УДК 621.391.825

ЭЛЕКТРОМАГНИТНЫЙ ТЕРРОРИЗМ КАК НОВЫЙ ВИД УГРОЗ ФУНКЦИОНАЛЬНОЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

К.А. БОЧКОВ, Д.В. КОМНАТНЫЙ, И.О. ЖИГАЛИН

Белорусский государственный университет транспорта,
г. Гомель, 246653, Республика Беларусь

Проблема борьбы с терроризмом во всем мире с каждым годом становится все более актуальной. При этом терроризм со временем проникает в различные сферы жизнедеятельности людей и государств. Примерно два десятка лет назад появилось понятие электромагнитного терроризма, связанное с воздействием преднамеренных электромагнитных помех (ПЭМП) на микроэлектронные технические средства (МТС) информационно-телекоммуникационных автоматизированных систем, связанных с защитой информации и на МТС автоматизированных систем управления ответственными технологическими процессами (АСУ ОТП) на транспорте, энергетике, химических производствах. В обоих случаях эти системы относятся к критически важным объектам информатизации (КВОИ в Республике Беларусь) и критическим системам информационной инфраструктуры (КСИИ в Российской Федерации).

Под ПЭМП понимают преднамеренное оказание в преступных или террористических целях мощного электромагнитного воздействия на электронные и электрические системы, нарушающего их функционирование. Этот термин является дословным переводом общепринятого Международной электротехнической комиссией термина Intentional Electromagnetic Interference (IEMI). Воздействие ПЭМП на микроэлектронные системы возможно как по цепям питания, интерфейсным линиям, так и через свободное пространство.

Применительно к МТС информационно-телекоммуникационных автоматизированных систем ПЭМП рассматриваются как фактор угрозы информации в целях ее уничтожения, искажения или блокирования, т.е. относятся к предметной области информационной безопасности.

Воздействие ПЭМП на АСУ ОТП рассматривается как фактор угрозы нарушений условий безопасности функционирования в целях создания условий возникновения аварий, крушений, запредельных режимов работы и относятся к предметной области функциональной безопасности.

Наибольшую опасность для МТС информационно-телекоммуникационных систем (ИТС) и АСУ ОТП представляют малогабаритные переносные генераторы электромагнитных импульсов преднамеренного воздействия (ЭИПВ), излучающие энергию в диапазоне до 10 ГГц.

Существующие сегодня технологические возможности позволяют создавать излучатели электромагнитных импульсов (ЭМИ) с различными массогабаритными характеристиками [1] (от портативных до располагаемых на мобильной платформе), способные формировать с относительно больших расстояний (от единиц метров для портативных до нескольких сотен метров для мобильных источников) уровни падающих полей от 3 до 30 кВ/м, которые могут представлять опасность для микроэлектронных систем информационных инфраструктур. Воздействие таким малогабаритным генератором с близкого расстояния может вывести из строя до 20 компьютеров.

В отличие от проблемы электромагнитного терроризма классические вопросы электромагнитной совместимости (ЭМС) опираются на строгие, вполне определенные нормы и требования, заложенные в стандартах и используемые при испытаниях и измерениях. Современные микроэлектронные устройства АСУ ОТП (в том числе и в защищенном исполнении) и ИТС разрабатываются, проектируются и изготавливаются исходя из предъявляемых к ним требованиям стандартов по ЭМС. И если злоумышленники будут использовать генераторы ЭИПВ с характеристиками, превышающими уровни по помехозащищенности заложенные в соответствующих стандартах, то с большой вероятностью при воздействии (атаке) с помощью ЭИПВ это приведет к нарушению

функционирования микроэлектронных объектов защиты с различными последствиями нарушения их информационной и функциональной безопасности. Хотя многие из этих микроэлектронных систем АСУ ТП, ИТ-технологий спроектированы с учетом защиты от ударов молнии и ЭМ помех, заданных стандартами по ЭМС, однако они остаются уязвимыми к ЭИПВ из-за высокой импульсной мощности излучения и наличия разнообразных путей проникновения и наличия высокочувствительной быстродействующей элементной базы.

