УДК 656.25

Д. В. Комнатный, канд. техн. наук

Кафедра автоматики, телемеханики и связи,
Белорусский государственный университет транспорта,
Гомель (Белоруссия)

КОМПЛЕКСНЫЙ АНАЛИЗ УСТОЙЧИВОСТИ СИСТЕМ УПРАВЛЕНИЯ ДВИЖЕНИЕМ ПОЕЗДОВ К СВЕРХШИРОКОПОЛОСНЫМ ЭЛЕКТРОМАГНИТНЫМ ИМПУЛЬСАМ ПРЕДНАМЕРЕННОГО ВОЗДЕЙСТВИЯ

Рассматривается проблема обеспечения устойчивости микропроцессорных систем железнодорожной автоматики к сверхширокополосным импульсам электромагнитного поля. Показана уязвимость современных микропроцессорных систем управления и обеспечения безопасности движения поездов к электромагнитным импульсам преднамеренного воздействия. Выделены особенности критичных к безопасности микропроцессорных систем железнодорожной автоматики, которые определяют отличие проблемы обеспечения устойчивости этих систем от той же проблемы в отношении информационных систем.

Электростатические разряды обладают наибольшей шириной частотного спектра. Они воздействуют на те же апертуры в корпусах технических средств микропроцессорных систем железнодорожной автоматики, что и импульсы преднамеренного воздействия. При падении электромагнитной волны импульса преднамеренного воздействия апертура выделяет этот импульс и передает его внутрь корпуса. Поэтому излучаемый внутрь корпуса импульс преднамеренного воздействия и импульс электростатического разряда могут быть сопоставлены по форме и амплитуде с помощью спектрально-энергетического условия эквивалентности. Рассмотрен расчет энергии и активной полосы частот импульсов, наиболее часто используемых в качестве импульсов преднамеренного воздействия. Продемонстрировано, что расчет активной полосы частот в инженерной практике производится путем построения интегральной кривой распределения энергии в спектре. Разработана методика косвенной оценки воздействия электромагнитного импульса преднамеренного воздействия по данным расчетного прогнозирования устойчивости к электростатическим разрядам.

В статье получен аналог уравнения силового подавления радиоэлектронных средств, который позволяет найти параметры генератора электромагнитных импульсов, создающего опасные для микропроцессорных систем железнодорожной автоматики импульсы. Приведено также выражение для интенсивности помех, характеризующей вклад электромагнитных импульсов преднамеренного воздействия в электромагнитную обстановку на месте расположения микропроцессорной аппаратуры железнодорожной автоматики.

Микропроцессорные системы железнодорожной автоматики, электромагнитный импульс преднамеренного воздействия, помехоустойчивость, киберзащищенность, энергия, электростатический разряд, эквивалентность импульсов, активная полоса частот, неоднородность корпуса, косвенная оценка воздействия

DOI: 10.20295/2412-9186-2021-7-3-379-394

Введение

На современном этапе развития систем железнодорожной автоматики и телемеханики (СЖАТ) происходит не просто широкое внедрение микропроцессорных и микроэлектронных систем, но переход к новым концепциям разработки и эксплуатации систем управления движением поездов – цифровизации и интеллектуализации [1]. Это объясняется необходимостью на новом уровне решить две основные задачи функционирования железнодорожного транспорта – по обеспечению высокого уровня безопасности движения поездов и требуемой провозной способности. Самым эффективным путем решения этих задач является создание комплексной системы управления и обеспечения безопасности движения поездов. В современных условиях повышение безопасности движения требует не только развития традиционных систем железнодорожной автоматики, но и привлечения дополнительных ресурсов на базе информационных технологий и цифровых систем. Таким образом, на базе микропроцессорных СЖАТ организуется система обеспечения безопасности движения, а на базе автоматизированных систем верхнего уровня – система управления процессами перевозок. Взаимодействуя между собой, они создают комплексную систему центров управления процессами перевозок на сети железных дорог [2, 3]. Следовательно, система управления процессами перевозок в настоящее время представляет собой единый комплекс, основанный на единой вычислительной среде и единой цифровой сети. В ней образуются три контура безопасности. Первый из них централизованный, он возникает путем централизации управления маршрутами и координатного управления в диспетчерском центре управления. Второй – децентрализованный, его образуют системы железнодорожной автоматики и телемеханики и технической диагностики. Третий – бортовой, в его составе имеются системы АЛС и автоведения [4].

Вместе с тем возрастает чувствительность элементной базы СЖАТ к электромагнитным помехам и воздействиям. Число возможных видов электромагнитных воздействий также увеличилось, в т. ч. появилась техническая возможность генерирования сверхширокополосных импульсов электромагнитного поля для преднамеренного воздействия ими на микроэлектронные технические средства с целью создания большого потока сбоев в этих средствах или вывода их из строя. Объектами воздействия электромагнитных импульсов преднамеренного воздействия (ЭИПВ) может оказаться и аппаратура современных систем управления перевозочным процессом железнодорожных магистралей, особенно на крупных железнодорожных узлах и линиях скоростного движения [5–7], что повлечет за собой снижение уровня безопасности движения.

1. Постановка проблемы

Для микропроцессорных СЖАТ можно выделить следующие особенности, которые определяют отличие проблемы обеспечения устойчивости этих систем

к ЭИПВ от проблемы обеспечения устойчивости систем информационных технологий к этим же импульсам [8, 9].

Микропроцессорные системы автоматики и телемеханики относятся к нижнему уровню инфраструктуры управления движением поездов, поэтому к ним предъявляются повышенные требования по функциональной безопасности.

