быть автоматизирована, что не только уменьшает затраты во время разработки и верификации, но и снижает влияние человеческого фактора.

Одним из способов обнаружения отказов микропроцессорных систем является метод обнаружения отказов на основе доступности адресных данных, при применении которого происходит выбор определённого набора адресов, зависящего от того множества отказов, наличие которых требуется проверить. Ключевая идея метода состоит в том, что в случае отказа один из адресов становится недоступным, и на этом основании система может перейти в безопасное состояние или запустить процедуры самовосстановления. Данный метод предоставляет способы для быстрого определения требуемого набора адресов, которые применяются вручную.

Задачу автоматического поиска адресов можно решить с помощью программных средств. На практике требуется на основании множества проверяемых отказов и разрешенных адресных диапазонов вычислить возможные наборы адресов и определить оптимальные согласно заданным критериям. Целью данной автоматизации является уменьшение ошибок во время поиска адресов, нахождение оптимального из возможных наборов и уменьшение затрат. Разработанный алгоритм может применяться на стадии компиляции, когда становятся известными доступные свободные адресные диапазоны и автоматически на их основании определяются адреса по рассматриваемому методу.

Множество проверяемых отказов для СКБ, как правило, регламентируется стандартом IEC 61508, где описаны наиболее часто проявляющиеся на практике отказы константного нуля или единицы (*stack-at faults*, *SA*) и отказы короткого замыкания (*bridge faults*, *B*). Рассмотрение данных моделей в контексте автоматизации показало, что решение для *SA*-отказов не является сложным, так как каждая из проверок маскирует по биту один или два адреса. Для *B*-отказов проверка короткого замыкания потребуется между любыми двумя битами, и для решения необходим перебор $n!$ вариантов (где n – размер рассматриваемого регистра). Если существует решение для одного адреса, то данная задача становится эквивалентной задаче о раскраске графа двумя цветами, которая если имеет решение, то оно находится за линейное время. Если решения нет, то задача становится *NP*-сложной.

На практике метод обнаружения отказов на основе доступности адресных данных в основном применяется для небольшого числа *B*-отказов и соответственно решением является малое число адресов. В данной ситуации было принято решение, что программное обеспечение должно хорошо решать задачу для одновременно рассматриваемых обоих типов отказов и предоставлять удобные параметры поиска и критерии выбора. При рассмотрении большого числа *B*-отказов могут быть эффективно применены вероятностные алгоритмы, решающие задачу поиска максимального разреза графа.

Разработанное программное обеспечение *Address Detection* позволяет определять возможные решения для 1 и 2 адресов, при этом задается произвольное множество *SA*- и *B*-отказов, имеется возможность указания запрещённых диапазонов (где располагается программа, данные и др.). При обнаружении решения из 1 адреса программа предоставляет максимальный и минимальный адреса из возможных, а для 2 адресов в решении выбираются пары по двум критериям: минимальное расстояние между адресами и выбор таких пар, где минимальный адрес максимален (в этом случае весь диапазон до минимального остается свободным для использования). Имеется возможность определения всех решений при указанных условиях.

Критерии и настраиваемые параметры выбраны и реализованы исходя из практического опыта применения для СКБ.

Программное обеспечение *Address Detection* опробовано в лаборатории «БЭМС ТС» БелГУТа и зарегистрировано в 2017 году в Национальном центре интеллектуальной собственности, г. Минск.

УДК 656.2.08

ОЦЕНКА БЕЗОПАСНОСТИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ БЕЛОРУССКОЙ ЖЕЛЕЗНОЙ ДОРОГИ

П. М. БУЙ, С. Г. КУЛЬГАВИК
Белорусский государственный университет транспорта, г. Гомель

На Белорусской железной дороге активно внедряются и используются автоматизированные системы управления технологическими процессами (АСУ ТП), содержащие в своем составе или ис-

пользующие такие элементы информационных технологий, как компьютеры и телекоммуникационные системы. Проанализировав тенденции эволюции угроз, направленных на нарушение как информационной, так и функциональной безопасности объектов информатизации [1], становится очевидной необходимость системного подхода при организации защиты таких АСУ ТП.

