].

Для проведения имитационных испытаний на безопасность разработаны собственные оригинальные методики, отличающиеся от известных учетом влияния проблемы ЭМС на безопасность функционирования микроэлектронных СЖАТ. При этом на первом этапе проведения имитационных испытаний на наличие опасных отказов анализируется поведение системы (функциональная безопасность) при всех возможных константных неисправностях как одиночных, так и кратных, а также при программном задании сбоев всех элементов. Это дает возможность выявить как опасные отказы, так и узлы и элементы СЖАТ, наиболее подверженные влиянию сбоев (слабые по ЭМС места СЖАТ).

На втором этапе при проведении физических испытаний этих систем на ЭМС с помощью имитаторов помех электромагнитные помехи различного вида помимо предусмотренных стандартами точек подаются на слабые по ЭМС точки системы. Это позволяет существенно повысить адекватность комплексных испытаний на безопасность и ЭМС и их жесткость.

В лаборатории разработан комплекс аппаратно-программных средств для проведения имитационных испытаний на безопасность функционирования микроэлектронных и микропроцессорных систем железнодорожной автоматики и телемеханики (КИИБ).

Комплекс включает в себя имитационный комплекс для испытаний на безопасность цифровых схем (КИИБ-ц) и имитационный комплекс для испытаний на безопасность микропроцессорных систем (КИИБ-м).

Имитационный комплекс для испытаний на безопасность цифровых схем представляет собой библиотеку специализированных компонентов C++Builder и несколько вспомогательных программ. Он предназначен для проведения имитационных испытаний микроэлектронных устройств при наличии отказов и сбоев их элементов для определения таких характеристик, как самопроверяемость (способность обнаруживать отказы и сбои элементов внутренней структуры), помехоустойчивость, устойчивость работы при изменении временных параметров компонентов. Комплекс имеет средства автоматизации испытаний и специальное программное обеспечение для анализа результатов испытаний.

Имитационный комплекс для испытаний на безопасность микропроцессорных систем пред-

ставляет собой библиотеку объектов в виде подгружаемых динамических библиотек DLL (dynamic-link libraries). Каждый объект моделирует определенный элемент микропроцессорной системы. Дополнительно разрабатывается эмулятор объекта управления (рисунок 3).

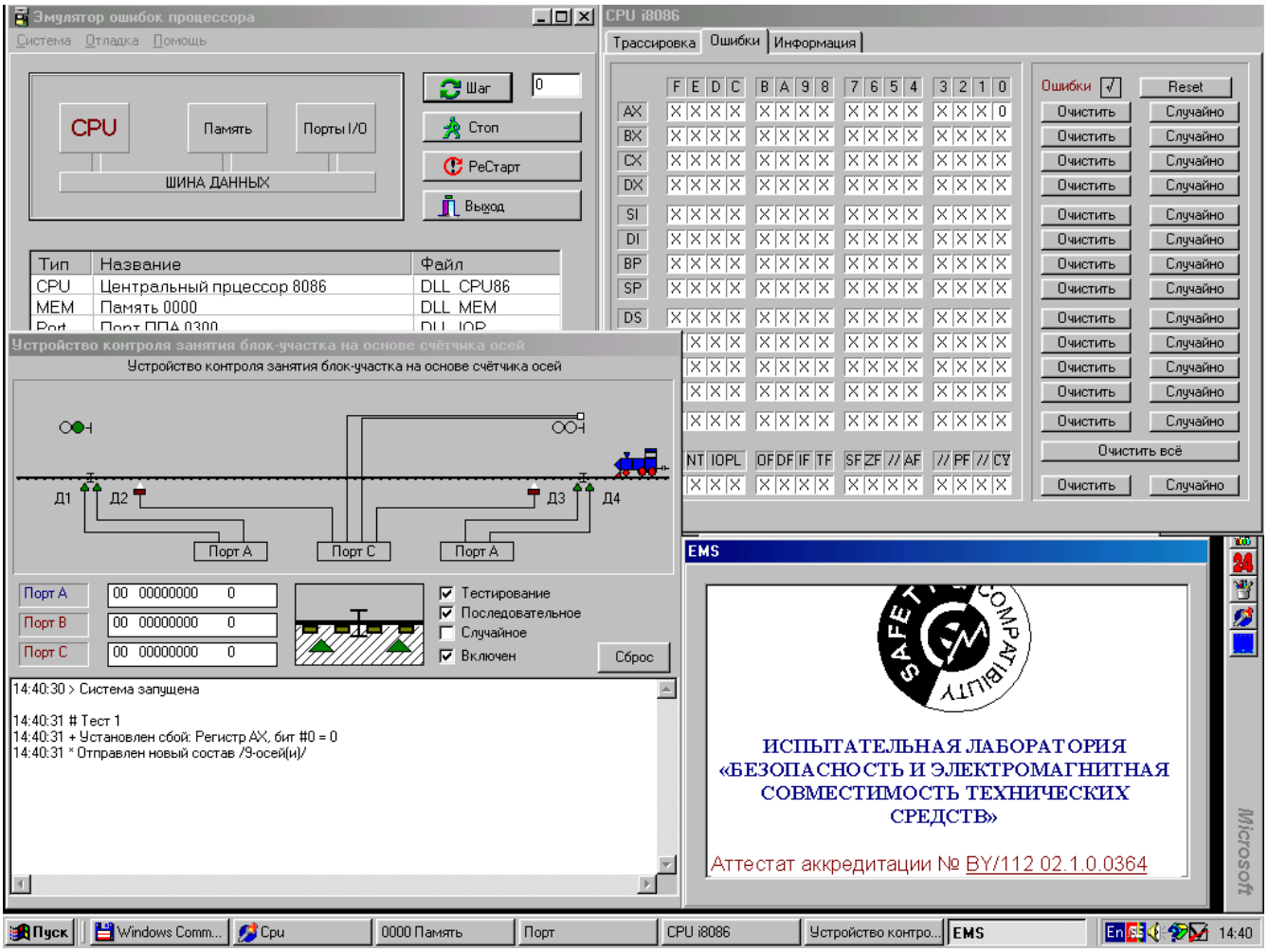

Рисунок 3 – Имитационный комплекс для испытаний на безопасность микропроцессорных систем КИИБ-м