Основными причинами возрастания угрозы со стороны воздействия ЭИПВ (электромагнитного терроризма) являются:

1. Увеличение использования сложной и чувствительной электроники в системах обработки информации и управления критически важными компонентами инфраструктуры различных отраслей (энергетика, транспорт, связь, ответственные технологические процессы в промышленности и государственном управлении).

2. Эволюция микроэлектронных систем в направлении миниатюризации, увеличения плотности упаковки, повышения восприимчивости к электромагнитным помехам, увеличения количества портов, через которые проникают помехи и которые ранее не учитывались при разработке и производстве технических средств.

3. Увеличение количества коммерческих, весьма доступных источников ЭМ излучения, которые могут быть использованы в преступных целях.

4. В отличие от многих современных военных систем и автоматизированных систем в защищенном исполнении многие гражданские системы на основе использования компьютерных информационно-телекоммуникационных технологий не имеют охранных зон и специальных методов защиты от проникновения ЭИПВ.

5. Множество контуров в сложной микроэлектронной системе означает наличие множества резонансных частот, а спектр одиночного наносекундного импульса или пачки периодической последовательности импульсов имеют широкий спектр распределения энергии, перекрывающий тактовые частоты современных микроэлектронных систем.

Воздействие ЭИПВ на МТС ИТС и АСУ ОТП, как правило, приводит к нарушению требований по обеспечению как информационной, так и функциональной безопасности. При этом основные угрозы безопасности систем создаются за счет возможности уничтожения, искажения, блокирования информации или нарушения условий безопасности функционирования, приводящие к отказам в обслуживании или авариям, крушениям и нарушении условий обеспечения безопасности ответственных технологических процессов.

Особое место среди автоматизированных систем управления ответственными технологическими процессами занимают современные микроэлектронные системы железнодорожной автоматики и телемеханики (СЖАТ) призванные обеспечивать в первую очередь безопасность движения поездов. Это обусловлено предъявляемыми к ним техническими нормативно-правовыми актами (ТНПА), самыми высокими требованиями уровня полноты безопасности SIL4 по основополагающему международному и гармонизированному с ним межгосударственному стандарту ГОСТ МЭК 61508 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью», состоящему из 7 частей [2].

Отличительной особенностью современных микроэлектронных систем обеспечения безопасности движения поездов (СЖАТ) является территориальная распределенность, расположение в городской среде (часто без определенного периметра охраны). При замене старых релейных СЖАТ на современные микроэлектронные, как правило в тех же зданиях и помещениях, уделяется мало внимания на обеспечение защиты от воздействия ЭИПВ по электромагнитному полю.

Поэтому разработка методов обеспечения защиты микроэлектронной аппаратуры СЖАТ к ЭИПВ, распространяющимся по свободному пространству, является актуальной научно-технической проблемой. Эти методы востребованы как на этапе разработки, так и на этапе сертификации СЖАТ. Подтверждением этому является реализация в Евросоюзе проекта «SECRET Security of railways against electromagnetic attacks» (Защита железнодорожных

систем от воздействия электромагнитных атак) [3], задачей которого является разработка превентивных мер по защите микроэлектронных и компьютерных СЖАТ от электромагнитных помех, в том числе и преднамеренного воздействия. В проекте задействовано десять организаций из пяти стран Евросоюза. Координатором является Французский институт науки и технологии транспорта (IFSTTAR). Однако в открытом доступе имеются лишь общие сведения по данному проекту.

Также в Евросоюзе реализован проект HIPOW Protection of Critical Infrastructures against High Power Microwave Threats (Защита критически важной инфраструктуры от угроз со стороны микроволнового излучения высокой мощности) [4]. Концепция HIPOW заключается в разработке новой нормативно-правовой и организационной базы для защиты от всех соответствующих электромагнитных угроз, которая включает методологии, процедуры и установленные обязанности, возможности для оценки рисков, тестирования, защиты и мер по обеспечению готовности к чрезвычайным ситуациям.

В США аналогичные исследования проводятся в рамках программы DEW (Directed Energy Weapons / направленное энергетическое оружие) Управления военно-морских исследований ONR (Office of Naval Research) [5]. Программа DEW была инициирована в ответ на быстрое развитие и растущую угрозу технологий направленной энергии.

