счет рассеяния в среде. Поэтому плоские волны являются наиболее опасными с точки зрения функционирования аппаратуры СЖАТ.

Из приведенного соотношения для плоской волны следует, что волна в точке наблюдения имеет ту же форму. что и волна, излученная антенной. Амплитуда волны в точке наблюдения мало изменяется по сравнению с излучаемой. Отверстие в корпусе-экране АПК СЖАТ вырезает из фронта волны импульс напряженности поля $E(t)$, форма которого совпадает с формой импульса излученной волны.

При воздействии на то же отверстие генератором-имитатором сверхширокополосных импульсных помех напряжение генератора также создает импульс напряженности поля в отверстии. Поэтому подобрав генератор соответствующих импульсов или воздействуя на отверстие эквивалентным импульсом, можно косвенно оценить последствия электромагнитного импульса преднамеренного воздействия. Наиболее близким по форме и ширине спектра является использование стандартного генератора электростатических разрядов, например, в соответствии с ГОСТ 30804.4.2

При использовании такого подхода не требуется проводить испытания в безэховых камерах с использованием дорогостоящих генераторов и излучателей СШИП с напряженностями электрического поля от единиц до сотен кВ/м.

Это позволит спрогнозировать поведение АПК СЖАТ при преднамеренном воздействии «электромагнитного терроризма» с предполагаемыми характеристиками используемого генератора в функции от расстояния прямой видимости на объект АПК СЖАТ.

Зная характеристики электрической составляющей поля в раскрытии отверстия, можно численным или аналитическим методом получить оценку поля, проникающего сквозь неоднородность внутрь корпуса ТС ЖАТ, и энергии помех, наведенной в паразитных антеннах узлов ТС. При этом оценка аналитическим методом является пессимистической, так как перекрывает все возможные резонансы в электродинамической системе ТС ЖАТ.

Для практической реализации описанной методики, ускорения расчетной работы в Научно-исследовательской лаборатории (НИЛ) «Безопасность и электромагнитная совместимость технических средств» (БЭМС ТС) НИИЖТа при БелГУТе разработана программа [1], которая осуществляет расчеты параметров помех внутри корпуса-экрана с неоднородностями. Предусмотрена возможность расчета параметров помехового излучения от круглого и прямоугольного отверстий, тонкой щели, болтового соединения, при воздействии на апертуру биэкспоненциального и гауссового импульсов напряжения. При этом в окне программы выбираются вид импульса, форма неоднородности экрана, задаются параметры импульса, неоднородности, координаты точки наблюдения внутри корпуса. Затем в результате работы программы пользователь получает значения составляющих вектора потока энергии в заданной им точке наблюдения.

Полученные в НИЛ «БЭМС ТС» НИИЖТа при БелГУТе научные результаты позволяют проводить оценку соответствия по требованиям к функциональной безопасности, а также прогнозировать поведение АПК СЖАТ при преднамеренном воздействии СШИП.

Список литературы

1 **Бочков, К. А.** Системный подход к прогнозированию воздействия сверхширокополосных импульсов помех на ключевые системы информационной инфраструктуры / К. А. Бочков, Д. В. Комнатный // Технологии ЭМС. – 2017. – № 4. – С. 3–10.

УДК 004.021

АВТОМАТИЗАЦИЯ ОЦЕНКИ ВРЕМЕННЫ́Х ПАРАМЕТРОВ МИКРОПРОЦЕССОРНЫХ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

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

Развитие современных систем железнодорожной автоматики и телемеханики сопровождается разработкой и внедрением микропроцессорных аппаратно-программных комплексов. Данные системы предоставляют широкий спектр функциональных возможностей и находят повсеместное

применение, в том числе и для систем, связанных с безопасностью (*safety-critical systems*, или ССБ), к которым относятся системы обеспечения безопасного движения поездов (СОБД).

Практика внедрения и эксплуатации микропроцессорных СОБД должна проводиться таким образом, чтобы выполнять предъявляемые требования безопасности. Обеспечение данных требований для микропроцессорных систем является сложной проблемой, и для её решения применяется комплекс методов и средств на всех этапах жизненного цикла системы. Так как СОБД относятся к системам реального времени, то для них необходимо выполнение определённых временны́х параметров: тайм-аута перехода в безопасное состояние, периода обновления устройств индикации, гарантированной частоты опроса внешних устройств и других.

Для повышения качества разработки и верификации обеспечение требований к временны́м параметрам выполняется несколькими способами, в том числе и на этапе верификации. К таким способам относят тестирование, экспертную проверку, формальные методы. Для ССБ необходимо применение нескольких из них, и при этом важно их качественное исполнение, а для его улучшения могут быть задействованы средства автоматизации, позволяющие уменьшить влияние человеческого фактора. Помимо этого, автоматизация может уменьшить затраты во время разработки и верификации, а также применяется на этапе проектирования.

Практика верификации программных средств микропроцессорных СОБД показывает, что к основным задачам при оценке временны́х параметров относятся определение времени выполнения между двумя произвольными точками, обстоятельств зацикливания программы и обязательного завершения алгоритма. Помимо этого, при рассмотрении циклических свойств системы актуален поиск мест, которых программа обязательно достигает на каждом выполнении цикла.

Для автоматического определения временных параметров в рамках описанных выше типичных задач верификации разработано программное обеспечение *Formal Time Verifier*. С его помощью возможно проведение верификации программ PIC-контроллеров модели 16F877A. При этом во время анализа используется общая база команд PIC-контроллеров, и поэтому *Formal Time Verifier* может применяться без изменений для PIC-микроконтроллеров других модификаций.

