Учет фактора CCF настоятельно рекомендуется стандартом IEC 61508, и в настоящее время основным способом защиты от CCF является аппаратный и программный диверситет. Для оценки диверситета могут быть использованы BETA-метод и модель BETAPLUS, рекомендованные стандартом IEC 61508. Однако имеющиеся решения проблемы CCF являются экспертными, что ограничивает их эффективность и глубину решения.

Метод на основе диверситетных аксиоматических базисов основан на аксиоматико-базисном подходе и позволяет сравнивать системы относительно их диверситета и тем самым предоставляет инструмент по целенаправленному усилению диверситета. Как результат, это дает возможность выполнять диверсификацию и её доказательство целенаправленно и формализованно.

Рассматриваемый метод позволяет выделить общий базис, нарушение утверждений которого приводит к CCF. Как следствие, можно определить факторы, ведущие к CCF, и обратить на них особое внимание. Вместе с тем, метод позволяет формализованно развести факторы, ведущие к CCF, на разные базисы, и тем самым решать проблему CCF.

В настоящее время эффективность метода подтверждена посредством имитационного моделирования с помощью КИИБ (комплекс имитационных испытаний на безопасность), который предназначен для проведения имитационных испытаний на функциональную безопасность в соответствии с IEC 61508, EN 50126, ОСТ 32.146 микропроцессорных систем управления ответственными технологическими процессами. Метод применялся при анализе типовой микропроцессорной железнодорожной системы счета осей подвижного состава. В дальнейшем разработанная система подвергалась испытаниям, во время которых вносились все возможные отказы, которые могли повлиять на её функционирование. В последующем свойства отказоустойчивости и безопасности определялись исходя из анализа результатов моделирования, которые подтвердили положения метода.

Практика разработки и имитационного моделирования показала, что отказы в независимых базисах не коррелированы, и на основании этого возможно улучшение показателей безопасности и отказоустойчивости. Также было экспериментально подтверждено, что диверситет, достигнутый с помощью метода на основе диверситетных аксиоматических базисов, позволяет обнаружить все одиночные отказы независимых базисов. Вместе с тем показано, что метод предоставляет формализованное описание для периодической проверки базисов, которая может быть выполнена средствами самотестирования.

Таким образом, в настоящее время эффективность метода на основе диверситетных аксиоматических базисов подтверждена экспериментально и отработана практика его применения. В докладе рассматриваются как основные положения метода, так и его особенности использования при разработке и верификации безопасных и отказоустойчивых систем.

УДК 621.38

КРИТЕРИИ ОТНЕСЕНИЯ МИКРОПРОЦЕССОРНЫХ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ К КРИТИЧЕСКИ ВАЖНЫМ ОБЪЕКТАМ ИНФОРМАТИЗАЦИИ

П. М. БУЙ, О. А. ЧЕКАНОВА
Белорусский государственный университет транспорта, г. Гомель

Понятие критически важного объекта информатизации (КВОИ) введено Указом Президента Республики Беларусь № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации» от 25 октября 2011 г. В соответствии с ним КВОИ – это объект информатизации, который:

1) обеспечивает функционирование экологически опасных и (или) социально значимых производств и (или) технологических процессов, нарушение штатного режима которых может привести к чрезвычайной ситуации техногенного характера;

2) осуществляет функции информационной системы, нарушение (прекращение) функционирования которой может привести к значительным негативным последствиям для национальной безопасности в политической, экономической, социальной, информационной, экологической, иных сферах;

3) обеспечивает предоставление значительного объема информационных услуг, частичное или полное прекращение оказания которых может привести к значительным негативным последствиям для национальной безопасности в политической, экономической, социальной, информационной, экологической, иных сферах.

В Концепции национальной безопасности Республики Беларусь относительно КВОИ, утвержденной Указом Президента Республики Беларусь № 575 от 9 ноября 2010 г., отмечено:

1) основными национальными интересами в информационной сфере являются: …обеспечение надежности и устойчивости функционирования критически важных объектов информатизации (Глава 2 – Национальные интересы);

2) основными потенциальными либо реально существующими угрозами национальной безопасности являются: …нарушение функционирования критически важных объектов информатизации (Глава 4 – Основные угрозы национальной безопасности);

3) в информационной сфере внутренними источниками угроз национальной безопасности являются: …несовершенство системы обеспечения безопасности критически важных объектов информатизации (Глава 5 – Внутренние источники угроз национальной безопасности).

Микропроцессорные системы железнодорожной автоматики и телемеханики (СЖАТ) – это объекты информатизации, которые основаны на использовании современных информационных технологий. Они находят все большее распространение при автоматизации процесса управления движением поездов на железнодорожном транспорте. При этом микропроцессорные СЖАТ относятся к системам управления нижнего уровня, непосредственно связанным с обеспечением безопасности движения поездов. Вместе с неоспоримыми преимуществами современных микропроцессорных СЖАТ появляются и новые угрозы, связанные с обеспечением информационной безопасности и рисками кибератак, которые могут привести к нарушению функционирования железнодорожного транспорта, гибели людей и значительным материальным потерям. Следует ли считать данные объекты информатизации критически важными?