Значительный опыт в НИЛ «Безопасность и ЭМС технических средств» БелГУТа, накопленный при испытаниях на ЭМС микроэлектронных СЖАТ в соответствии с установленными стандартами, позволяет рассматривать два подхода к решению проблемы защиты МТС от преднамеренных электромагнитных помех. Первый подход – физическое моделирование воздействия ЭИПВ на такие средства при помощи генераторов тестовых помеховых воздействий. Проведение таких экспериментов сталкивается со следующими трудностями. Во-первых, число помех и, соответственно, процедур испытаний, оказывается достаточно большим. Поэтому, возрастают сроки проведения испытаний. Во-вторых, генераторы-имитаторы ЭИПВ являются уникальными установками, как правило разрушающего действия, эксплуатация которых затрудняется необходимостью обеспечения безопасности прилегающих объектов. Поэтому в научно-технической литературе ставится задача комплексирования испытаний на электромагнитную совместимость микроэлектронного и компьютерного оборудования критически важных объектов информационной инфраструктуры к различным электромагнитным помехам. Эта же задача возникает в рамках проблемы анализа и прогнозирования стойкости микропроцессорной аппаратуры СЖАТ к ЭИПВ.

Существующей нормативно-технической документацией установлены испытания микроэлектронной аппаратуры СЖАТ на устойчивость к электростатическим разрядам (ЭСР) [6]. Используя принцип подобия, можно указать следующие сходные свойства ЭСР и ЭИПВ: длительность порядка единиц наносекунд и широкая полоса спектра; достаточная для создания сбоев и отказов энергия; воздействие на одни и те же каналы проникновения – неоднородности корпусов аппаратуры СЖАТ.

Допустимо считать, что паразитная антенна – неоднородность выделяет из фронта волны ЭИПВ импульс неизменной, по сравнению с импульсом на выходе генератора, формы с амплитудой, определяющейся условиями распространения. Иными словами, временные параметры импульса не изменяются [7]. Вся поглощаемая антенной мощность излучается внутрь корпуса аппаратуры СЖАТ. Такое предположение допустимо по принципу наихудших условий.

Если осуществить испытания микроэлектронной аппаратуры СЖАТ импульсом генератора-имитатора ЭСР с подобранными методом подобия параметрами, то по результатам испытания можно косвенно судить об устойчивости этих МТС к соответствующему ЭИПВ. Это обосновывается тем, что испытания осуществляются пропорционально-подобными импульсами. При этом появляется возможность исследовать наиболее интересующие проектировщика режимы воздействия ЭИПВ, спрогнозировать максимальную дальность поражения МТС источником ЭИПВ с его максимальной мощностью. Кроме того, одновременно можно установить устойчивость аппаратуры МТС СЖАТ к ЭСР. Согласно

действующим стандартам на ЭМС, использование такой процедуры испытаний, как минимум, исключает необходимость применения уникального испытательного оборудования, сокращает затраты средств, и, в меньшей степени, затраты времени на проведение сертификации СЖАТ по требованиям ЭМС.

Вторым подходом является математическое моделирование процесса проникновения ЭИПВ в корпуса аппаратуры микроэлектронных СЖАТ численными методами либо по аналитическим выражениям для электромагнитного излучения паразитных антенн-неоднородностей корпусов технических средств СЖАТ. Преимуществами этого подхода являются низкие затраты средств, универсальность используемых методов. Но недостатком этого подхода является то, что любая расчетная модель отражает процессы в реальном оборудовании всегда с некоторым приближением, связанным с ограничением математических моделей.

Применяя современные программные комплексы для численного моделирования, можно разработать 3D модель объекта испытаний (ОИ), учитывающую используемые в конструкции объекта материалы и параметры среды распространения. По этой модели производится расчет электромагнитных процессов в ОИ при воздействии ЭИПВ.