В последние годы в статистике нарушений информационной безопасности зафиксирован резкий сдвиг от внешних к внутренним угрозам безопасности объектов информатизации: примерно две трети от общего числа всех наиболее серьезных инцидентов, связанных с безопасностью, составляют нарушения или ошибки законных пользователей объектов информатизации [2]. В таких условиях функционирования объектов информатизации Белорусской железной дороги необходимо адекватно подходить к разработке моделей нарушителей безопасности таких объектов, а также максимально объективно оценивать опасность потенциальных угроз, реализуемых против безопасности объекта, и возможных его уязвимостей.

В качестве потенциального внутреннего нарушителя объекта информатизации Белорусской железной дороги был выбран законный пользователь одного из компьютеров, подключенных к сети. Сокращенная неформальная модель такого нарушителя имеет следующий вид:

– нарушитель имеет точку доступа к сети и собственное помещение или закрытое пространство общего помещения, позволяющее ему скрытно подключать собственное сетевое оборудование;

– нарушитель обладает достаточно неплохими знаниями в сфере IT, включающими, в частности, знания о работе протоколов IP, TCP, UDP, SNMP, TFTP, стандарта IEEE 802.1Q для VLAN, навыками конфигурирования сетевого оборудования;

– нарушитель своей целью ставит доступ к трафику других пользователей сети;

– причинами, побуждающими внутреннего нарушителя к неправомерным действиям, могут быть демонстрация своего превосходства (самоутверждение), «борьба с системой», корыстные интересы;

– характер действий нарушителя – скрытый;

– финансовые возможности нарушителя достаточны для приобретения в собственность необходимого сетевого оборудования.

Такой нарушитель способен после непродолжительной подготовительной работы анализировать сетевой трафик любых двух пользователей локальной сети, к которой он относится, что было экспериментально проверено в среде моделирования Cisco Packet Tracer.

Максимально объективно разработанная модель нарушителя является гарантией построения адекватной системы обеспечения информационной безопасности [3].

Для совокупной оценки угроз и уязвимостей целесообразно использовать метод экспертных оценок, при котором экспертам предлагается оценить возможность реализации некоторого перечня угроз. Совокупная оценка позволяет не просто определить оторванные друг от друга перечни угроз и уязвимостей, но и проследить их возможное взаимодействие в процессе реализации данных угроз через уязвимости объекта информатизации. При этом необходимо использовать следующие критерии:

1) возможность возникновения источника угрозы в достаточном окружении от объекта информатизации для реализации угрозы через уязвимость;

2) степень готовности источника угрозы воспользоваться уязвимостью объекта информатизации и реализовать угрозу;

3) распространенность уязвимости по объекту информатизации или частота ее появления;

4) доступность уязвимости для реализации угрозы ее источником;

5) фатальность от реализации угрозы источником угрозы через уязвимость объекта информатизации.

Для оценки угроз и уязвимостей объекта информатизации необходимо:

– определить совокупности угроз и уязвимостей безопасности объекта информатизации;

– увязать между собой угрозы и уязвимости, установив потенциальную реализацию первых через вторые;

– перевести в резерв несвязанные уязвимости и угрозы;

– вычислить коэффициент опасности реализации каждой угрозы через каждую увязанную с ней уязвимость;

– для каждой из угроз и уязвимостей определить коэффициенты их опасностей;

– произвести ранжирование угроз и уязвимостей, определив тем самым наиболее опасные из них.

Список литературы

1 Kaspersky security bulletin 2016 [Электронный ресурс] – Режим доступа: https://securelist.ru/files/2016/12/Kaspersky-Security-Bulletin-2016_RUS.pdf – Дата доступа: 11.09.2017.

