Список литературы

1. О государственной программе «Цифровое развитие Беларуси на 2021 – 2025 годы» [Электронный ресурс]: Пост. Сов. безоп. Респ. Беларусь от 2 февр. 2021 г. № 66 // Нац. Правовой Интернет-портал Респ. Беларусь. – Режим доступа: https://pravo.by/document/?guid=12551&p0=c22100066&p1=1. – Дата доступа: 2.09.2021.
2. СТБ 34.101.74-2017 Информационные технологии. Системы сбора и обработки данных событий информационной безопасности. Общие требования. [Электронный ресурс] // Интернет-магазин БелГИСС. – Режим доступа: https://shop.belgiss.by/ru/gosudarstvennye-standarty/stb-34-101-74-2017 . – Дата доступа: 2.09.2021.

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 микроэлектронную элементную базу. Воздействие ПЭМП представляет особую опасность для автоматизированных цифровых систем управления ответственными технологическими процессами (АСУ ТП) на транспорте, энергетике , химических производствах.

Это обусловлено непредсказуемым поведением объектов управления при воздействии ПЭМП, приводящим к катастрофам и авариям и связанными с ними потерей жизни людей, огромным материальным ущербом и загрязнением окружающей среды.

Под преднамеренной электромагнитной помехой, 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.

Техническими средствами создания ПЭМП, как правило, являются специальные генераторы сверхкоротких электромагнитных импульсов, как большие стационарные, так и малогабаритные переносные.

Наибольшую опасность для цифровых ИТ систем и АСУ ТП представляют малогабаритные переносные наносекундные импульсные генераторы, излучающие энергию в диапазоне до 10 ГГц. Воздействие таким генератором с близкого расстояния может вывести из строя до 20 компьютеров.

Это связано как с высоким быстродействием современных микроэлектронных компонентов, так и с низким значением напряжения пробоя переходов. Так, например, у запоминающих устройств пороговое напряжение составляет порядка 7 В, а логических интегральных микросхем на МОП-структурах от 7 до 15 В. При этом анализ отказов и повреждений в оборудовании цифровых систем не позволяет порой однозначно идентифицировать причину возникновения повреждений, так как причиной может быть как ПЭМП, так и непреднамеренные помехи, вызванные индуктированными перенапряжениями в цепях питания и другими природными и паразитными техногенными процессами.

Воздействие ПЭМП на цифровые информационные системы и АСУ ТП как правило приводят к нарушению требований по обеспечению как информационной, так и функциональной безопасности. При этом основную угрозу безопасности систем создает не столько несанкционированное раскрытие обрабатываемой информации, сколько нарушение штатного функционирования с последующим нарушением управления системами жизнеобеспечения и условий обеспечения безопасности ответственных технологических процессов.

Особое место среди автоматизированных систем управления технологическими процессами занимают современные микроэлектронные системы железнодорожной автоматики и телемеханики (СЖАТ) призванные обеспечивать в первую очередь безопасность движения поездов. Это обусловлено предъявляемым 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.

Кроме того, особое место СЖАТ обуславливается тем, что они обладают существенными особенностями, усложняющими защиту указанных систем от преднамеренных электромагнитных помех. Во-первых, системы железнодорожной автоматики и телемеханики являются распределенными, многоуровневыми. Количество точек возможного преднамеренного воздействия значительно возрастает. Во-вторых, воздействие на оборудование микроэлектронных и микропроцессорных СЖАТ может осуществляться по свободному пространству, что организуется проще, нежели воздействие по кабельным линиям. В-третьих, затруднительно создать периметры защиты мест размещения оборудования СЖАТ, особенно на перегонах и малых станциях.

Поэтому разработка методов обеспечения защиты микропроцессорной аппаратуры СЖАТ к ПЭМП, 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» (Безопасность железных дорог от электромагнитных атак), задачей которого является разработка превентивных мер по защите микроэлектронных и компьютерных СЖАТ от электромагнитных помех, в том числе и преднамеренного воздействия. В рамках проекта производится и разработка аппаратно-программных комплексов защиты СЖАТ. В проекте задействовано десять организаций из наиболее влиятельных стран Евросоюза. Координатором является Французский

институт науки и технологии транспорта (IFSTTAR). Однако в открытом доступе имеются лишь общие сведения по данному проекту.