Численное моделирование позволяет учесть отражение и поглощение электромагнитных помех, что важно при сложной конструкции объекта испытаний. При моделировании воздействия наносекундных импульсных помех, в частности ЭСР и ЭИПВ, большое значение имеет возможность проследить пути распространения помехи внутри исследуемого объекта, учесть резонансы в корпусе аппаратуры. При подборе материала и конструкции ОИ можно сократить количество испытаний, предварительно промоделировав различные варианты их проведения. Также, появляется возможность предварительно проверить различные варианты защиты от воздействия широкополосных помех (геометрию расположения плат в корпусе и помехоподавляющих экранов).

Результат моделирования может быть наглядно представлен в виде диаграммы визуализации электромагнитного поля помехи либо в виде графиков (рис. 1).

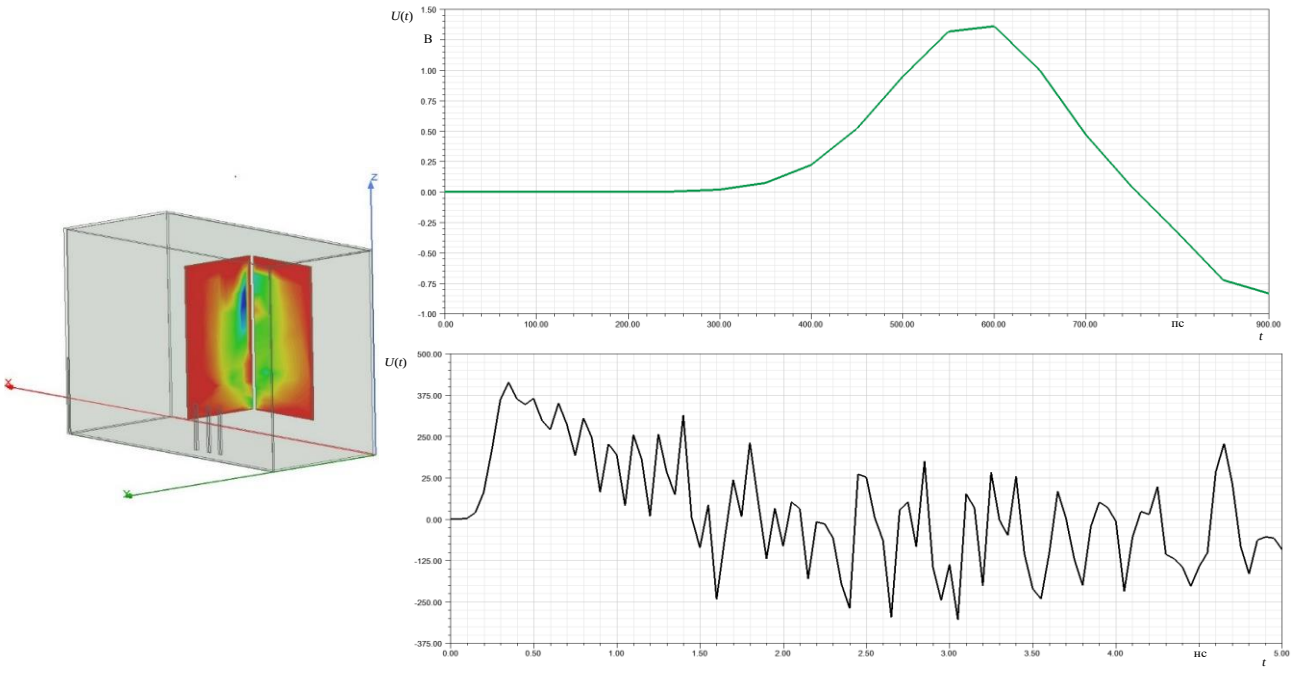

Рисунок 1. – Представление результатов моделирования

При оценке защищенности ОИ численное моделирование может дать гораздо больше информации чем аналитический расчет, но разработка компьютерной модели ОИ достаточно трудоемкий процесс. Вместе с тем, компьютерная модель, отражающая все особенности расположения узлов и элементов ОИ, оказывается настолько сложной, что начинают

проявляться ограничения численных методов и программно-аппаратного обеспечения. Эти ограничения и погрешности расчетов, а также влияние погрешностей задания исходных данных, не отражаются разработчиками доступных программных продуктов. Поэтому достоверность и адекватность результатов моделирования является неполной.