Возможная попытка воздействия будет иметь целью как нарушение функциональной безопасности систем железнодорожной автоматики, так и вывод их из строя. Оба этих направления атаки вызывают нарушение условий безопасности движения поездов. Воздействие может быть сосредоточено на тех объектах систем, последствия отказа или сбоя которых наиболее опасны.

Микропроцессорные СЖАТ территориально распределены, часть аппаратуры систем управления концентрируется на постах электрической и диспетчерской централизации. Отдельные блоки и устройства систем (объектные контроллеры на станциях, переездах, перегонах, сигнальные точки автоблокировки) находятся на территории парка станции или на перегонах в непосредственной близости от объектов управления. Системы железнодорожной автоматики практически не имеют периметров защиты, особенно это касается систем автоблокировки и переездной сигнализации, электрической централизации и диспетчерской централизации малых станций. Следовательно, они доступны для преднамеренного электромагнитного воздействия с близкого расстояния.

Таким образом, перед разработчиками СЖАТ встает задача обеспечения устойчивости современных микропроцессорных и компьютерных систем автоматики к возможному воздействию ЭИПВ, которая входит составной частью в комплексную проблему киберзащищенности систем обеспечения безопасности движения поездов [8]. Объединение проблем объясняется тем, что одним из аспектов киберзащищенности является минимизация последствий внешних деструктивных воздействий. Актуальность проблемы подтверждается следующим фактом: в Европейском союзе создан консорциум HIPOW, среди задач которого – анализ воздействия ЭИПВ на системы управления железнодорожным транспортом и разработка мер защиты инфраструктуры железных дорог [10, 11].

2. Косвенная оценка электромагнитных импульсов преднамеренного воздействия

Устойчивость аппаратуры СЖАТ к установленным в настоящее время в технических нормативных правовых актах видам электромагнитных помех подтверждается хорошо апробированными процедурами испытаний. Для ЭИПВ такое подтверждение усложняется тем, что адекватное моделирование этих импульсов требует применения генераторов, являющихся уникальными установками [7]. Поэтому для сокращения цикла испытаний следует применить комплексирование испытаний на устойчивость к разным видам сверхширокополосных импульсов.

Среди испытательных воздействий, предусмотренных действующей нормативно-технической документацией на обеспечение электромагнитной совместимости (ЭМС), электростатические разряды (ЭСР) обладают наиболее широкой полосой частотного спектра. Такая же полоса спектра у ЭИПВ. Энергия обоих типов импульсов концентрируется в малом промежутке времени и имеет большую величину. Неоднородность корпуса (отверстие, щель, болтовое соединение) при воздействии импульса ЭСР становится паразитной антенной, излучающей помеховое электромагнитное поле внутрь корпуса. Поэтому существующие стандарты в области электромагнитной совместимости требуют производить испытательные воздействия на все доступные паразитные антенны [12–15]. Испытания микроэлектронной и микропроцессорной аппаратуры СЖАТ на устойчивость к электростатическим разрядам обязательны, поэтому всегда имеются данные о параметрах импульсов ЭСР, вызывающих отказы и сбои этого средства автоматики.

Предполагается, что импульсы преднамеренного воздействия излучаются направленными антеннами и могут быть представлены в виде сферических или плоских электромагнитных волн. Эти волны незначительно затухают с расстоянием; среда распространения и конфигурации трассы также не вызывают значительного снижения амплитуды импульса и изменения его формы. Это предположение допустимо, т. к. воздействие генераторами ЭИПВ производится, как уже упоминалось, с близкого расстояния. При падении электромагнитной волны ЭИПВ на паразитную антенну образуется неоднородность, которая выделяет из фронта волны импульс и переизлучает его внутрь объема корпуса технического средства. Амплитуды напряженностей электрической составляющей электромагнитного поля, принимаемого и изучаемого импульсов связаны коэффициентом использования антенны [16–18]:

$$E_{т\text{изл}} = \sqrt{K_{\text{и}}}\, E_{т\text{прин}}, \tag{1}$$

где $E_{т\text{изл}}$ – амплитуда напряженности электрического поля импульса, излучаемого внутрь корпуса, В/м; $E_{т\text{прин}}$ – амплитуда напряженности электрического поля импульса, принимаемого паразитной антенной, В/м; $K_{\text{и}}$ – коэффициент использования.

Напряжение на паразитной антенне и напряженность электрической составляющей поля в раскрыве если антенны связаны простыми соотношениями [16, 17, 19]. Так, для прямоугольного отверстия

$$E(t) = \frac{u(t)}{b},\ u(t) = E(t)b, \tag{2}$$

для круглого

$$u(t) = E(t)r,\ E(t) = \frac{u(t)}{r}, \tag{3}$$

для узкой щели

$$E(t)=\frac{u(t)}{l},\ u(t)=E(t)l, \tag{4}$$

где $E(t)$ – напряженность поля, В/м; $u(t)$ – напряжение импульса, В; t – время, с; b – длина стороны отверстия, м; r – радиус круглого отверстия, м; l – длина щели, м.

