5. Проведение испытаний систем или отдельных частей систем воздействием на них частичными токами молнии с целью выбора оптимального способа защиты

Действующая лаборатория импульсных токов и напряжений на производственной площадке DEHN, квалифицированный персонал и большой опыт исследований в области защиты от грозового электричества позволяют проводить испытания систем и установок на устойчивость к воздействиям удара молнии и подбирать оптимальные варианты защиты оборудования.

Все вышеперечисленные мероприятия могут обеспечить высокую надежность работы оборудования в нормальном режиме эксплуатации, при аварийных импульсных перенапряжениях в сети и в грозовой обстановке.

УДК 621.38

РАЗВИТИЕ СОВРЕМЕННЫХ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ С УЧЕТОМ ТРЕБОВАНИЙ ФУНКЦИОНАЛЬНОЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

К.А. Бочков[1], В.А. Гапанович[2], Д.В. Комнатный[3], Е.Н. Розенберг[4]
1 – Белорусский государственный университет транспорта; 2 – ОАО «РЖД»;
3 – Гомельский государственный технический университет им. П.О. Сухого;
4 – АО «НИИАС»

На железнодорожном транспорте системы железнодорожной автоматики и телемеханики (СЖАТ) призваны, в первую очередь, обеспечить безопасность движения поездов и затем своевременность доставки грузов и пассажиров. Повышенные требования по обеспечению безопасности движения поездов предполагают 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.

Отличительной особенностью СЖАТ является непрерывный (ночью и днем) и длительный (десятки лет) характер работы в сложных климатических условиях, в том числе и на открытом воздухе при воздействии динамических нагрузок и электромагнитных помех.

Современные СЖАТ строятся на основе аппаратно-программных комплексов (АПК) с использованием микроэлектронной элементной базы с симметричными отказами. Для 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 СЖАТ или её компонентов формулируются критерии опасных отказов в соответствующих НТД.

Высокая степень ответственности функций, выполняемых АПК СЖАТ, требует особого подхода к выполнению требований по обеспечению безопасности движения поездов.

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. Проведение оценки соответствия требованиям информационной безопасности (ИБ) АПК СЖАТ осуществляется аккредитованными испытательными лабораториями (центрами), где целесообразно организовать выявление уязвимых мест, закладок и возможных ошибок программного обеспечения (ПО), действие которых может привести к нарушению условий ИБ, отраженных в ТНПА. Такое выявление может производиться также с помощью группы экспертов, пытающихся поставить себя на место злоумышленников, внедряющих закладки. Помимо этого, система защиты должна быть организована таким образом, чтобы информационная безопасность АПК СЖАТ не нарушалась при появлении ошибок ПО или внедрении закладки.

Можно предложить следующие рекомендации по обнаружению закладок и минимизации числа уязвимостей при обеспечении информационной безопасности АПК СЖАТ:

1 Закладки в прикладном ПО можно обнаружить при наличии исходного кода и собственноручной его компиляции.

2 Закладки в системном ПО в первую очередь необходимо искать в операционной системе, в драйверах для промышленных микроконтроллеров.

3 Закладки часто встречаются в аппаратном обеспечении (USB, RS232, RS485, мышь, клавиатура и пр.), а также в нестандартном аппаратном обеспечении (разрабатываемые производителем не стандартизированные платы сопряжения).

4 При минимизации уязвимостей прикладного ПО в первую очередь анализируются:

4.1 уязвимости стека протоколов TCP/IP – здесь должен использоваться контроль целостности и принадлежности пакетов, IP адресов и MAC адресов;

4.2 уязвимости прикладного протокола – сообщения должны быть подписаны или зашифрованы каждым отправителем и проверяться на принимающей стороне, также должно быть исключено дублирование пакетов, подключение

промежуточного сетевого оборудования (концентраторов), и вклинивание в сеть Ethernet;

4.3 уязвимости в графическом интерфейсе – должна быть предусмотрена обязательная аутентификация пользователя, а также невозможность выполнения не декларированных функций.

