– сбои и отказы в работе приемопередающих устройств каналов связи, что приведет к нарушению передачи информации в системе ЖАТ;

– сбои и отказы в работе узлов самопроверки и аппаратуры защиты информации микропроцессорных многоканальных СЖАТ;

– повреждение и разрушение устройств хранения долговременной информации в центральных компьютерах и АРМ СЖАТ.

Отсюда следует, что воздействие СШИП может привести к нарушению как информационной, так и функциональной безопасности одновременно. Это обстоятельство делает указанное воздействие более опасным, чем кибератака или искажение алгоритмов работы СЖАТ.

Следует также учитывать, что СЖАТ являются распределенными системами. Их аппаратура территориально разнесена на большие расстояния: посты ЭЦ, ДЦ, путевые парки железнодорожных станций, переезды, перегоны и др. Поэтому защита таких систем путем оперативно-охранных мероприятий по периметру территории объекта затруднительна.

Сверхширокополосные импульсы, в отличие от традиционных источников помех, обладают распределением спектральной плотности в диапазоне от сотен МГц до единиц ГГц, что позволяет им легко проникать в АПК микроэлектронных устройств через паразитные емкостные каналы. Отличительной особенностью СШИП является также соизмеримость длительности воздействия импульсов с длительностью рабочих и тактовых импульсов АПК СЖАТ, что делает их значительно опаснее, чем уже изученное воздействие электромагнитного импульса высотного ядерного взрыва микросекундной длительности с шириной спектра от единиц кГц до сотен МГц.

Приведенный краткий анализ заставляет сделать вывод об обязательности обеспечения устойчивости микроэлектронных СЖАТ к СШИП в рамках решения проблемы киберзащищенности систем обеспечения безопасности движения поездов.

В докладе приводятся результаты проведенных в НИЛ БЭМС ТС БелГУТа исследований, позволяющих прогнозировать поведение ЛПК микропроцессорных СЖАТ при преднамеренном электромагнитном воздействии и определить направление работ по повышению их устойчивости к этим воздействиям.

Таким образом, в докладе показано, что для микроэлектронных АПК СЖАТ определяющим является выполнение требований по функциональной безопасности на уровне SIL4 по ГОСТ Р МЭК 61508–2012 и выполнение исследований, направленных на повышение устойчивости к преднамеренным электромагнитным воздействиям.

УДК 004.021

## АВТОМАТИЗАЦИЯ МЕТОДОВ ВЕРИФИКАЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ МИКРОПРОЦЕССОРНЫХ СИСТЕМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДВИЖЕНИЯ ПОЕЗДОВ

*К. А. БОЧКОВ, С. Н. ХАРЛАП, Б. В. СИВКО*
*Белорусский государственный университет транспорта, г. Гомель*

Системы железнодорожной автоматики и телемеханики (СЖАТ) необходимы для обеспечения безопасного управления транспортными процессами на железных дорогах, и главным в них является аспект безопасности. При этом СЖАТ регулируют процессы перевозок и предупреждают аварии и крушения. Соответственно, к ним предъявляются повышенные требования функциональной безопасности, что относится в том числе и к современным системам, построенным на микропроцессорной элементной базе.

Микропроцессорные СЖАТ представляют собой аппаратно-программные комплексы (АПК), использующие различные методы и средства передачи и обработки информации. Их неотъемлемой частью является программное обеспечение (ПО), для которого характерна высокая сложность. В связи с этим разработка и верификация микропроцессорных АПК, относящихся к системам обеспечения безопасности движения поездов (СОБД), сопровождается дополнительными мероприятиями, позволяющими получить необходимый уровень безопасности и отказоустойчивости. В то же время для подобных задач отсутствует единый подход решения, что формирует потребность в создании

эффективных методов и средств для повышения качества решения ключевых проблем разработки и верификации микропроцессорных СОБД.

К одному из вышеописанных способов относится автоматизация задач с помощью дополнительного специального ПО. Такой подход позволяет уменьшить влияние человеческого фактора во время проверки спецификаций и упростить разработку контролепригодного АПК. Средства автоматизации могут сократить затраты, например, выявляя ошибки проектирования до тестирования или имитационных испытаний. Для СОБД важным является то, что автоматизация дает возможность улучшить показатели отказоустойчивости и безопасности. Однако данный способ требует формализации, что затруднительно при разнообразии решаемых задач и элементной базы.

В докладе рассматривается три программных комплекса (ПК), разработанных для автоматизации ряда процессов разработки и верификации микропроцессорных СОБД. Данные ПК работают с программами PIC-контроллеров модели 16F877A и других, имеющих аналогичный набор команд исполнения.

Первый из них, *Formal Time Verifier,* основан на практике верификации микропроцессорных СЖАТ и предназначен для оценки временных параметров анализируемых систем: определение гарантированного времени перехода в безопасное состояние по тайм-ауту, вычисление частоты опроса внешних устройств и др. Такие задачи характерны для СОБД, так как они относятся к системам реального времени. ПК позволяет вычислять время выполнения между двумя произвольными точками, определять обстоятельства зацикливания программы, формировать доказательство обязательного завершения алгоритма, выполнять поиск точек программы, где выполнение обязательно произойдет при каждом выполнении тела цикла. Функционально *Formal Time Verifier* проводит синтаксический разбор исходного кода программы, далее создается граф переходов и в последующем ПК использует специально разработанные алгоритмы, представляющие собой решения задач на графах.

Во вторую группу задач входит оценка степени диверситета систем. Диверситет является одним из основных способов повышения отказоустойчивости и безопасности СОБД; он заключается в создании как можно более разных систем таким образом, чтобы в случае отказа они вели себя по-разному. Это позволяет обнаружить проблему и перейти в безопасное состояние. Важной задачей при построении таких систем является оценка достигнутой степени диверситета, которая позволяет сделать вывод о его эффективности. Для решения подобных задач разработан ПК *Diverse Axiomatic Basis Checker,* который использует диверсификацию аксиоматических базисов, когда проектируемая система опирается на заранее определенные формализованные утверждения. Соответственно, ПК проверяет данные утверждения на основе исходного кода программ, анализируя константные отказы и отказы короткого замыкания произвольных информационных линий, охватывая отказы ячеек памяти, дешифратора команд и выполнения инструкций микроконтроллера, отказы регистров и аккумулятора.

Третий ПК *Address Detection* автоматизирует метод обнаружения отказов на основе доступности адресных данных, выбирая набор адресов по запросу пользователя. В него входят такие параметры, как множество отказов для проверки или разрешенные адресные диапазоны, и на их основании ПК проводит поиск оптимальных адресов. Целями автоматизации данного ПК являются уменьшение ошибок во время поиска адресов, нахождение оптимального из возможных наборов и уменьшение затрат.

В докладе рассматриваются задачи автоматизации, разработанные алгоритмы и особенности применения предложенных программных средств. Представленные ПК опробованы в лаборатории «Безопасность и электромагнитная совместимость технических средств» БелГУТа и зарегистрированы в 2017 году в Национальном центре интеллектуальной собственности (г. Минск).

УДК 621.38

## КОМПЛЕКСНЫЙ ПОДХОД ПО ОБЕСПЕЧЕНИЮ ФУНКЦИОНАЛЬНОЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ЭТАПАХ ЖИЗНЕННОГО ЦИКЛА МПСУ ЖАТ

*А. Ю. ВАСИЛЬЕВ*
*ООО «ЛокоТех-Сигнал», Российская Федерация, г. Москва*

Широкое применение цифровых технологий в системах автоматизированного управления технологическими процессами обуславливает возникновение нового класса угроз – угроз информационной безопасности [1].