Существуют два подхода к решению проблемы защиты микроэлектронной аппаратуры от преднамеренных электромагнитных помех. Первый подход – физическое моделирование воздействия ПЭМП на такую аппаратуру 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 ПЭМП 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 и микроэлектронного и микропроцессорного оборудования критических объектов информационной инфраструктуры к различным электромагнитным помехам. Эта же задача возникает в рамках проблемы анализа и прогнозирования стойкости микропроцессорной аппаратуры СЖАТ к ПЭМП.

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

Допустимо считать, что паразитная антенна – неоднородность выделяет из фронта волны ПЭМП импульс неизменной, по сравнению с импульсом на выходе генератора, формы с амплитудой, определяющейся условиями распространения. Иными словами, временные параметры импульса не изменяются [1]. Вся поглощаемая антенной мощность излучается внутрь корпуса аппаратуры СЖАТ. Такое предположение допустимо по принципу наихудших условий. Тогда амплитуда импульса, излучаемого внутрь корпуса, может быть найдена по балансу мощности антенны, выраженной через вектор Пойнтинга [2]

$$\Pi_{\text{прин}} A_{\text{эфф}} = \Pi_{\text{изл}} A_{\text{геом}}, \quad (1)$$

где $\Pi_{\text{прин}}$ – принимаемый вектор Пойнтинга, Вт/м^2; $A_{\text{эфф}}$ – эффективнаия площадь антенны, м^2, В; $\Pi_{\text{изл}}$ – излучаемый вектор Пойнтинга, Вт/м^2, $A_{\text{геом}}$ – геометрическая площадь антенны, м^2.

Амплитуда принимаемого импульса электромагнитного поля выражается формулой [2]

$$E_{m,\text{пр}} = \frac{FOM}{r} e^{-\gamma r}, \; FOM = \sqrt{60PG}, \quad (2)$$

где FOM – параметр антенны, численно равный амплитуде напряженности электрического поля антенны на расстоянии 1 метр в направлении максимального излучения [2], В/м; P – мощность генератора, Вт; G – коэффициент усиления анетнны генератора, r – расстояние, м; γ – коэффициент ослабления в воздухе.

В данном случае можно принять простейшую функцию ослабления электромагнитного излучения $F(r,\omega) = 1 \cdot e^{-\gamma r}$, так как воздействие ПЭМП предполагается с незначительного расстояния [3].

Вектор Пойнтинга принимаемого импульса имеет вид

$$\Pi_{\text{пр}} = \frac{FOM^2}{240\pi r^2} e^{-2\gamma r}. \quad (3)$$

Вектор Пойнтинга излучаемого импульса

$$\Pi_{\text{изл}} = \frac{E_{m\text{изл}}^2}{240\pi}, \tag{4}$$

где $E_{m\text{изл}}$ – амплитуда излучаемого внутрь корпуса импульса, В/м.

После подстановки (2), (3) и (4) в (1) получается формула для амлитуды излучаемого импульса

$$E_{m\text{изл}} = \frac{FOM}{r}\sqrt{K_{\text{и}}}e^{-\gamma r}, \tag{5}$$

где $K_{\text{и}}$ – коэффициент использования антенны.

Амплитуда напряжения, созданного на антенне импульсом ПЭМП $U_{m\text{изл}} = xE_{m\text{изл}}$, тогда

$$U_{m\text{изл}} = FOM\frac{x}{r}\sqrt{K_{\text{и}}}e^{-\gamma r}, \tag{6}$$

где x – характерный размер отверстия, м.