5 При минимизации уязвимостей системного ПО рекомендуется:

5.1 не устанавливать драйверы для BlueTooth, Wi-Fi, USB и пр., а установленные удалить;

5.2 отключить или заблокировать Firewall неиспользуемые сетевые порты (например, FTP и пр.);

6 При минимизации аппаратных уязвимостей следует:

6.1 запретить аппаратное подключение дополнительных устройств – USB/COM порты должны быть физически отключены, PnP устройства должны быть отключены в BIOS;

6.2 опломбировать или закрыть на ключ корпус (статив);

6.3 физически отключить устройства накопителей на CD, DVD, Floppy и пр.;

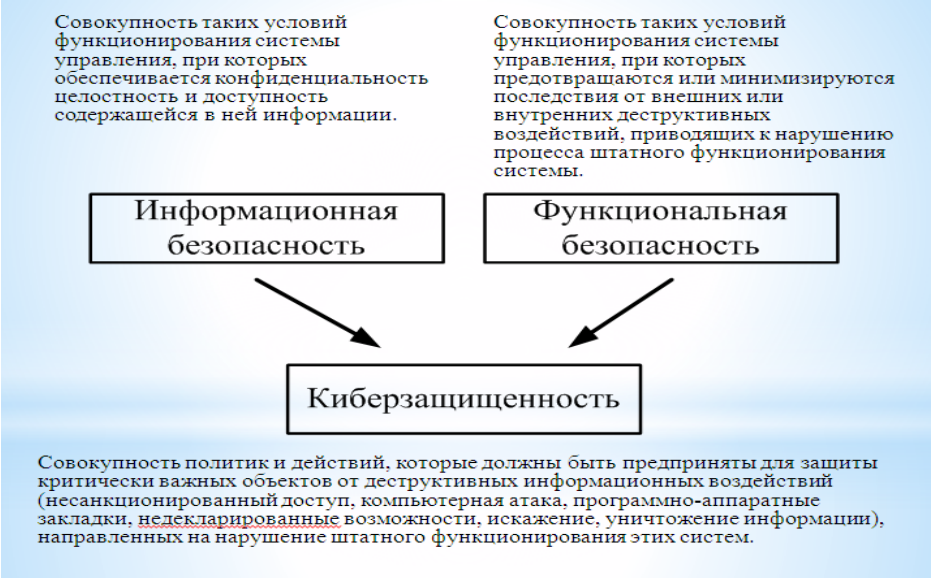
7 Подключение к внешним сетям должно быть организовано только через DMZ (демилитаризованную зону, отдельный компьютер с Firewall).

К основным нормативным документам для анализа защищённости информационных технологий (ИТ) относятся стандарты ГОСТ Р ИСО-МЭК 15408 (3 части) [1–3] и ГОСТ Р ИСО-МЭК 18045 [4] 2012 и 2013 гг. (в Республике Беларусь – это стандарты СТБ с номерами 1, 2 и 3 серии 34.101 2014 г. [5–7].

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 не достаточно для микропроцессорных СЖАТ.

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 воздействий, в том числе и кибератаках.

Комплексный подход к оценке соответствия программного обеспечения (ПО) СЖАТ, учитывающий требования к функциональной и информационной безопасности (рисунок), отражен в СТО РЖД 02.049-2014г.



Понятие киберзащищенности

Микропроцессорные СЖАТ, имеют следующие дополнительные особенности с позиций обеспечения киберзащищенности по сравнению с массовым «промышленным» автоматизированными системами управления технологическими процессами (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 (контроллеры управления исполнительными объектами) с помощью специально разработанных средств, поэтому традиционные (шаблонные), средства защиты могут быть неэффективными;

− микропроцессорные СЖАТ, объединенные в АСУ процессом перевозок верхнего уровня, территориально распределены, работают в реальном масштабе времени и применение средств защиты основанных, например, на методах криптографии, шифрования потребует дополнительных вычислительных ресурсов, что ведет к увеличению времени на реализацию команд и получении информации о состоянии объектов, а это 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 киберзащищенности методами эшелонированной защиты хорошо ложится на эту концепцию.

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

Следует отметить, что воздействие сверхширокополосных импульсных помех (СШИП) различной энергии на микроэлектронные СЖАТ могут приводить к сбоям в работе объектных контроллеров как наиболее ответственных узлов, влияющих на возможное появление опасных отказов, так и к физическому разрушению элементной базы.

Такие 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 воздействие электромагнитного импульса высотного ядерного взрыва микросекундной длительности с шириной спектра от единиц кГц до сотен МГц.

В начале 2000-х гг. на международных симпозиумах по электромагнитной совместимости угроза «электромагнитного терроризма» стала отдельным разделом, а в справочнике «Оружие мира» [8] описаны типы электромагнитного оружия.

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;

$E(t)$ – закон изменения напряженности электрического поля в точке размещения источника поля;

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 расчетной работы в научно-исследовательской лаборатории (НИЛ) «Безопасность и электромагнитная совместимость технических средств» (БЭМС ТС) НИИЖТа при БелГУТе разработана программа [9], 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 биэкс-

поненциального 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 при разработке и создании современных микроэлектронных АПК СЖАТ необходимо учитывать особые требования, предъявляемые им по функциональной и информационной безопасности, киберзащищенности и возможного преднамеренного воздействия СШИП.