Электростатический разряд характеризуется импульсом напряжения, который воздействует на неоднородность корпуса технического средства ЖАТ. Из (2–4) следует, что при этом в раскрыве паразитной антенны формируется импульс напряженности электрического поля, который создает помеховое излучение. Из (2–4) также следует, что для каждой неоднородности можно определить импульс напряжения, возникающий в ней под действием принятого ЭИПВ. Допустимо считать, что этот импульс создает излучаемый внутрь корпуса технического средства импульс напряженности поля в раскрыве антенны. Из вышеизложенного следует, что импульс напряжения от импульса преднамеренного воздействия имеет в общем случае выражение

$$u_{\text{изл}}(t)=xE_{m\text{изл}}A_{\text{ЭИПВ}}(t).$$

Если амплитуду напряженности излучаемого импульса выразить по (1), то окончательное выражение для напряжения излучаемого импульса примет вид

$$u_{\text{изл}}(t)=xE_{m\text{прин}}\sqrt{K_{\text{и}}}A_{\text{ЭИПВ}}(t), \tag{5}$$

где x – размерный коэффициент, м; $A_{\text{ЭИПВ}}(t)$ – временная функция формы импульса.

Очевидно, что амплитуда импульса напряжения равна $xE_{m\text{прин}}\sqrt{K_{\text{и}}}$, а форма совпадает с формой электромагнитного импульса преднамеренного воздействия, принятого паразитной антенной.

В статье базой для сопоставления принят импульс ЭСР и результаты испытаний микроэлектронных устройств ЖАТ на устойчивость к электростатическому разряду. Поэтому производится сопоставление импульса напряжения электростатического разряда и импульса напряжения от ЭИПВ. Допустимо полагать, что импульс напряжения от электромагнитного импульса преднамеренного воздействия, эквивалентный импульсу ЭСР соответствующей степени жесткости испытания, создаст в раскрыве паразитной антенны и в корпусе рецептора помеховое электромагнитное поле, вызывающее отказы и сбои рецептора.

Представляется, что эквивалентные импульсы должны обладать одинаковой энергией и иметь одинаковую активную полосу частот. От уровня энергии

зависят последствия воздействия помех на элементную базу. Следовательно, в паразитную антенну от разных импульсов должна поступать одинаковая энергия, которая затем передается в рецепторы при пренебрежимо малых потерях. Активная полоса частот определяет проникающую способность импульсов. Поэтому целесообразно использовать спектрально-энергетический способ вывода условий эквивалентности импульсов [19]

$$\begin{cases} W_1 = W_2 \\ \Delta f_1 = \Delta f_2 \end{cases}, \tag{6}$$

где W_1 и W_2 – энергии импульсов, Дж; Δf_1 и Δf_2 – активные полосы частот, Гц.

Все изложенное позволяет предложить следующую последовательность оценки параметров ЭИПВ, опасного для микроэлектронной аппаратуры систем железнодорожной автоматики.

1. Выбрать форму импульса преднамеренного воздействия.

2. Найти по (6) параметры импульса $u_{изл}$ (t), эквивалентного ЭСР той степени жесткости, для которой проведены испытания и который вызывает отказы и сбои рецептора.

3. Из (5) вычислить амплитуду ЭИПВ, принимаемого паразитной антенной.

Таким образом, может быть получена косвенная оценка воздействия ЭИПВ на технические средства ЖАТ по данным расчетного прогнозирования и экспериментальной проверки устойчивости тех же технических средств к электростатическому разряду.

Оценка позволяет определить параметры принимаемых паразитной антенной импульсов преднамеренного воздействия, вызывающие сбои или отказы микропроцессорных систем автоматики и телемеханики. Испытания на устойчивость к ЭСР являются обязательной составной частью обеспечения электромагнитной совместимости микроэлектронных СЖАТ; методы испытаний электростатическими разрядами достаточно хорошо апробированы [12–15]. Следовательно, таким способом можно получить достоверные данные об устойчивости к электромагнитному импульсу преднамеренного воздействия при сокращении числа испытаний.

3. Определение параметров импульсов спектрально-энергетическим способом

Для реализации приведенной выше методики требуется рассчитывать энергию и активную полосу частот импульсов различной формы. Расчет энергии импульса основывается на известной теореме Рэлея. Расчет активной полосы частот выполняется путем решения уравнения [20]

$$\frac{1}{\pi}\int_{0}^{\Delta\omega} F^2(\omega)\,d\omega = \frac{0.95}{\pi}\int_{0}^{\infty} F^2(\omega)\,d\omega, \tag{7}$$

где $\Delta\omega$ – активная полоса частот, рад/с; ω – круговая частота, рад/с; $F(\omega)$ – модуль спектральной функции, В·с.

Также активная полоса частот может быть вычислена методом моментов [20]. В значительном числе случаев получить решение уравнения (7) крайне затруднительно, так как оно сводится к трансцендентному уравнению с неэлементарными функциями. Метод моментов не универсален и требует вычисления несобственных интегралов. Поэтому для решения уравнения (7) применяется графический метод. Он заключается в построении интегральной кривой распределения энергии $\gamma(f)$ в спектре по выражению

$$\gamma(f) = \frac{\frac{1}{\pi}\int_{0}^{\Delta 2\pi f} F^2(2\pi f)\,d2\pi f}{W}, \tag{8}$$

где W – энергия импульса, Дж.

По графику кривой находится значение активной полосы частот импульса, соответствующее значению $\gamma(f)$=0,95. Активная полоса частот выражается через параметры импульса. Таким образом, графический метод является инженерным методом решения уравнения (7).

Далее рассматриваются особенности применения графического метода для импульса электростатического разряда и импульсов той же формы, что и ЭИПВ, применение которых можно прогнозировать.

Наиболее часто применяется представление ЭСР биэкспоненциальным импульсом. Электромагнитные импульсы преднамеренного воздействия также зачастую имеют биэкспоненциальную форму [21]. Математическое выражение такого импульса целесообразно представить в виде

$$u(t) = A\left(e^{-\gamma\beta_2 t} - e^{-\beta_2 t}\right)\ \beta_1 = \gamma\beta_2, \tag{9}$$

где A – амплитуда импульса, В; β_1, β_2 – характеристические числа импульса, 1/с; γ – отношение характеристических чисел.