Импульс ЭСР наиболее просто аппроксимируется импульсом биэкспоненциальной формы [4]. Поэтому для напряжения ПЭМП заданной формы и амплитуды, рассчитанной по (6), необходимо определить амплитуду и временные параметры эквивалентного биэкспоненциального импульса ЭСР по условиям эквивалентности импульсов. Физическим процессам передачи энергии через паразитную антенну наиболее соответствует спектрально-энергетический способ вывода условий эквивалентности импульсов [5]

$$\begin{cases} W_1 = W_2 \\ \Delta f_1 = \Delta f_2 \end{cases}, \tag{7}$$

где W_1 и W_2 – энергии импульсов, Дж; Δf_1и Δf_2 – активные полосы частот, Гц.

Параметры импульса генератора имитатора ЭСР подбираются из следующих соображений. Длительность и временные параметры импульса генератора устанавливаются близкими к параметрам импульса, эквивалентного ПЭМП. Амплитуда импульса генератора-имитатора ЭСР и импульса, эквивалентного ПЭМП, связаны коэффициентом подобия

$$K_{\text{под}} = \frac{W_{\text{экв}}}{W_{ЭСР}} = \frac{U_{m\text{экв}}^2}{U_{mЭСР}^2}. \tag{8}$$

Если осуществить испытания аппаратуры СЖАТ импульсом генератора-имитатора ЭСР с подобранными таким способом параметрами, то по результатам испытания можно косвенно судить об устойчивости этой аппаратуры к соответствующему ПЭМП. Это обосновывается тем, что испытания осуществляются пропорционально-подобными импульсами. Появляется возможность исследовать наиболее интересующие проектировщика режимы воздействия ПЭМП, спрогнозировать пороговые области расположения источников ПЭМП и свойства источников. Кроме того, можно установить устойчивость аппаратуры СЖАТ к ЭСР. 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.

Вторым подходом является математическое моделирование процесса проникновения ПЭМП 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, сравнительно небольшие затраты времени, 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 современное ПО можно разработать 3D модель объекта испытаний (ОИ), учитывающую используемые в конструкции объекта материалы и параметры среды распространения.

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 ПЭМП, 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.

