УДК 621.38

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ФУНКЦИОНАЛЬНОЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МИКРОЭЛЕКТРОННЫХ СИСТЕМ УПРАВЛЕНИЯ ДВИЖЕНИЕМ ПОЕЗДОВ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ

К.А.БОЧКОВ, Д.В.КОМНАТНЫЙ, С.Н.ХАРЛАП

Белорусский государственный университет транспорта, г.Гомель

На железнодорожном транспорте системы железнодорожной автоматики и телемеханики (СЖАТ) призваны в первую очередь обеспечить безопасность движения поездов. Повышенные требования по обеспечению безопасности движения поездов налагали и особые методы построения СЖАТ. Ранее СЖАТ строились на основе аппаратной реализации с использованием специальных реле первого класса надежности с несимметричными отказами. При этом не существовало проблем обеспечения информационной безопасности и доказательства функциональной безопасности и угроз преднамеренного электромагнитного воздействия на СЖАТ.

Современные СЖАТ строятся на основе аппаратно-программных комплексов (АПК) с использованием микроэлектронной элементной базы с симметричными отказами. Для АПК СЖАТ принято различать согласно ГОСТ Р 53431-2009 два вида неработоспособного состояния: защитное и опасное. При этом в защитном состоянии все функции по обеспечению безопасности движения поездов соответствуют требованиям нормативно-технической документации (НТД). В опасном состоянии, значение хотя бы одного параметра по обеспечению функций безопасности движения поездов, не соответствуют требованиям НТД. В опасное состояние система переходит при наличии опасного отказа. Для возможности оценки наличия опасных отказов для каждой из АПК СЖАТ или её компонентов формулируются критерии опасных отказов в соответствующих НТД.

Согласно нормативных документов Федеральная служба по техническому и экспортному контролю (ФСТЭК России) микроэлектронные и микропроцессорные АПК СЖАТ относятся к критическим системам информационной инфраструктуры (КСИИ), в Беларуси – к критически важным объектам информатизации (КВОИ), также, как и практически во всех западных странах. К сожалению, в Республике Беларусь не все СЖАТ отнесены к КВОИ.

Вопросы информационной безопасности таких систем регламентируются различными техническими нормативно-правовыми актами (ТНПА). 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 (в Республике Беларусь – это стандарты СТБ с номерами 1, 2 и 3 серии 34.101 2014 года).

Отдельные аспекты особенностей КСИИ (КВОИ) 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).

Эти стандарты ограничены рамками программно-технического уровня информационной безопасности, что вполне достаточно для оценки продуктов информационных технологий. Однако их недостаточно для микропроцессорных СЖАТ.

Следует отметить, что объектом защиты с позиции информационной безопасности является информация. Основными требованиями по защите информации циркулирующей в АПК СЖАТ является обеспечение ее конфиденциальности, целостности и доступности. При этом обеспечение конфиденциальности приобретает второстепенное значение поскольку циркулирующая в АПК СЖАТ технологическая информация не представляет интереса с позиции ее хищения и дальнейшего использования в корыстных или злонамеренных действиях. Более важными являются требования по целостности и доступности информации.

Целостность предполагает надежное и безопасное управление за счет сохранения контроля над структурой управляющих воздействий, а доступность – над их авторизацией и временем появления.

АПК СЖАТ построены таким образом, что лицо, принимающее решения(ЛПР) (дежурный по станции, диспетчер, машинист и др.) использует эту информацию только по прямому назначению организации движения поездов на станциях и участках железной дороги. И даже если по ошибке или злому умыслу ЛПР попытается создать своими действиями на автоматизированном рабочем месте (АРМ) условия, ведущие к нарушению безопасности движению поездов, то АПК СЖАТ при их исправном состоянии не допустят этого исходя из заложенных в них принципах недопущения опасного отказа.

Вопросы же нарушения целостности информации должны решаться известными методами кодирования, квитирования, криптографии и др. и является основным предметом обеспечения информационной безопасности АПК СЖАТ в соответствии с требованиями НТД.

Микропроцессорные АПК 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, ошибках ПО и внешних воздействий, в том числе и кибератаках.