Энергия биэкспоненциального импульса

$$W = A^2\left[\frac{1}{2\gamma\beta_2} - \frac{2}{\beta_2(\gamma+1)} + \frac{1}{2\beta_2}\right]. \tag{10}$$

Квадрат модуля его спектральной функции [19]

$$F^2(\omega)=\frac{A^2\beta_2^2(1-\gamma)^2}{\left(\gamma\beta_2^2\right)^2+\omega^2\beta_2^2\left(1+\gamma^2\right)+\omega^4}. \quad (11)$$

Подстановка (11) в (7) или (8) приведет к необходимости вычислить несобственный интеграл со сложной первообразной [22]. Поэтому интегральную кривую целесообразно строить методами компьютерной математики для диапазона частот $f\in\left(0,\ldots\frac{\beta_2}{5},\ldots\frac{n\beta_2}{5}\right)$ где n – счетная переменная. Это объясняется тем, что длительность биэкспоненциального импульса принимается равной $\frac{5}{\beta_2}$ [23].

В настоящее время в качестве ЭИПВ используется модифицированный биэкспоненциальный импульс [24], который описывается выражением

$$u(t)=A\left(\frac{t}{\tau}\right)^n\left[M^{n-1}\exp\left(\frac{-Mt}{\tau}\right)-\exp\left(\frac{-t}{\tau}\right)\right], \quad (12)$$

где τ – постоянная времени, с; M – параметр импульса.

Энергия данного импульса по [24]

$$W=A^2\tau\Gamma(2n+1)\left[1-\left(\frac{2\sqrt{M}}{M+1}\right)^{2n+2}\right], \quad (13)$$

где Γ – гамма-функция Эйлера.

В [24] приведено выражение для спектра импульса (12) на основании которого получено выражение для квадрата модуля спектральной функции

$$F^2(\omega)=A\tau\Gamma(n+1)\times$$
$$\times\left[\frac{1}{\left(1+\left(\frac{\omega\tau}{M}\right)^2\right)^{n+1}}+\frac{1}{(1+(\omega\tau)^2)^{n+1}}+\frac{2\cos(n+1)\left[\operatorname{arctg}\left(\frac{\omega\tau}{M}\right)+\operatorname{arctg}(\omega\tau)\right]}{\left[\left(1+\left(\frac{\omega\tau}{M}\right)^2\right)\left(1+(\omega\tau)^2\right)\right]^{\frac{n+1}{2}}}\right]. \quad (14)$$

Сложность этого выражения приводит к необходимости строить интегральную кривую с помощью программ компьютерной математики. Частота при построении кривой выбирается также, как и в случае биэкспоненциального импульса.

Гауссов импульс вида

$$u(t) = Ae^{-\left(\frac{t}{\tau}\right)^2} \tag{15}$$

используется для описания ЭИПВ также часто, как и биэкспоненциальный [21].

Энергия гауссова импульса

$$W = A^2\tau\sqrt{\frac{\pi}{2}}\,. \tag{16}$$

Для гауссова импульса уравнение (7) имеет вид [25]

$$\frac{1}{\sqrt{2}}\Phi\left(\frac{\omega\tau}{2}\right) = 0{,}95, \tag{17}$$

где Ф – интеграл вероятности.

В нем имеется «неберущийся» интеграл («интеграл вероятности»), оценка которого по графикам и таблицам не дает высокой точности. Поэтому дополнительно использован метод вычисления активной полосы частот из [26]. В этом методе активная полоса частот выражается через моменты времени, которым соответствуют точки перегиба гауссовой кривой напряжения. Комбинация методов дает для гауссова импульса формулу активной полосы частот

$$\omega = \frac{3{,}5}{\tau}. \tag{18}$$

Иногда для описания ЭИПВ используются косинусный, косинус-кубический и косинусный колоколоподобный импульсы. В отношении этих импульсов существуют замкнутые выражения для интегральной кривой (8) [19]. Если задать частоту в диапазоне $f \in \left(0,\ldots\frac{1}{\tau},\ldots\frac{n}{\tau}\right)$, то по интегральной кривой можно найти активную полосу частот этих импульсов как функцию длительности импульса. Соответствующие расчетные соотношения представлены в [19].

Изложенный материал показывает, что метод построения интегральных кривых в сочетании с методами компьютерной математики позволяет решить задачу определения параметров эквивалентных импульсов и, в некоторых случаях, получить замкнутые выражения для активной полосы частот.

4. Энергетический подход к описанию электромагнитной обстановки, созданной ЭИПВ

Поскольку для анализа воздействия ЭИПВ на микроэлектронные СЖАТ целесообразен спектрально-энергетический способ вывода условий эквивалентности, то для описания электромагнитной обстановки, возникающей при наличии ЭИПВ, предпочтителен энергетический подход, основанный на рассмотрении спектра импульса преднамеренного воздействия [28]. В рамках этого подхода спектр принимаемого импульса, который распространяется в виде электромагнитной волны от источника к неоднородностям корпуса рецептора, имеет выражение

$$S(j\omega)=\frac{\sqrt{60PG}}{r}F(r,\omega)\int_{-\infty}^{+\infty}A_{\text{ЭИПВ}}(t)e^{-j\omega t}dt, \qquad (19)$$

где P – мощность генератора, Вт; G – коэффициент усиления передающей антенны; r – расстояние от источника до рецептора помех, м; F– коэффициент затухания.

