Этап 1. Определение требуемых значений ослабления ЭМИ формируемых конструкций экранов.

Этап 2. Выбор типа порошкообразного материала (шунгит, перлит), используемого в качестве наполнителя для формируемой конструкции экрана, либо изготовление смеси на основе указанных порошкообразных материалов путем их смешивания в определенных объемных долях. Такой выбор зависит от требований, предъявляемых к значениям ослабления и коэффициента отражения ЭМИ формируемых конструкций экранов. Увеличение на 10 об. % содержания порошкообразного шунгита в смеси приводит к увеличению в среднем на 5 дБ значений ослабления ЭМИ в диапазоне частот 8–12 ГГц формируемых конструкций экранов ЭМИ. Значения коэффициента передачи при этом увеличиваются в среднем на 4 дБ.

Этап 3. Определение соотношения массы (объема) порошкообразного наполнителя и связующего вещества. Значение соотношения зависит от типа порошкообразного материала, использованного для изготовления наполнителя, а также требований, предъявляемых к значениям ослабления ЭМИ формируемой конструкции экрана.

Этап 4. Смешивание наполнителя и связующего вещества в смешивающем механизме.

Этап 5. Раскрой металлической или целлюлозной армирующей подложки, предназначенной для нанесения полученного в результате реализации этапа 4 композиционного материала, на фрагменты размером 50×50 см. Выбор типа подложки зависит от требований, предъявляемых к значениям ослабления ЭМИ формируемых конструкций экранов. В случае использования металлической армирующей подложки для нанесения композиционного материала значения ослабления ЭМИ в диапазоне частот 8–12 ГГц формируемых конструкций экранов будут составлять более 40 дБ, а в случае использования целлюлозной подложки – от 10 до 30 дБ.

Этап 6. Очищение и обеззараживание армирующей подложки.

Этап 7. Нанесение полученного в результате реализации этапа 4 композиционного материала на армирующую подложку слоем толщиной 1,5–2 мм.

Этапа 8. Выдерживание в течение 24 ч нанесенного на армирующую подложку композиционного материала в условиях комнатной температуры до полного его высыхания.

Этап 9. Проверка качества полученного базового модуля экрана ЭМИ (адгезия порошкообразного материала со связующим веществом и армирующим полотном, соответствие значений ослабления ЭМИ сформированного базового модуля требованиям, предъявляемым к этому параметру).

Этап 10. Повторное нанесение на базовые модули полученного в результате реализации этапа 4 композиционного материала (при необходимости).

Этап 11. Соединение внахлест полученных базовых модулей с помощью эпоксидного клея марки ЭДП (ТУ 2385-024-75678843–2010). Количество используемых при этом базовых модулей определяется требованиями, предъявляемыми к габаритным размерам формируемых конструкций экранов.

В зависимости типа порошкообразного наполнителя, а также соотношения наполнителя и связующего вещества удельный вес базового модуля для формирования конструкций экранов ЭМИ, получаемого согласно предложенной методике, составляет 0,1–0,6 кг.

Работа выполнена при поддержке Белорусского республиканского фонда фундаментальных исследований (грант Т15М-025).

УДК 621.38

ОСОБЕННОСТИ МИКРОПРОЦЕССОРНЫХ СИСТЕМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДВИЖЕНИЯ ПОЕЗДОВ КАК КРИТИЧЕСКИХ СИСТЕМ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

К. А. БОЧКОВ, П. М. БУЙ

Белорусский государственный университет транспорта, г. Гомель

Е. Н. РОЗЕНБЕРГ

Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте, г. Москва

Микропроцессорные системы железнодорожной автоматики и телемеханики (СЖАТ), основанные на использовании современных информационных технологий находят все большее распро-

странение в 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.

В соответствии с нормативными документами Федеральной службы по техническому и экспортному контролю России микропроцессорные СЖАТ относятся к критическим системам информационной инфраструктуры (КСИИ). Вопросы информационной безопасности таких систем регламентируются различными техническими нормативно-правовыми актами (ТНПА), в том числе и требованиями аттестации по защите информации, циркулирующей в их аппаратно-программных комплексах. При этом основное внимание в этих ТНПА уделяется угрозам нарушения конфиденциальности, целостности и доступности информации.

К основным нормативным документам для анализа защищённости информационных технологий (ИТ) относятся стандарты ГОСТ Р ИСО-МЭК 15408 (3 части) и ГОСТ Р ИСО-МЭК 18045 2012 и 2013 годов. Эти стандарты ограничены рамками программно-технического уровня информационной безопасности, что вполне достаточно для оценки продуктов информационных технологий. Однако их недостаточно для микропроцессорных СЖАТ.