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

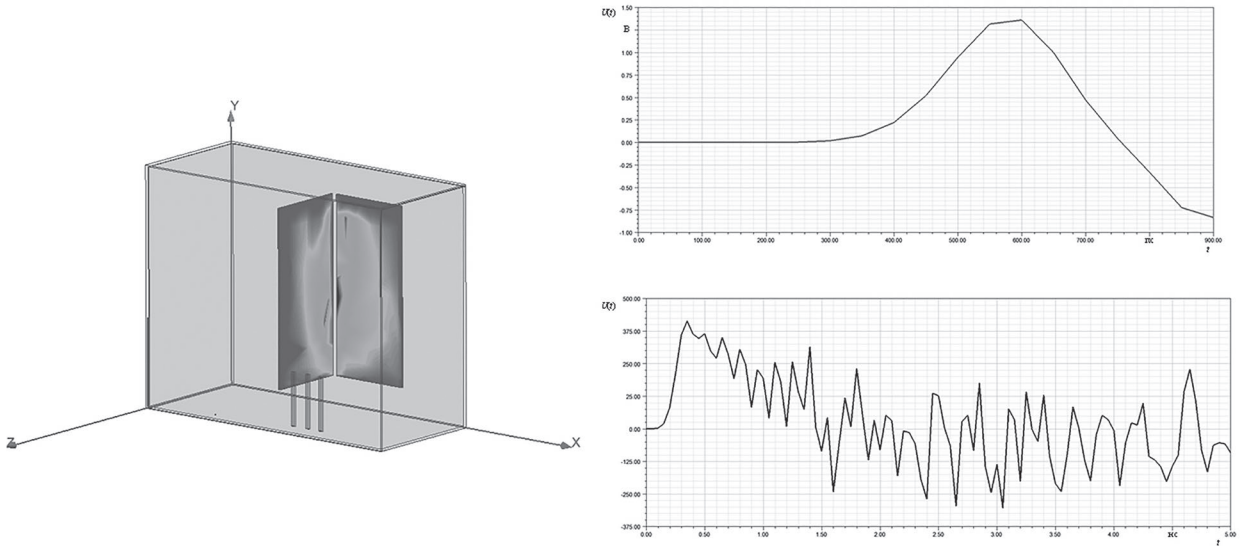

Рисунок 1. Представление результатов моделирования

При оценке защищенности ОИ численное моделирование может дать гораздо больше информации чем аналитический расчет, но разработка компьютерной модели ОИ достаточно трудоемкий процесс. Использование аналитического расчета целесообразно при нормировании параметров испытаний. Прогнозирования воздействия ПЭМП полезно при планировании процедуры натурных испытаний, так как позволяет осуществить целенаправленную подготовку экспериментов, исключить влияние человеческого фактора, охватить испытанием наиболее опасные режимы воздействия ПЭМП в пороговых областях. Проводить численное моделирование полезно, если аппаратура СЖАТ 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, выполнить которые аналитически затруднительно.

Таким образом, проблема защиты СЖАТ от нового вида угроз – электромагнитного терроризма – может быть успешно решена путем комплексирования испытаний на устойчивость к электромагнитным помехам и совместного использования численного моделирова-

ния и аналитического расчета распространения ПЭМП. Это позволяет обеспечить требуемый уровень функциональной и информационной безопасности СЖАТ, как критически важных объектов информационной инфраструктуры.

Список литературы

1. Никольский, В. В. Теория электромагнитного поля / В. В. Никольский. – М.: Высшая школа, 1964. – 584 с.
2. Аполлонский, С. М. Расчеты электромагнитных полей / С. М. Аполлонский, А. Н. Горский. М.: Маршрут, 2006. – 992 с.
3. Кравченко, В. И. Радиоэлектронные средства и мощные электромагнитные помехи / В. И. Кравченко, Е. А. Болотов, Н. И. Летунова. М.: Радио и связь, 1987. – 255 с.
4. Кечиев, Л. Н. Защита электронных средств от воздействия статического электричества / Л. Н. Кечиев, Е. А. Пожидаев. М.: Издательский дом «Технологии», 2005. – 352 с.
5. Бочков, К. А. Элементы моделирования электромагнитной совместимости устройств железнодорожной автоматики и телемеханики / К. А. Бочков, Д. В. Комнатный. Гомель : БелГУТ, 2013. – 185 с.

УДК 004.056.5

О ЗАЩИТЕ ИНФОРМАЦИИ ПРИ ЕЕ УТЕЧКЕ ИЗ ВОЛС

С.В.КРУГЛИКОВ, В.А.ДМИТРИЕВ, Е.П.МАКСИМОВИЧ
Государственное научное учреждение «Объединенный институт проблем информатики Национальной академии наук Беларуси»,
220012, г. Минск, Республика Беларусь

Степень защищенности критически важных объектов от деструктивных информационных воздействий во многом определяется уровнем защищенности информационно-вычислительных и телекоммуникационных средств.

Одним из важнейших требований, предъявляемых к современным телекоммуникационным системам, является обеспечение скрытности и конфиденциальности связи. В волоконно-оптических линиях связи должна быть сформирована надежная, защищенная инфраструктура с использованием всех доступных средств и способов информационной защиты.

Одним из методов защиты информации от несанкционированного доступа при ее распространении в ВОЛС (волоконно-оптические линии связи) являются метод, основанный на использовании лазера, генерирующего импульсы оптического излучения столь малой длительности, что в пределах каждого импульса содержится один фотон, находящийся в состоянии линейной или круговой поляризации.

В современных системах ВОЛС самый перспективный способ передачи информации основан на модуляции интенсивности света. При этом способе передачи каналы утечки информации напрямую связаны с интенсивностью светового потока. Самый простой и действенный способ защиты информации при ее утечке из ВОЛС – снижение мощности модулированного сигнала. Снижение мощности модулированного сигнала может обеспечить полную защищенность информации только от пассивного съема. При активном съеме