В наиболее вероятном на практике случае, когда генератор преднамеренного воздействия размещен на диффузной поверхности (трава, почва, гравий) и на расстоянии прямой видимости до рецептора помех, коэффициент затухания рассчитывается по формуле [29–31]

$$F(r,\omega)=1\cdot e^{-\gamma r}, \qquad (20)$$

где γ – коэффициент затухания в воздухе.

Тогда из (19) для амплитуды принимаемого ЭИПВ справедлива формула

$$P_{\text{отк},j,k}=0. \qquad (21)$$

Формула (21) – аналог известного уравнения силового подавления радиоэлектронных средств [32, 33]. Расчет по этой формуле тем точнее, чем выше частота спектральных составляющих ЭИПВ. Такие условия характерны для излучения радиолокаторов, которые зачастую используются при расчетах и экспериментах как аналоги генераторов электромагнитных импульсов преднамеренного воздействия [7, 29].

По уравнению силового подавления и его аналогу (21) можно решать различные задачи расчета воздействия ЭИПВ на микроэлектронную аппаратуру железнодорожной автоматики. В частности, найти мощность и коэффициент усиления антенны генератора, который расположен на заданном расстоянии от микропроцессорной аппаратуры ЖАТ и создает в паразитной антенне импульс, способный вызвать отказ или сбой. Другая задача – расчет расстояния

от генератора импульсов преднамеренного воздействия до рассматриваемой системы автоматики, на котором возможно вызвать сбой или отказ [33].

Из (19) может быть получено выражение для энергии принимаемого электромагнитного импульса преднамеренного воздействия [28]:

$$W = \frac{1}{\pi}\int_{-\infty}^{\infty} S^2(j\omega)\,d\omega = \frac{60PG}{\pi r^2} F^2(r,\omega)\int_{-\infty}^{+\infty} A^2_{\text{ЭИПВ}}(t)\,e^{-j2\omega t}\,dt\,. \qquad (22)$$

Величина

$$I = \frac{60PG}{\pi r^2} e^{-2\gamma r} \qquad (23)$$

является интенсивностью помех и определяет вклад различных сверхширокополосных импульсных помех, в т. ч. ЭИПВ, в электромагнитной обстановке на месте эксплуатации микроэлектронной аппаратуры СЖАТ. Она служит для оценки электромагнитной обстановки и ее влияния на функциональную безопасность систем железнодорожной автоматики [28].

Заключение

В статье показано, что по результатам аналитического расчета и натурного моделирования воздействия электростатического разряда на технические средства СЖАТ возможна косвенная оценка формы и параметров ЭИПВ, опасных для исследуемой СЖАТ, а также прогнозирование устойчивости ее к этим импульсам.

Обосновано применение спектрально-энергетического способа вывода условий эквивалентности импульсов для косвенной оценки формы и параметров ЭИПВ. Расчет энергии импульсов выполняется по теореме Рэлея. Для расчета активной полосы частот установлено, что эта задача может быть решена путем построения интегральной кривой распределения энергии в спектре.

Для описания электромагнитной обстановки, созданной импульсами преднамеренного воздействия, необходимо применять энергетический подход. Приведен аналог уравнения силового подавления радиоэлектронных средств, который позволяет рассчитывать параметры генератора ЭИПВ и размеры зон подавления. Выведено выражение для интенсивности помех от ЭИПВ в составе электромагнитной обстановки на месте эксплуатации аппаратуры железнодорожной автоматики.

Достоинства предлагаемого метода – сокращение объема испытаний, снижение потребности в дорогостоящем и малодоступном оборудовании. Математический аппарат метода позволяет избежать математических трудностей решения трансцендентных уравнений, а в некоторых случаях – получить замкнутое

выражение для активной полосы частот. Немаловажным обстоятельством является и то, что исследование нового вида электромагнитных угроз – электромагнитных импульсов преднамеренного воздействия – ведется на основе уже достаточно изученного электростатического разряда.

К сожалению, графоаналитический метод оказывается довольно трудоемким и требует высокой аккуратности при выполнении графической части расчета.

Поэтому предлагаемый в статье комплексный анализ устойчивости к ЭИПВ можно считать полезным и востребованным для решения проблемы обеспечения киберзащищенности микропроцессорных СЖАТ, критичных к безопасности, на ранних этапах разработки и проектирования с учетом современных угроз. Эта проблема возникла сравнительно недавно, следовательно, предлагаемые в статье методы являются актуальными.