2. **Олифер, В.** Компьютерные сети. Принципы, технологии, протоколы : учеб. – 5-е изд. / В. Олифер, Н. Олифер. – СПб. : Питер, 2016. – 992 с.

3. **Бочков, К. А.** Модель внутреннего нарушителя информационной безопасности сети дистанции сигнализации и связи / К. А. Бочков, П. М. Буй, М. В. Лукашеня // Проблемы и перспективы развития транспортных систем и строительного комплекса : материалы III Междунар. науч.-практ. конф. / под общ. ред. В. И. Сенько. – Гомель : БелГУТ, 2013. – С. 109–110.

УДК 621.311

ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ ЛИНИЙ ДПР С ПОТРЕБИТЕЛЯМИ ЭЛЕКТРОЭНЕРГИИ НА ДОРОГАХ ПЕРЕМЕННОГО ТОКА

Д. Р. ЗЕМСКИЙ
Днепропетровский национальный университет железнодорожного транспорта им. акад. В. Лазаряна, Украина

На железнодорожном транспорте, как и в промышленности, немалую роль играет оборудование, чувствительное к качеству электроэнергии, от которого зависит не только производственный процесс, но и безопасность роботы персонала. Устройства СЦБ относятся к потребителям электроэнергии первой категории, что вызвано исключительной важностью системы автоматики и управления в вопросе обеспечения безопасности движения поездов. Следовательно, к надежности электроснабжения таких потребителей предъявляют высокие требования. Тем не менее, резервное питание устройств СЦБ осуществляется линиями ДПР («два провода – рельс»), которые уступают линиям продольного электроснабжения в области электромагнитной совместимости.

Отличительной особенностью линий ДПР являются использование рельсов железнодорожного пути в качестве третьей фазы линии. Вследствие этого передача электроэнергии сопровождается дополнительным ухудшением ее качества, что проявляется в виде искажения синусоиды, несимметрии, колебаний и отклонения питающего напряжения в точке присоединения потребителей.

Провода линии ДПР, как и у линии продольного электроснабжения, размещены на опорах контактной сети и подвергаются сильному воздействию её электромагнитного поля. Наведенное в проводах напряжение, в случае электрификации железной дороги на переменном токе, имеет в своем составе гармонические составляющие, кратные 50 Гц. Наличие лежащей на земле фазы приводит к тому, что потенциал рельса, относительно земли, в отличие от потенциала двух размещенных на опоре проводов, остается практически неизменным вдоль всей длины сближения контактной сети и линии ДПР. В результате возникает смещение треугольника линейных напряжений у потребителя по отношению к треугольнику напряжений на шинах подстанции, что проявляется в виде несимметрии питающего напряжения. При большой несимметрии происходит значительное снижение мощности асинхронных двигателей, в частности стрелочных электроприводов.

Качество электроэнергии на шинах тяговой подстанции может ухудшаться из-за неравномерной загрузки фаз трансформатора, гармонического состава тягового тока, воздействия системы внешнего электроснабжения, интенсивности и режима роботы электроподвижного состава. Кроме того, ток нагрузки нетягових потребителей неравномерно распределяется по рельсам железнодорожного пути, что создает дополнительное мешающие воздействие на сигналы автоблокировки. Сильные помехи могут стать причиной отказов работы устройств СЦБ, оказавшихся под их воздействием.

К вышесказанному стоит добавить, что вследствие особенности подключения вводов тяговых подстанций переменного тока к системе внешнего электроснабжения, в большинстве случаев невозможно обеспечить двустороннее питание линий электроснабжения нетяговых потребителей. В результате этого эксплуатация линии ДПР, с позиции надёжности питания и потерь мощности в системе, имеет существенные недостатки по сравнению с аналогичной системой на дорогах постоянного тока.

В целом, неудовлетворительное качество питающего напряжения приводит к ухудшению условий работы нетяговых потребителей, подключенных к линии ДПР, вызывает дополнительные потери мощности, уменьшает срок эксплуатации оборудования.