Для АПК СЖАТ более важным является обеспечение их функциональной безопасности. При этом объектом защиты предмета функциональной безопасности является недопущение опасного отказа. Для этого для различных элементов, устройств систем ЖАТ и программного обеспечения АПК СЖАТ во взаимосвязанных с ТР ТС 003/2011 стандартов формулируются четкие однозначные критерии опасного отказа.

Основные принципы обеспечения безопасного функционирования систем управления определяются концепцией, принятой разработчиком. Наибольшее распространение получила следующая концепция обеспечения безопасности: «Одиночные отказы аппаратных и программных средств не должны приводить к опасным отказам и должны обнаруживаться при рабочих и тестовых воздействиях до того, как в системе произойдет второй отказ».

Основным способом реализации данной концепции является параллельное выполнение ответственных функций в нескольких вычислительных каналах (многоканальная обработка) с последующим сравнением результатов. Если результаты вычислений в различных каналах совпадают, то считается, что система исправна и правильно выполняет свои функции. Если наблюдается расхождение, то принимается решение о наличии отказа в системе и выполняется ее отключение (переход в защитное состояние). При таком подходе любые одиночные отказы не могут привести к опасному отказу, т.к. выработка опасного управляю-

щего воздействия блокируется вторым исправным каналом. Переход в защитное состояние при обнаружении отказа гарантирует, что к опасным последствиям не приведут последующие отказы.

Взаимосвязанными стандартами в разделе 5 (методы контроля) четко определены перечни работ на всех этапах жизненного цикла АПК СЖАТ, начиная с разработки и заканчивая утилизацией, кто их выполняет и какими документами подтверждается соответствие требований этим стандартам.

Основополагающим «вертикальным» стандартом верхнего уровня «Umbrella standard» для функциональной безопасности является МЭК 61508 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью» (IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems), включающий семь частей.

Стандарт дает общие понятие о функциональной безопасности, включает в себя общие требования к организации жизненного цикла систем, связанных с безопасностью, и методы, которые могут использоваться для достижения заданного уровня полноты безопасности.

Общие положения МЭК 61508 детализированы для потенциально опасных областей. Существует ряд стандартов в области функциональной безопасности для различных отраслей, например:

- IEC 62425, «Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling» (системы железнодорожной автоматики и телемеханики);
- IEC 61511, «Functional safety – Safety instrumented systems for the process industry sector» (системы управления опасными производствами);
- IEC 61513, «Nuclear power plants – Instrumentation and control for systems important to safety» (системы контроля и управления атомных станций).

В аэрокосмической отрасли МЭК 61508 явно не используют, но используют такой же подход. Для авионики разработан стандарт RTCA DO-178C «Software Considerations in Airborne Systems and Equipment Certification», в космической отрасли стандарты разрабатываются космическими агентствами, например, NASA использует стандарт STD 8719.13 «Software Safety Standard».

На территории Евразийского экономического союза основным документом, определяющим требования в области функциональной безопасности, является технический регламент Таможенного союза ТР ТС 003/2011 «О безопасности инфраструктуры железнодорожного транспорта». Регламент устанавливает требования к инфраструктуре железнодорожного транспорта, включая системы железнодорожной автоматики. В свою очередь детализация требований осуществляется с помощью ряда поддерживающих стандартов (ГОСТ).

К таким стандартам в области функциональной безопасности систем железнодорожной автоматики можно отнести:

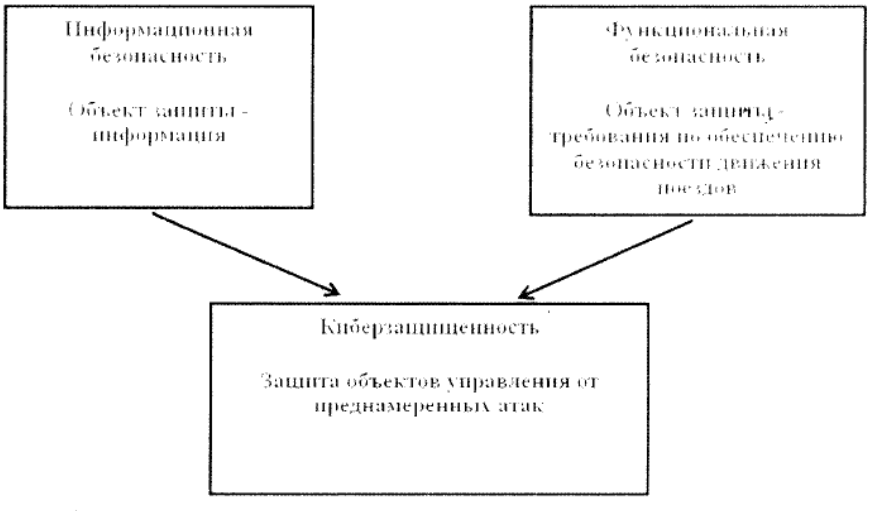
- ГОСТ 33432-2015 «Безопасность функциональная. Политика, программа обеспечения безопасности. Доказательство безопасности объектов железнодорожного транспорта»;
- ГОСТ 33433-2015 «Безопасность функциональная. Управление рисками на железнодорожном транспорте»;
- ГОСТ 34012-2016 «Аппаратура железнодорожной автоматики и телемеханики. Общие технические требования».

Кроме того, имеется ряд национальных стандартов стран Евразийского экономического союза, гармонизированных со стандартами IEC или EN, например:

- СТБ IEC 61508-2014 «Функциональная безопасность электрических, электронных, программируемых электронных систем, относящихся к безопасности»;
- СТБ IEC 62425-2011 «Железные дороги. Системы связи, сигнализации и обработки данных. Электронные системы сигнализации, связанные с безопасностью»;
- СТБ EN 50126-1-2011 «Железные дороги. Требования и подтверждение надежности, пригодности к эксплуатации, ремонтопригодности и безопасности. Часть 1. Основные требования и общий процесс»;
- ГОСТ Р МЭК 61508-2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью»;
- ГОСТ Р МЭК 62279-2016 «Железные дороги. Системы связи, сигнализации и обработки данных. Программное обеспечение систем управления и защиты на железных дорогах»;
- ГОСТ Р МЭК 62280-2017 «Железные дороги. Системы связи, сигнализации и обработки данных. Требования к обеспечению безопасной передачи информации»;
- СТ РК EN 50128-2012 «Железные дороги. Системы телекоммуникационные, сигнализационные и системы для обработки данных, применяемые на железных дорогах. Программное обеспечение для систем управления и защиты на железных дорогах».

Общая тенденция последних лет явно показывает сближение нормативной базы Европейского Союза и Евразийского экономического союза за счет применения единых стандартов МЭК, хотя данный процесс еще не завершен.

Комплексный подход к оценке соответствия программного обеспечения (ПО) АПК СЖАТ, учитывающий требования к функциональной и информационной безопасности, отражен в СТО РЖД 02.049-2014г. (Автоматизированные системы управления технологическими процессами и техническими средствами железнодорожного транспорта. Требования к функциональной и информационной безопасности программного обеспечения. Порядок оценки соответствия), в котором введено понятие киберзащищенности. Это совокупность политик и действий, которые должны быть предприняты для защиты критически важных объектов от деструктивных информационных воздействий (несанкционированный доступ, компьютерная атака, программно-аппаратные закладки, не декларированные возможности, искажение, уничтожение информации), направленные на нарушение штатного функционирования микропроцессорных АПК СЖАТ.



Микропроцессорные АПК СЖАТ, имеют следующие дополнительные особенности с позиций обеспечения киберзащищенности по сравнению с массовым «промышленным» АСУ ТП:

- главной целью кибератаки на микропроцессорные АПК СЖАТ является не информация сама по себе, а возможность воздействия на исполнительные объекты;
- возможная атака будет направлена на вывод из строя микропроцессорной АПК 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 АПК СЖАТ (контроллеры управления исполнительными объектами) с помощью специально разработанных средств, поэтому традиционные (шаблонные), средства защиты могут быть неэффективными.