Библиографический список

1. *Розенберг М. Н.* Инновационные технологии интервального регулирования – основа системы управления движением на МЦК / М. Н. Розенберг // Автоматика, связь, информатика – 2019. – № 6. – С. 5–10.
2. *Рогачева И. Л.* Эксплуатационная надежность систем электрической централизации нового поколения / И. Л. Рогачева. – М.: Маршрут, 2006. – 220 с.
3. Системы железнодорожной автоматики, телемеханики и связи. В 2-х ч. / под. ред. А. В. Горелика. – М.: ФГБОУ «Учебно-метод. центр по образованию на ж.-д. трансп., 2012. – 212 с.
4. Высокоскоростной железнодорожный транспорт. Общий курс. В 2-х т. / под. ред. И. П. Киселева. – М.: Ф ГБОУ «Учебно-метод. центр по образованию на ж.-д. трансп., 2014. – Т. 1. – 308 с.
5. *Ogunsola A*. Electromagnetic compatibility in railways: Analysis and Management / A. Ogunsola, A. Mariscotti. – Berlin-Heidelberg: Springer-Verlag, 2013. – 544 p.
6. *Flammini F.* Railway Safety, Reliability and Security: Technologies and System Engineering / F. Flammini. N. Y.: IGI Global, 2012. – 488 p.
7. Электромагнитный терроризм на рубеже тысячелетий / М. Бакстром; под ред. Т. Р. Газизова. – Томск: Изд-во Томского университета, 2002. – 206 с.
8. *Бочков К. А*. Развитие современных систем железнодорожной автоматики и телемеханики с учетом требований функциональной и информационной безопасности / К. А. Бочков, В. А. Гапанович, Д. В. Комнатный, Е. Н. Розенберг // Автоматика и телемеханика на железнодорожном транспорте: Сборник докладов 9-й международной конференции / РГУПС, ОАО РЖД, Северокавказская ж. д. – Ростов-на-Дону, 2018. – С. 224–231.
9. *Торокин А. А*. Инженерно-техническая защита информации / А. А. Торокин. – М.: Гелиос АРВ, 2005. – 960 с.
10. *Schleger A*. Infrastructure Risk Assesment and Management / A. Schleger, C. A. Brebbia. – N. Y.: WIT Press, 2016. – 158 p.
11. *Wright D*. Surveillance in Europe / D. Wright, R. Kreissl. – L.: Routledge, 2015. – 415 p.

12. *Кечиев Л. Н.* Защита электронных средств от воздействия статического электричества / Л. Н. Кечиев, Е. А. Пожидаев. – М.: Издательский дом «Технологии», 2005. – 352 с.
13. *Voldman S. H.* ESD circuits and Devices / S. H. Vodman. – N. Y.: Wiley & Sons, 2015. – 544 p.
14. *Voldman S. H.* Electrical Overstress (EOS): Devices, Curcuits and Systems / S. H. Vodman. – N. Y.: Wiley & Sons, 2013. – 370 p.
15. *Vashchenko V.* System Level ESD Protection / V. Vashchenko, M. Scholz. – N. Y.: Springer International Publishing, 2014. – 331 p.
16. *Лавров А. С.* Антенно-фидерные устройства / А. С. Лавров, Г. Б. Резников. – М.: Советское радио, 1974. – 386 с.
17. *Stutzman W. L.* Antenna theory and design / W. L. Stutzman, G. A. Thiele. – N. Y.: Wiley&Sons, 2012. – 843 p.
18. Handbook of Antenna Technologies / Z. N. Chen, D. Liu, H. Nakano, X. Qing, T. Zwich (edit). – Singapure: Springer Singapure, 2016. – 3470 p.
19. *Бочков К. А.* Элементы моделирования электромагнитной совместимости устройств железнодорожной автоматики и телемеханики / К. А. Бочков, Д. В. Комнатный. – Гомель: БелГУТ, 2013. – 185 с.
20. *Харкевич А. А.* Избранные труды: в 3 т. – М.: Наука, 1973. – Т. 2. Линейные и нелинейные системы. – 560 с.
21. *Гайнутдинов Р. Р.* Прогнозирование электромагнитных помех в межсоединениях печатных плат цифровых электронных средств при преднамеренном воздействии сверхширокополосного электромагнитного импульса / Р. Р. Гайнутдинов, З. М. Гизатуллин. – Технологии ЭМС. – 2010. – № 3 (39). – С. 44–52.
22. *Прудников А. П.* Интегралы и ряды / А. П. Прудников, Ю. А. Брычков, О. И. Маричев. – М.: Наука, 1981. – 800 с.
23. *Шебес М. Р.* Задачник по теории линейных электрических цепей / М. Р. Шебес, М. В. Каблукова. – М.: Высш. школа, 1990. – 544 с.
24. *Беличенко Н. П.* Сверхширокополосные импульсные радиосистемы / Н. П. Беличенко, Ю. И. Буянов, В. И. Кошелев. – Новосибирск: Наука, 2015. – 475 с.
25. *Гоноровский И. С.* Радиотехнические цепи и сигналы. – М.: Радио и связь, 1986. – 511 с.
26. *Баскаков С. И.* Радиотехнические цепи и сигналы. – М.: Высшая школа, 2000. – 462 с.
27. *Ellingson S. W.* Radio Systems Engineering / S. W. Ellingson. – L.: Cambridge University Press, 2016. – 716 p.
28. *Иванов В. А.* Электромагнитная совместимость радиоэлектронных средств / В. А. Иванов, Л. Я. Ильницкий, М. И. Фузик. – Киев: Техника, 1983. – 189 с.
29. *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.
30. *Аполлонский С. М.* Расчеты электромагнитных полей / С. М. Аполлонский, А. Н. Горский. – М.: Маршрут, 2006. – 992 с.
31. *Sadiku M. T.* Elements of Electromagnetic / M. T. Sadiku. – Oxford: Oxford University Press, 2018. – 926 p.
32. *Комиссаров Ю. Я.* Помехоустойчивость и электромагнитная совместимость радиоэлектронных средств / Ю. Я. Комиссаров, С. С. Родионов. – Киев: Техника, 1978. – 208 с.
33. Радиоэлектронная борьба. Силовое подавление радиоэлектронных систем / В. Д. Добыкин, А. И. Куприянов, В. Г. Пономарев, Л. Н. Кустов, под ред. А. И. Куприянова. – М.: Вузовская книга, 2007. – 468 с.