Отнесение объекта информатизации к КВОИ осуществляется на основании методики, указанной в постановлении Совета Министров Республики Беларусь № 293 «О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации» от 30 марта 2012 г. с применением отраслевых критериев:

– экологической опасности производства, функционирование которого обеспечивается объектом информатизации;

– социальной значимости производства, функционирование которого обеспечивается объектом информатизации;

– важности объекта информатизации, осуществляющего функции информационной системы;

– важности объекта информатизации, обеспечивающего предоставление значительного объема информационных услуг.

Так как микропроцессорные СЖАТ являются системами нижнего уровня при обеспечении безопасности движения поездов, то говорить об их важности с точки зрения информационной системы или при предоставлении информационных услуг не приходится. Однако первые два из перечисленных критериев нельзя оставить без внимания при анализе возможных последствий при нарушении функционирования системы железнодорожной автоматики и телемеханики.

В качестве грузов, перевозимых железнодорожным транспортом, могут быть как взрывоопасные смеси и жидкости, так и ядовитые вещества, которые при крушении поезда могут привести к существенным негативным экологическим последствиям, чему, к сожалению, время от времени мы становимся свидетелями.

Транспорт в целом имеет большую социальную значимость, а железнодорожный транспорт играет ведущую роль в грузо- и пассажироперевозках в нашей стране. Существенные задержки в исполнении графика движения поездов могут привести к падению престижа Белорусской железной дороги и неудовлетворенности граждан в качестве предоставляемых ею услуг.

Опираясь на указанное выше и рассматривая примерный перечень показателей уровня ущерба национальным интересам Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах в случае возникновения угроз различного характера в отношении объекта информатизации (его составляющих элементов), отмеченных в постановлении Совмина, достаточно сложно предсказать возможное количество жертв или величину материально-

го ущерба, нанесенного отрасли и государству в целом, при крушении вследствие нарушения функциональной и (или) информационной безопасности микропроцессорной СЖАТ в результате успешной реализации кибератаки. В связи с этим нужно однозначно поднимать вопрос о необходимости отнесения таких систем к критически важным объектам информатизации.

УДК 681.3

ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ ПРОЦЕССА ПРОЕКТИРОВАНИЯ ЖЕЛЕЗНОДОРОЖНЫХ СТАНЦИЙ

И. О. ЖИГАЛИН

Белорусский государственный университет транспорта, г. Гомель

Одним из важнейших этапов жизненного цикла железнодорожной станции является проектирование, при котором предъявляются требования на принятие тех или иных концептуальных решений. Ошибка в требованиях, допущенная на этой стадии, приведет к большим потерям на последующих этапах жизненного цикла.

Существующие методы проектирования можно классифицировать по степени автоматизации и методологиям процесса разработки. На текущий момент в основном применяются методы автоматизированного проектирования, т.к. при неавтоматизированном методе резко возрастают затраты на проектирование. Автоматизация процесса проектирования может охватывать различные этапы жизненного цикла процесса, при этом работы этапов могут быть изолированы друг от друга.

Наиболее распространенными подходами при проектировании являются:

– структурное проектирование;

– информационное моделирование предметной области;

– объектно-ориентированное проектирование.

При использовании методов структурного проектирования осуществляется анализ, структурирование и создание моделей данных, для которых устанавливается необходимый состав процедур обработки и функций.

Для информационного моделирования моделируются функции предметной области, уточняется состав входной и выходной информации. Алгоритм обработки данных можно представить как совокупность процедур преобразований структур данных в соответствии с внешними моделями данных.

Объектно-ориентированное проектирование соединяет процесс объектной декомпозиции с использованием моделей данных проекта в статике и динамике.

Для проектирования железнодорожных станций наиболее удобным является использование методов структурного проектирования и информационного моделирования, т.к. современные условия проектирования предполагают процесс проектирования в режиме непрерывной информационной поддержки, обеспечивающей единообразные способы управления процессами и взаимодействия всех участников цикла (методология CALS). Внедрение CALS предполагает реорганизацию процесса проектирования. Необходимым является создание функциональной модели, отражающей этапы проектирования и функции отделов, а также потоки информации, что является одним из шагов внедрения единого информационного пространства проектирования железнодорожных станций.

В общем виде процесс проектирования в САПР можно упрощенно представить схемой, показанной на рисунке 1. Важнейшую роль в этих системах играет проектировщик. Человек в САПР решает все неформализованные проектные задачи и задачи планирования работ. Современная САПР является инструментом проектировщика, поэтому тесное взаимодействие человека и ЭВМ в процессе проектирования – один из важнейших принципов построения и эксплуатации САПР.

Результаты проектирования должны быть представлены в виде, удобном для восприятия человеком, и содержать информацию, на основании которой разработчик мог бы вынести суждение о результатах проектирования. Даже при автоматическом получении вариантов проектных решений за проектировщиком остаются важнейшие функции: ввод исходных данных для проектирования, окончательная оценка и утверждение проектных решений. В интерактивном режиме проектирования оператор непосредственно участвует в решении задач, воздействуя на выбор факторов решения и уточняя независимые переменные.