Функционально *Formal Time Verifier* проводит синтаксический разбор исходного кода программы, которая далее преобразуется в граф переходов, а последующие алгоритмические решения представляют собой решения задач на графах.

Первой решаемой задачей *Formal Time Verifier* является определение возможного зацикливания программ, которое может произойти, если граф программы циклический. В противном случае алгоритм вычисляет время выполнения программы между двумя точками. Для определения свойства цикличности (или ацикличности) используется алгоритм поиска в глубину, имеющий линейную сложность.

Второй задачей является расчёт времени выполнения между двумя точками программы, где *Formal Time Verifier* задействует эвристический поиск в ширину с объединением путей поиска в узлах графа согласно методу ослабления верификации без учёта логики программы. Здесь при рассмотрении разрыва цикла с фиксированным числом повторений проводится дополнительный анализ, аналогичный решению общей задачи при определении времени выполнения между двумя точками.

Третьей решаемой *Formal Time Verifier* задачей является определение таких контрольных точек программы, которые обязательно достигаются при её циклическом выполнении на каждой итерации цикла. Данное определение представляет собой решение задачи определения набора рёбер по разрезанию цикла. В общем случае задача является *NP*-сложной, но для рассматриваемого типа задач и используемого анализа разрыв цикла имеет смысл только одного ребра. С учётом этого частного случая *Formal Time Verifier* выполняет полный перебор по известным точкам цикла, что в худшем случае имеет квадратичную сложность. Практика показала, что для имеющихся задач верификации для программ со сложностью до 10 KLOC такое решение достаточно, так как вычисления происходят за время менее одной секунды.

Formal Time Verifier включает решения описанных трёх задач и во время их решения проверяет дополнительные условия, например, баланс стека. Практика применения показала, что данное программное обеспечение может использоваться для автоматизации верификации, в качестве дополнительного способа проверки, а также для других задач, например, определения достаточного времени имитационного моделирования.

Программное обеспечение *Formal Time Verifier* опробовано в лаборатории «БЭМС ТС» БелГУТа на микропроцессорных устройствах железнодорожной автоматики и телемеханики, таких как блок

телеуправления ТУ16-1 диспетчерской централизации «Нёман», блоки телеуправления ТУ-8Б и телесигнализации и телесигнализации ТС-16Б, применяемых в микропроцессорных централизациях «Ипуть» и «Днепр». В 2017 году *Formal Time Verifier* зарегистрировано в реестре компьютерных программ Национального центра интеллектуальной собственности, г. Минск.

УДК 621.38

ОЦЕНКА РИСКОВ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ МЕТОДИКИ ПЕРЕКРЕСТНОЙ ОЦЕНКИ ИХ УЯЗВИМОСТЕЙ И ПОТЕНЦИАЛЬНЫХ УГРОЗ

П. М. БУЙ
Белорусский государственный университет транспорта, г. Гомель

С. Г. КУЛЬГАВИК
Белорусская железная дорога, г. Барановичи

Риск для безопасности информационной системы – возможность нарушения ее функциональной и/или информационной безопасности в результате реализации угрозы с негативными последствиями, имеющими определенную цену в денежном эквиваленте (размер ожидаемого ущерба).

Оценка рисков занимает центральное место в системе управления информационной безопасностью, позволяет идентифицировать и оценить существующие активы, определить необходимость внедрения и эффективность уже внедренных средств защиты информации.

Активы информационной системы – это всё то, что необходимо для ее штатного функционирования и находится в ее распоряжении, например, аппаратные средства, программное обеспечение, хранимая и/или обрабатываемая информация и т. п. Ущерб, нанесенный организации, в собственности которой находится информационная система, в результате нарушения безопасности актива определяется аналитически в зависимости от его свойств [1].

При количественной оценке рисков безопасности информационной системы помимо ущерба необходимо учитывать вероятности появления угроз и их реализации через конкретные уязвимости отдельных активов или информационной системы в целом. При этом для адекватной оценки рисков важно охватить существенное количество угроз и соответствующих им уязвимостей. Такой подход дополнительно усложняется, если принять во внимание, что несколько угроз могут реализовываться через одну и ту же уязвимость и аналогично несколько уязвимостей могут быть причиной реализации одной и той же угрозы. В таких обстоятельствах целесообразно будет воспользоваться методикой перекрестной оценки угроз безопасности информационных систем и их уязвимостей [2]. Это позволит учесть очевидную взаимосвязь угроз и уязвимостей, являющуюся обязательным условием реализации любой угрозы, а также вопросы не только информационной, но и функциональной безопасности, которые зачастую остаются в «тени» при использовании существующих методов, ориентированных на оценку исключительно информационной безопасности.

Проведение методики перекрестной оценки угроз и уязвимостей предполагает определение совокупностей угроз и уязвимостей безопасности информационной системы. После этого необходимо определить, через какие уязвимости могут быть реализованы угрозы, т. е. связать уязвимости с угрозами, причинами реализации которых они могут стать.

Методика перекрестной оценки угроз безопасности информационных систем и их уязвимостей опирается на методику экспертных оценок. В связи с этим квалифицированные эксперты должны определить и выставить баллы следующим специальным критериям для каждой пары «угроза – уязвимость» дискретно в диапазоне от 1 до 10: C_1 – возможность возникновения источника угрозы в достаточном окружении от информационной системы для реализации угрозы через уязвимость; C_2 – степень готовности источника угрозы воспользоваться уязвимостью информационной системы и реализовать угрозу; C_3 – распространенность уязвимости по информационной системе или частота ее появления; C_4 – доступность уязвимости для реализации угрозы ее источником; C_5 –фатальность от реализации угрозы источником угрозы через уязвимость информационной системы.