С другой стороны, аналитические модели отличаются более простым математическим аппаратом, вычислительной эффективностью, простотой реализации, отсутствием вычислительных трудностей. Таким образом, применение аналитических методов оправдано там, где требуется высокая скорость вычислений и быстрое получение результата, не в ущерб адекватности моделирования [8]. Наличие простых моделей и методов для расчета помех позволяет выполнить необходимые оценки на этапах проектирования и испытания МТС и принимать решения по оптимизации процедуры испытаний и повышению стойкости этих средств к ЭИПВ.

Прогнозирования воздействия ЭИПВ полезно при планировании процедуры натурных испытаний, так как позволяет осуществить целенаправленную подготовку экспериментов, исключить влияние человеческого фактора, охватить испытанием наиболее опасные режимы воздействия ЭИПВ в пороговых областях.

Проводить численное моделирование целесообразно, если аппаратура СЖАТ на этапе разработки не прошла натурные испытания. В этом случае результаты моделирования применяются для поиска уязвимых мест. Для повышения помехоустойчивости потребуется проведение широкого комплекса расчетов большого числа вариантов конструкции аппаратуры СЖАТ, причем должна быть обеспечена высокая степень соответствия результатов расчетов и реально протекающих электромагнитных процессов. Аналитические методы на современном уровне развития обеспечивают только пессимистические оценки, т.е. с позиций наихудших условий, что гарантирует соответствие требованиям обеспечения УПБ/SIL 4 по ГОСТ Р МЭК 61508-2012 [2].

Заключение

1. В НИЛ «Безопасность и электромагнитная совместимость технических средств» Белорусского государственного университета транспорта разработаны аналитические методы расчета и прогнозирования поведения АСУ ОТП и, в частности, МТС СЖАТ при воздействии на них ЭИПВ. Исследования основаны на использовании принципа подобия при проведении стандартных методов испытаний на устойчивость к электростатическим разрядам.
2. Разработана методика оценки соответствия объекта защиты требованиям функциональной и информационной безопасности в соответствии с требованиями с СТО РЖД 02.049-2014 «Автоматизированные системы управления технологическими процессами и техническими средствами железнодорожного транспорта. Требования к функциональной и информационной безопасности программного обеспечения. Порядок оценки соответствия».
3. Необходимо дальнейшее развитие (исследование) методов анализа механизмов проникновения и прогнозирования последствий воздействия ЭИПВ через различные порты ТС современных микроэлектронных АСУ ТП в различных отраслях промышленности и информационных телекоммуникационных систем передачи, хранения и обработки информации.
4. Конечной целью таких исследований и внедрения их в практику защиты современных микроэлектронных систем в различных отраслях деятельности, связанных с обработкой, хранением и использованием информации в системах управления различного уровня, является минимизация последствий от влияния электромагнитных импульсов преднамеренного воздействия.

Литература

1. Белоконь И.Н., Гончаров А.Н., Долбня С.Н., Кудряшов А.С., Фотеев А.В. Оценка защищенности информационных инфраструктур от воздействия сверхкороткоимпульсных электромагнитных излучений техногенного происхождения. − Технологии электромагнитной совместимости. − 2010. − № 1. − С. 58−67.

2. ГОСТ Р МЭК 61508-2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью.

3. SECRET – SECurity of the Railway network against Electromagnetic aTtacks, http://www.secret-project.eu (Дата доступа: 15.05.2023).

4. The HIPOW Project proposal. EU project grant nr. 284802.

5. Directed Energy Weapons: High Power Microwaves, https://www.nre.navy.mil/organization/departments/aviation-force-projection-and-integrated-defense/aerospace-science-research-351/directed-energy-weapons-high-power-microwaves (Дата доступа: 15.05.2023).

6. ГОСТ 30804.4.2-2013 (IEC 61000-4-2:2008) Совместимость технических средств электромагнитная. Устойчивость к электростатическим разрядам. Требования и методы испытаний.

8. Никольский, В. В. Теория электромагнитного поля / В. В. Никольский. – М.: Высшая школа, 1964. – 584 с.

7. Газизов, Т. Р. Уменьшение искажений электрических сигналов в межсоединениях / Т. Р. Газизов. – Томск: Изд-во НТЛ, 2003. – 167 с.