Отдельные аспекты особенностей КСИИ учтены в стандарте США NIST 800-82 (2011) и стандарте EEC 62279 (2012) Railway applications. Communications, signaling and processing systems. Software for rail way control and protection systems (Железные дороги. Системы связи, сигнализации и обработки данных. Программное обеспечение систем управления и защиты на железных дорогах).

Микропроцессорные СЖАТ относятся к нижнему уровню информационной инфраструктуры управления железнодорожным транспортом. К таким системам, в первую очередь, предъявляются повышенные требования к обеспечению безопасности движения поездов, то есть определяющие их функциональную безопасность, при отказах и внешних воздействиях, в том числе и кибератаках.

В сфере безопасности КСИИ имеются две наиболее серьезные проблемы. Это недостатки моделей безопасности, разработанных для обычных промышленных систем, и недостатки сред, в которых используются эти модели.

До последнего времени при создании моделей информационной безопасности критически важных промышленных объектов бытовало мнение, что одной лишь физической изоляции объекта достаточно для его защиты. Как правило, модель безопасности таких объектов основана на принципах «Security by obscurity» (безопасность через сокрытие) и «Air gap» (физическая изоляция). Компьютерный «червь» Stuxnet развеял этот миф, продемонстрировав способность вторгаться в изолированные сети систем управления как через подключаемые к ним компьютеры, так и посредством беспроводных технологий. Многие современные сетевые угрозы являются еще более изощренными и могут исходить, в том числе, из косвенных источников, заставляя разработчиков встраиваемых КСИИ учитывать все большее количество требований к безопасности в своих продуктах.

Для микропроцессорных СЖАТ наивысшим приоритетом является обеспечение их длительной непрерывной безопасной работы по организации движения поездов на основе графиков и маршрутов передвижения. Обработка и циркулирование же коммерческой информации о характере груза, его владельце, пунктах назначения, стоимости и др. осуществляется в других автоматизированных системах по организации перевозочного процесса, и для этих систем более приоритетным является обеспечение информационной безопасности.

Современные микропроцессорные СЖАТ не могут быть физически полностью изолированы от систем управления перевозочным процессом. С одной стороны, микропроцессорные СЖАТ нижнего уровня получают информацию от систем верхнего уровня управления перевозочным процессом в виде графиков движения, сортировочных листков и т. п. С другой стороны, текущее состояние элементов нижнего уровня является важным источником информации по организации перевозочного процесса верхнего уровня.

Микропроцессорные СЖАТ имеют следующие дополнительные особенности с позиций обеспечения кибербезопасности по отношению к массовым промышленным АСУ ТП:

– главной целью кибератаки на микропроцессорные СЖАТ является не информация сама по себе, а возможность воздействия на исполнительные объекты;

– возможная атака будет направлена на вывод из строя микропроцессорной СЖАТ (в том числе и методами электромагнитного терроризма) или нарушения функциональной безопасности, а следовательно, и нарушения безопасности движения поездов;

– атака может быть направлена на конкретные (наиболее опасные по последствиям) объекты СЖАТ с помощью специально разработанных средств, поэтому традиционные (шаблонные) средства защиты могут быть неэффективными;

– микропроцессорные СЖАТ, объединенные в АСУ процессом перевозок, территориально разобщены и работают в реальном масштабе времени, и применение средств защиты, основанных, например, на методах криптографии, шифрования потребует дополнительных вычислительных ресурсов и, естественно, к увеличению времени на реализацию команд и получении информации о состоянии объектов, что может явиться ограничивающим фактором в обеспечении функциональности систем.

Эти отличия затрудняют применение в микропроцессорных СЖАТ традиционных подходов в обеспечении информационной безопасности бизнес-систем и обычных промышленных АСУ ТП.

Современный подход в обеспечении непрерывности и безопасности перевозочного процесса основан на концепции построения микропроцессорных СЖАТ по принципу многоуровневых систем обеспечения функциональной безопасности. При этом наиболее совершенная стратегия обеспечения кибербезопасности методами эшелонированной защиты хорошо ложится на эту концепцию.

В процессе жизненного цикла микропроцессорной СЖАТ всех субъектов, которые каким-либо образом с ней связаны, можно разделить на четыре категории:

– разработчики;

– владельцы или заказчики;

– внешние аккредитованные эксперты в области информационной безопасности, которые производят аттестацию системы защиты информации;

– злоумышленники, которые нарушают информационную безопасность и функционирование СЖАТ.

Если микропроцессорная система управления была введена в эксплуатацию до вступления в силу ТНПА по оценке информационной безопасности, то процесс разработки для нее системы защиты информации ложится на плечи владельца. Если система вводится в эксплуатацию позже, то в ее состав еще на стадии разработки должна быть включена система защиты информации, которую затем владелец обязан аттестовать.