D. V. Komnatny, PhD in Technical Sciences

Department of Automation, Telemechanics and Communication,
Belarusian State University of Transport, Gomel (Belarus)

COMPREHENSIVE STABILITY ANALYSIS OF TRAIN CONTROL SYSTEMS TO ULTRA-WIDEBAND ELECTROMAGNETIC PULSES OF INTENTIONAL IMPACT

The problem of ensuring the stability of microprocessor systems of railway automatics to ultra-wideband pulses of an electromagnetic field is considered. The vulnerability of modern microprocessor control systems and ensuring the safety of train traffic to electromagnetic impulses of deliberate influence is shown. The features of safety-critical microprocessor systems of railway automatics are highlighted, which determine the difference between the problem of ensuring the stability of these systems from the same problem with respect to information systems.

Electrostatic discharge has the widest frequency spectrum. They act on the same apertures in the housings of technical means of microprocessor systems of railway automation, as the impulses of deliberate action. When an electromagnetic wave of an intentional impulse is incident, the aperture releases this impulse and transmits it to the inside of the case. Therefore, an intentional impulse emitted into the housing and an electrostatic discharge impulse can be compared in shape and amplitude using the spectral-energy equivalence condition. The calculation of the energy and the active frequency band of the pulses most often used as deliberate pulses is considered. It is demonstrated that the calculation of the active frequency band in engineering practice is carried out by constructing an integral curve of the energy distribution in the spectrum. A technique has been developed for the indirect assessment of the impact of an electromagnetic pulse of deliberate action according to the calculated prediction of resistance to electrostatic discharges.

An analogue of the equation of power suppression of radio-electronic means is demonstrated in the article allowing finding the parameters of an electromagnetic pulses generator which creates pulses dangerous for microprocessor systems of railway automation. An expression is also given for the intensity of interference, which characterizes the contribution of deliberate electromagnetic pulses to the electromagnetic environment at the location of the microprocessor equipment of railway automation.

Microprocessor-based railway automation systems, deliberate electromagnetic pulse, noise immunity, cyber resistance, energy, electrostatic discharge, pulse equivalence, active frequency band, body heterogeneity, indirect impact assessment

DOI: 10.20295/2412-9186-2021-7-3-379-394

References

1. *Rozenberg M. N.* (2019) Innovatsionnyye tekhnologii interval'nogo regulirovaniya – osnova sistemy upravleniya dvizheniyem na MTSK [Innovative train spacing control technologies as a bases for the traffic management system at the Moscow central ring]. *Avtomatika, svyaz, informatika* [*Automation, communication, informatics*], no. 6, pp, 5–10. (In Russian)
2. *Rogacheva I. L.* (2006) *Ekspluatatsionnaya nadezhnost' sistem elektricheskoy tsentralizatsii novogo pokoleniya* [*Operational reliability of new generation electrical centralization systems*]. Moscow, Marshrut Publ., 220 p.
3. *Sistemy zheleznodorozhnoy avtomatiki, telemekhaniki i svyazi. V. 2-kh ch. pod. red. A. V. Gorelika* [*Railway automation, telemechanics and communication systems. In 2 parts. Under general*

editorship of A. V. Gorelik]. Moscow, Federal State Budgetary Educational Institution of Further Professional Education "Educational and Methodological Center for Education in Railway Transport", 2012, 348 p. (In Russian)
4. *Vysokoskorostnoy zheleznodorozhnyy transport. Obshchiy kurs. V 2-kh t., pod. red. I. P. Kiseleva* [*High speed rail transport. General course. In 2 volumes, under general editorship of I. P. Kiselev*]. Moscow, Federal State Budgetary Educational Institution of Further Professional Education "Educational and Methodological Center for Education in Railway Transport", 2014, vol. 1, 308 p. (In Russian)
5. *Ogunsola A., Mariscotti A.* (2013) Electromagnetic compatibility in railways: Analysis and Management. Berlin-Heidelberg: Springer-Verlag, 544 p.
6. *Flammini F.* (2012) Railway Safety, Reliability and Security: Technologies and System Engineeryng. N. Y.: IGI Global, 488 p.
7. *Elektromagnitnyy terrorizm na rubezhe tysyacheletiy. pod red. T. R. Gazizova* [*Electromagnetic terrorism at the turn of the millennium. Under general editorship of T. R. Gazizov*]. Tomsk: Tomsk University Publ., 2002, 206 p. (In Russian)
8. *Bochkov K. A., Gapanovich V. A., Komnatnyy D. V., Rozenberg E. N.* (2018) Razvitiye sovremennykh sistem zheleznodorozhnoy avtomatiki i telemekhaniki s uchetom trebovaniy funktsional'noy i informatsionnoy bezopasnosti [Development of modern systems of railway automation and remote control in view of the requirements of functional and information security]. *Avtomatika i telemekhanika na zheleznodorozhnom transporte: Sbornik dokladov 9-y mezhdunarodnoy konferentsii* [*Automation and remote control on railway transport: collection of reports of the 9th international conference*]. Rostov-on-Don, 224–231 pp. (In Russian)
9. *Torokin A. A.* (2005) *Inzhenerno-tekhnicheskaya zashchita informatsii* [*Engineering and technical protection of information*]. Moscow, Helios ARV Publ., 960 p.
10. *Schleger A.***,** *Brebbia C. A.* (2016) Infrastructure Risk Assesment and Management. N. Y.: WIT Press, 158 p.
11. *Wright D., Kreissl R.* (2015) Surveillance in Europe. London: Routledge, 415 p.
12. *Kechiyev L. N., Pozhidayev E. A.* (2005) Zashchita elektronnykh sredstv ot vozdeystviya staticheskogo elektrichestva [Protection of electronic devices from the effects of static electricity]. Moscow, publ. house "Technologies", 352 p. (In Russian)
13. *Voldman S. H.* (2015) ESD circuits and Devices. N. Y.: Wiley & Sons, 544 p.
14. *Voldman S. H.* (2013*)* Electrical Overstress (EOS): Devices, Curcuits and Systems. N. Y.: Wiley & Sons, 370 p.
15. *Vashchenko V., Scholz M.* (2014) System Level ESD Protection. N. Y: Springer International Publishing, 331 p.
16. *Lavrov A. S, Reznikov G. B.* (1974) Antenno-fidernyye ustroystva [Antenna-feeder devices]. Moscow, Sovetskoye Radio Publ., 386 p. (In Russian)
17. *Stutzman W. L., Thiele G. A.* (2012) Antenna theory and design. N. Y.: Wiley&Sons, 843 p.
18. *Chen Z. N., Liu D., Nakano H., Qing X., Zwich T.* (2016) Handbook of Antenna Technologies. Singapure: Springer Singapure, 3470 p.
19. *Bochkov K. A., Komnatny D. V.* (2013) *Elementy modelirovaniya elektromagnitnoy sovmestimosti ustroystv zheleznodorozhnoy avtomatiki i telemekhaniki* [*Elements of modeling electromagnetic compatibility of railway automation and remote control devices*]. Gomel', Belorussian State University of Transport Publ., 185 p.
20. *Kharkevich A. A.* (1973) *Izbrannyye trudy v 3kh t. T. 2. Lineynyye i nelineynyye sistemy*. [*Selected works in 3 volumes Vol. 2. Linear and nonlinear systems]*. Moscow, Nauka Publ., 560 p. (In Russian)