Комплекс позволяет имитировать различные отказы и сбои в работе отдельных объектов и предназначен для проведения имитационных испытаний на безопасность программно-технических средств на базе микроконтроллеров и компьютеров. Определяются такие характеристики, как устойчивость функционирования, уровень обнаруживаемости отказов средствами контроля и диагностики, возможность накопления отказов и сбоев аппаратных и программных средств. Комплекс имеет средства автоматизации испытаний и специальное программное обеспечение для анализа результатов испытаний.

Лаборатория выполняет следующие виды работ:

– научно-техническая экспертиза принятых разработчиками технических решений на соответствие нормам и принципам построения безопасных микроэлектронных и компьютерных систем;

– разработка необходимой технической документации, например, программ обеспечения безопасности, программ и рабочих методик испытаний и др.;

– проведение испытаний на безопасность технологических алгоритмов, реализованных программным способом;

- проведение испытаний на безопасность при воздействии электромагнитных помех;
- проведение испытаний на достоверность передачи команд в системах телемеханики;
- проведение испытаний технических средств по показателям электромагнитной совместимости;
- проведение имитационных испытаний микроэлектронных устройств при наличии отказов и сбоев их элементов для определения таких характеристик, как самопроверяемость (способность обнаруживать отказы и сбои элементов внутренней структуры), помехоустойчивость, устойчивость работы при изменении временных параметров компонентов;
- проведение имитационных испытаний программно-технических средств на базе микроконтроллеров и компьютеров при наличии отказов и

сбоев аппаратных и программных средств для определения таких характеристик, как устойчивость функционирования, уровень обнаруживаемости отказов средствами контроля и диагностики, возможность накопления отказов во внутренней структуре;

- проведение комплексных испытаний на безопасность функционирования микроэлектронных и компьютерных систем.

Более подробную информацию о лаборатории, области аккредитации, выполняемых работах можно получить на сайте http://EMCLab.at.tut.by.

Таким образом, в настоящее время в лаборатории разработаны формализованные методы, позволяющие на основе использования единых принципов моделировать системы, состоящие из базовых элементов различной степени сложности, сохраняя при этом общие алгоритмы проверки. Использование таких методов моделирования позволяет автоматизировать процесс создания модели, снять ограничения по элементной базе моделируемых систем, моделировать специальные парафазные дискретные устройства, снизить требования к ресурсам ЭВМ и уменьшить время проверки за счет более эффективных алгоритмов анализа, способствует совершенствованию методов проведения испытаний на безопасность и повышению их адекватности. Данные испытания базируются на оригинальных методиках имитации отказов и сбоев в сложных устройствах и результатах научных исследований с использованием испытательного оборудования фирмы “Schaffner”.

Проведение имитационных испытаний компьютерной системы диспетчерской централизации «Неман» с помощью КИИБ-м позволило выявить ряд недостатков программного обеспечения (в том числе несколько влияющих на надежность и безопасность функционирования системы). Участники Международного семинара «Испытания систем железнодорожной автоматики и телемеханики на безопасность и электромагнитную совместимость» подтвердили, что в таком объеме имитационные испытания в России не проводятся.

В настоящее время проводятся работы по аккредитации испытательной лаборатории в Регистре сертификации на федеральном железнодорожном транспорте Российской Федерации.

Список литературы

1 Методы построения безопасных микроэлектронных систем железнодорожной автоматики / *В. В. Сапожников, В. В. Сапожников, Х. А. Христов, Д. В. Гавзов*; Под ред. *В. В. Сапожникова*. – М.: Транспорт, 1995. – 272 с.

2 Сертификация средств железнодорожной автоматики и телемеханики // Железнодорожный транспорт. Сер. Сигнализация и связь (экспресс-информ.). 1998. Вып. 4. 14 с.

3 *S. N. Kharlap*. Program Module to Detect and Register Errors and Failures of Microelectronic Devices // Proceedings international symposium on electromagnetic compability. – Wroclaw, 1996. – P. 651–653.

4 *Бочков К. А., Харлап С. Н., Логвиненко А. В.* Моделирование отказов и сбоев в микроэлектронных и микропроцессорных системах железнодорожной автоматики // “Інформаційно-кіруючі системи на залізничному транспорті”: Междунар. науч.-техн. журнал. – Харьков, 2000. № 3. – С. 28–38.

Получено 08.11.2001

I. I. Axioutik, K. A. Bochkov, S. N. Kharlap. Methods of testing on safety of operation and ЭМС of microelectronic control systems by responsible technological processes

The paper deals with main methods of testing on safety of operation and electromagnetic compatibility of microelectronic control systems of responsible technological processes. The problems of construction of models of microelectronic systems and realisations of imitative safety tests are solved. The necessity of realisation of full-scale safety and electromagnetic compatibility tests is reasonable.