При таком взаимодействии субъектов у владельца СЖАТ, заинтересованного в ее безопасном функционировании, вполне обоснованно могут возникнуть следующие вопросы:

1 Насколько компетентен разработчик в системах защиты информации? По данным компании «Hewlett Packard» на сегодняшний день можно выделить более 500 классов различных уязвимостей в программном обеспечении (ПО). Около 95 % всех дефектов программ, относящихся к безопасности, проистекают из 19 типичных ошибок, природа которых вполне понятна.

2 Кто является злоумышленником, какие он преследует цели и какими ресурсами обладает (модель нарушителя безопасности системы управления)? Например, компьютерный «червь» Stuxnet, обнаруженный в 2010 году белорусской антивирусной компанией «ВирусБлокАда». Имеются предположения, что он разработан в США и Израиле для кибератаки на иранский ядерный проект, которая продолжалась около девяти месяцев. Причем ни одна из атакованных систем не имела прямого соединения с Интернет. Это была первая известная и успешная кибератака на автоматизированные системы управления технологическими процессами (АСУ ТП). Известен также вирус «Flame», обнаруженный в мае 2012 года российской антивирусной компанией «Лаборатория Касперского». Этот вирус действовал, по крайней мере, с марта 2010 года. Предполагается, что его также разработали в США и Израиле для замедления иранской ядерной программы. Распространялся вирус через LAN и USB, записывал экраны, нажатия клавиатуры, сетевой трафик, включая Skype.

3 Не является ли разработчик злоумышленником преднамеренным (например, аппаратные или программные закладки) или случайным (например, ошибки в коде программного обеспечения)? По данным Software Engineering Institute опытный программист «пропускает» приблизительно один дефект на 100 строк кода. Если в течение жизненного цикла ПО 99 % этих дефектов будут обнару-

жены и исправлены, то в пакете программ, состоящем из одного миллиона строк исходного кода, останется тысяча дефектов. К примеру, дистрибутив Red Hat Linux 7.1 состоит приблизительно из 30 миллионов строк кода, а Microsoft Windows XP содержит около 40 миллионов строк кода. Следовательно, число невыявленных дефектов в Red Hat Linux и Windows XP можно оценить, соответственно, в 30 и 40 тысяч. При этом выявленные дефекты устраняются чаще всего путем установки программных «заплаток».

4 Насколько внешние аккредитованные эксперты в области информационной безопасности компетентны в принципах функционирования микропроцессорных СЖАТ?

5 Какие уязвимости случайно или преднамеренно заложены в аппаратную или программную часть ядра, поверх которой устанавливается микропроцессорная СЖАТ?

Ответы на эти вопросы очень важны!

Кроме того, особенностью систем управления нижнего уровня на железнодорожном транспорте является то, что в них практически отсутствует конфиденциальная информация. Поэтому обеспечение конфиденциальности информации приобретает второстепенное значение, а наиболее важными становятся целостность и доступность информации. Целостность предполагает надежное и безопасное управление за счет сохранения контроля над структурой управляющих воздействий, а доступность – над их авторизацией и временем появления. Все эти вопросы касаются безопасности функционирования с СЖАТ, которые должны отвечать требованиям, предъявляемым с точки зрения функциональной безопасности. Функциональная безопасность – это совокупность таких условий функционирования системы управления, при которых предотвращаются или минимизируются последствия от внешних или внутренних деструктивных информационных воздействий, приводящих к нарушению процесса штатного функционирования системы.

Таким образом, с точки зрения законодательства для микропроцессорных СЖАТ приоритетными являются вопросы информационной безопасности, а с точки зрения обеспечения безопасности движения поездов – функциональной. В итоге необходимо комплексно оценивать безопасность системам управления нижнего уровня.

Концепцией обеспечения кибербезопасности ОАО «РЖД» вводится понятие кибербезопасности микропроцессорных систем управления. Кибербезопасность – это совокупность политики и действий, которые должны быть предприняты для защиты критически важных объектов от деструктивных информационных воздействий (например, несанкционированный доступ, компьютерная атака, программно-аппаратные закладки, недекларированные возможности, искажение, кража, уничтожение информации), направленных на нарушение штатного функционирования этих систем. Следовательно, понятие кибербезопасности объединяет понятия информационной и функциональной безопасности.

В.В. Путин на заседании коллегии ФСБ России в апреле 2014 года сказал: «В 2013 году было обнаружено и пресечено более 9 миллионов воздействий на интернет-сайты информсистемы органов госвласти России. Нужно быть готовыми к тому, что такие попытки вторгнуться в наше информационное поле будут продолжаться…».