Полученные в НИЛ «БЭМС ТС» НИИЖТа при БелГУТе научные результаты и практический опыт работы аккредитованной НИЛ позволяют проводить оценку соответствия по требованиям к функциональной и информационной безопасности, киберзащищенности, а также прогнозировать поведение АПК СЖАТ при воздействии преднамеренного воздействия СШИП.

Это особенно важно в условиях обострения международной обстановки. Полученные результаты по воздействию СШИП могут быть использованы и для микроэлектронных систем двойного назначения.

Список литературы

1 ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель. – Взамен ГОСТ Р ИСО/МЭК 15408-1-2008 ; введ. 2013–12–01. – М. : Росстандарт, 2012. – 58 с.

2 ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 2. Функциональные компоненты безопасности. – Взамен ГОСТ Р ИСО/МЭК 15408-2-2008 ; введ. 2014–09–01. – М. : Росстандарт, 2013. – 164 с.

3 ГОСТ Р ИСО/МЭК 15408-3-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 3. Требования доверия к безопасности. – Взамен ГОСТ Р ИСО/МЭК 15408-3-2008 ; введ. 2014–09–01. – М. : Росстандарт, 2013. – 152 с.

4 ГОСТ Р ИСО/МЭК 18045-2013. Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий. – Взамен ГОСТ Р ИСО/МЭК 18045-2008 ; введ. 2014–07–01. – М. : Росстандарт, 2013.

5 СТБ 34.101.1-2014. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Ч. 1: Введение и общая модель. – Взамен СТБ 34.101.1-2004 ; введ. 2014–09–01. – Мн. : БелГИСС, 2014. – 35 с.

6 СТБ 34.101.2-2014. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Ч. 2: Функциональные требования безопасности. Взамен СТБ 34.101.2-2004 ; введ. 2014–09–01. – Мн. : БелГИСС, 2014. – 90 с.

7 СТБ 34.101.3-2014. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Ч. 3: Гарантийные требования безопасности. Взамен СТБ 34.101.3-2004 ; введ. 2014–09–01. – Мн. : БелГИСС, 2014. – 112 с.

8 **Салливен, Джон П.** Террористическое и нетрадиционное оружие: справочник «Оружие мира» / Джон П. Салливен. – М. : Моркнига, 2008. – 224 с.

9 **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.

МОДЕРНИЗАЦИЯ ЧИСЛОВОЙ КОДОВОЙ АВТОБЛОКИРОВКИ, ПОВЫШЕНИЕ НАДЕЖНОСТИ АППАРАТУРЫ И РАСШИРЕНИЕ ДИАГНОСТИЧЕСКИХ ФУНКЦИЙ В СИСТЕМАХ КОДОВОЙ ЭЛЕКТРОННОЙ АВТОБЛОКИРОВКИ. ПРОГРАММА ИМПОРТОЗАМЕЩЕНИЯ

О.И. Щукин
ЗАО «Ассоциация АТИС»

О компании

Коллектив разработчиков компании ЗАО «Ассоциация АТИС» уже более 25 лет занимается разработкой, выпуском, модернизацией и техническим сопровождением аппаратуры микропроцессорных систем ЖАТ, а также устройств для ее проверки и технического обслуживания.

В России и странах ближнего зарубежья хорошо известны такие разработки компании как:

– измерительные автоматизированные комплексы(стенды) ИАПК РТУ (Р, Б60/Б180, ДСШ, АБЧК), ПК-КОД 2.0;

– приборы МПИ-СЦБ, ИСБ-2;

– аппаратура кодовой электронной автоблокировки КЭБ-1, КЭБ-2;

– управляющий вычислительный комплекс для системы МПЦ-2;

– системы контроля заполнения путей для сортировочных горок КЗП-ИЗ и КЗП-ИЗД и др.

Одно из важнейших направлений деятельности компании – разработка, модернизация и техническое сопровождение аппаратуры интервального регулирования движения поездов – кодовой электронной автоблокировки КЭБ-1 и КЭБ-2.

1 КЭБ-1

Аппаратура кодовой электронной автоблокировки КЭБ-1 (генераторы кодов ГК5(7)-КЭБ и приемники-дешифраторы ПД5(7)-КЭБ) была разработана для реконструкции числовой кодовой автоблокировки (ЧКАБ) и эксплуатируется на железных дорогах с 1995 года. Используется на участках с автономной тягой,