Наиболее реальной и опасной по последствиям является возможная DDOS кибератака (отказ в обслуживании) путем перехвата злоумышленником управления и задание секущего маршрута в горловине станции, являющегося враждебным всем маршрутам приема и отправки, тем самым блокирующим движение поездов (без нарушения условий безопасности движения) и приносящим большой материальный ущерб. Но такая атака может быть парирована специальными техническими и организационными мероприятиями, один из возможных вариантов которых разработан с БелГУТе.

Одним из новых видов угроз микропроцессорным АПК СЖАТ является «электромагнитный терроризм», суть которого заключается в преднамеренном воздействии сверхширокополосным импульсом высокой энергии.

Европейским союзом в рамках «Seventh Framework Programme» в проекте SECRET SECurity of Railways against Electromagnetic aTtacks (Защита железнодорожных систем от воздействия электромагнитных атак), основной целью которого является оценка рисков и последствий электромагнитных (ЭМ) атак на системы железнодорожной автоматики и телемеханики, было выделено 3 основных вида ЭМ атак:

1. ЕМ-атаки, целью которых является разрушение электронного оборудования;
2. ЕМ-атаки, целью которых является изменение передаваемой информации для отправки ложной информации компонентам железнодорожные системы;
3. ЕМ-атаки, которые нацелены на блокировку передаваемой информации между компонентами железнодорожной системы, чтобы нарушить работу системы и повлиять на ее возможности.

Воздействие широкополосных импульсных помехи на микроэлектронные АПК СЖАТ может вызвать:

- сбои в работе объектных контроллеров, как наиболее ответственных узлов, влияющих на возможное нарушение условий безопасности движения поездов;
- отказ объектных контроллеров, вызванный физическим повреждением и разрушением микроэлектронной элементной базы;
- 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 АПК СЖАТ;
- повреждение и разрушение устройств хранения долговременной информации в центральных компьютерах и АРМ АПК 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 АПК СЖАТ.

Следует также учитывать, что АПК 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.

При проведении испытаний на устойчивость к воздействию СШИП обычно используют специальные генераторы с излучателями на основе антенной решетки из ТЕМ-рупоров или излучателей на основе параболических рефлекторов. Исходя из этого можно предположить использование таких же методов и при преднамеренном воздействии «электромагнитном терроризме» на микроэлектронные СЖАТ. Рупорные излучатели образуют сферические, сравнительно слабонаправленные волны, а параболические рефлекторы формируют плоскую остронаправленную волну с шириной диаграммы в несколько градусов.

В условиях прямой видимости объекта поражения допустимо использовать выражения для поля указанных типов волн во временной области:

плоская волна $E(R,t)=\frac{1}{2}E_m f\left(t-\frac{R}{c}\right)e^{-\frac{\gamma}{2}R}$,

сферическая волна $E(R,t)=\frac{1}{R}E_m f\left(t-\frac{R}{c}\right)e^{-\gamma R}$.

где $E(R,t)$ – мгновенное значение напряженности электрического поля, В/м;
E_m – амплитуда напряженности, В/м;
R – расстояние, м; t – время, с;
c – скорость света, м/с;
γ – коэффициент затухания, м$^{-1}$.

Из приведенных выражений следует, что плоская волна затухает за счет рассеяния в среде, которое в воздушном пространстве достаточно слабо. Сферическая волна затухает с расстоянием и за 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 применении преднамеренного воздействия «электромагнитного терроризма» с предполагаемыми характеристиками используемого генератора в функции от расстояния прямой видимости на объект АПК СЖАТ.

Зная характеристики электрической составляющей поля в раскрыве 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 расчетов в Научно-исследовательской лаборатории (НИЛ) «Безопасность и электромагнитная совместимость технических средств» (БЭМС ТС) НИИЖТа при БелГУТе разработана программа [1], которая осуществляет расчет 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.

Таким образом полученные в НИЛ «БЭМС ТС» БелГУТа научные результаты позволяют проводить оценку соответствия по требованиям к функциональной, информационной и кибербезопасности, 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 структуры / К.А. Бочков, Д.В. Комнатный // Технологии ЭМС. – 2017. – №4. – С. 3-10.