Причём поражению критически важных объектов подвержены прежде всего АСУ ТП на базе так называемых SCADA-систем. SCADA (supervisory control and data acquisition – диспетчерское управление и сбор данных) – программный пакет, предназначенный для разработки или обеспечения работы в реальном времени систем сбора, обработки, отображения и архивирования информации об объекте мониторинга или управления.

Максимально безопасной эксплуатации системы управления на железнодорожном транспорте можно достичь, если владелец (заказчик) выполнит ряд условий взаимодействия с причастными субъектами:

1 Владелец будет поддерживать постоянный тесный и взаимовыгодный контакт с разработчиком, который организует надежное сопровождение системы управления.

2 Владелец будет иметь в штате одного или нескольких сотрудников, аккредитованных в области защиты информации и имеющих достаточную квалификацию по СЖАТ.

3 Владелец будет не только осуществлять защиту информации, обеспечивающую выполнение требований, предъявляемых законодательством и условиями функционирования к СЖАТ, но и при помощи квалифицированных сотрудников («своих» злоумышленников) осуществлять попытки нарушения кибербезопасности системы управления с целью обнаружения ее уязвимостей.

Аналогом КСИИ в Республике Беларусь является критически важные объекты информатизации (КВОИ). По имеющимся данным Белорусская железная дорога, являясь владельцем микропроцессорных системы управления на железнодорожном транспорте, не отнесла данные объекты информатизации к КВОИ.

УДК 656.254

ПРОБЛЕМЫ ВЫБОРА И ТЕХНИКО-ЭКОНОМИЧЕСКОГО ОБОСНОВАНИЯ ВНЕДРЕНИЯ СОВРЕМЕННЫХ МПЦ

К. А. БОЧКОВ, А. Н. КОВРИГА
Белорусский государственный университет транспорта, г. Гомель

Система электрической централизации стрелок и сигналов (ЭЦ) относится к «долгоживущим» объектам техники, так как эксплуатируется в течение 25 лет и более. Потребность в новой системе возникает при постепенном накоплении объективных и субъективных обстоятельств, связанных с совершенствованием методов и способов управления технологическим процессом управлением движения поездов и маневровой работы на станциях. С одной стороны, это недостаточность функции, реализуемых существующими системами, и изменение параметров перевозочных процессов, к которым эти системы трудно адаптируются, а с другой стороны – развитие техники, позволяющее при небольших затратах совершенствовать и развивать функциональные возможности систем. Кроме того, важным является фактор морального и физического старения устройств в системах и несоответствие их современному уровню развития науки и техники.

Совершенствование релейных систем ЭЦ, связанное с унификацией, расширением функциональных возможностей, повышением надежности и безопасности, модернизацией питающих установок и др., привело к увеличению расхода реле на одну централизованную стрелку с 24 до 150–180 в новых системах ЭЦ-И, ЭЦ-К. В свою очередь, это вызвало увеличение необходимых площадей постов ЭЦ и дополнительный расход электроэнергии. Все это, наряду с моральным и физическим старением, свидетельствует об исчерпании возможностей дальнейшего совершенствования релейных систем.

Общепризнанной альтернативой релейным системам ЭЦ являются микропроцессорные системы централизации стрелок и сигналов (МПЦ). В настоящее время разработчики и производители МПЦ предлагают для внедрения целый ряд таких систем. При этом возникает необходимость выбора и технико-экономического обоснования внедрения тех или иных систем МПЦ как отечественного, так и зарубежного производства.

Проведение технико-экономического обоснования внедрения МПЦ на основе подходов, используемых для релейных ЭЦ, невозможно, поскольку, во-первых, МПЦ и релейные системы существенно отличаются по принципу построения и сравниваемой базой при внедрении, во-вторых, для технико-экономического обоснования оборудования станций системами релейных ЭЦ было достаточно таких показателей как пропускная способность станций и производительность труда станционных работников. В технико-экономических расчетах при внедрении МПЦ взамен релейных ЭЦ эти показатели использоваться не могут.

В докладе показано, что в этих случаях требуется принимать во внимание такие преимущества МПЦ, как:

– повышение надежности и безопасности за счет увеличения глубины резервирования;

– расширение функциональных возможностей по организации движения поездов за счет использования программно-аппаратных средств МПЦ;

– приспособленность к удобному интегрированию в верхние уровни управления;

– расширение возможности применения систем мониторинга диагностики и самодиагностики.

Важно также учитывать стоимость жизненного цикла МПЦ, в том числе стоимость сопровождения, связанную с ремонтом, совершенствованием по расширению функциональных возможностей и внедрению новых, более эффективных технологических схем оперативного управления.

Следует обращать внимание на принцип интеграции в системе МПЦ – вертикальный или горизонтальный. При этом предпочтительнее выбирать вариант с горизонтальным принципом интегра-