21. *Gaynutdinov R. R., Gizatullin R. R.* (2010) Prognozirovaniye elektromagnitnykh pomekh v mezhsoyedineniyakh pechatnykh plat tsifrovykh elektronnykh sredstv pri prednamerennom vozdeystvii sverkhshirokopolosnogo elektromagnitnogo. [Prediction of electromagnetic interference in interconnections of printed circuit boards of digital electronic devices under the deliberate action of an ultra-wideband electromagnetic pulse]. *Tekhnologii EMS* [*EMC Technologies*], no. 3(39), pp. 44–52. (In Russian)
22. *Prudnikov A. P., Brychkov Yu. A., Marichev O. I.* (1981) *Integraly i ryady* [*Integrals and series*]. Moscow, Nauka Publ., 800 p. (In Russian)
23. *Shebes M. R., Kablukova M. V.* (1990) *Zadachnik po teorii lineynykh elektricheskikh tsepey* [*Problem book on the theory of linear electric circuits*]. Moscow, Vysshaya shkola Publ., 544 p. (In Russian)
24. *Belichenko N. P., Buyanov Yu. I., Koshelev V. I.* (2015) *Sverkhshirokopolosnyye impul'snyye radiosistemy* [*Ultra-wideband impulse radio systems*]. Novosibirsk, Nauka Publ,. 475 p. (In Russian)
25. *Gonorovskiy I. S.* (1986) *Radiotekhnicheskiye tsepi i signaly* [*Radiotechnical circuits and signals*]. Moscow, Radio i svyaz' Publ., 511 p. (In Russian)
26. *Baskakov S. I.* (2000) *Radiotekhnicheskiye tsepi i signaly* [*Radiotechnical circuits and signals*]. Moscow, Vysshaya shkola, 462 p. (In Russian)
27. *Ellingson S. W.* (2016) Radio Systems Engineering. London: Cambridge University Press, 716 p.
28. *Ivanov V. A. Ilnitskiy L. Y., Fuzik M. I.* (1983) *Elektromagnitnaya sovmestimost' radioelektronnykh sredstv* [*Electromagnetic compatibility of radioelectronic devices*]. Kiev, Tekhnika Publ., 189 p. (In Russian)
29. Kravchenko V. I., Bolotov Y. A., Letunova N. I. (1987) *Radioelektronnyye sredstva i moshchnyye elektromagnitnyye pomekhi* [*Radioelectronic devices and powerful electromagnetic interference*]. Moscow, Radio i svyaz' Publ., 255 p. (In Russian)
30. Apollonsky S.M., Gorsky A.N. (2006) *Raschety elektromagnitnykh poley* [*Calculations of electromagnetic fields*]. Moscow, Marshrut Publ., 92 p. (In Russian)
31. Sadiku M. T. (2018) Elements of Electromagnetic. Oxford: Oxford University Press, 926 p.
32. Komissarov Yu. Ya., Rodionov S. S. (1978) *Pomekhoustoychivost' i elektromagnitnaya sovmestimost' radioelektronnykh sredstv* [*Noise immunity and electromagnetic compatibility of radio-electronic equipment*]. Kiev, Tekhnika Publ., 208 p. (In Russian)
33. Dobykin V. D., Kupriyanov A. I., Ponomarev V. G., Kustov L. N., under general editorship of Kupriyanov A. I. (2007) *Radioelektronnaya bor'ba. Silovoye podavleniye radioelektronnykh system* [*Electronic warfare. Power suppression of radio-electronic systems*]. Moscow, Vuzovskaya kniga Publ., 468 p. (In Russian)

Статья представлена к публикации членом редколлегии, профессором К. А. Бочковым
Поступила в редакцию 16.03.2021, принята к публикации 22.04.2021

КОМНАТНЫЙ Дмитрий Викторович – кандидат технических наук, старший научный сотрудник кафедры «Автоматика, телемеханика и связь» Белорусского государственного университета транспорта
toe4031@gstu.by