УДК 621.391.825

ПРОГНОЗИРОВАНИЕ УСТОЙЧИВОСТИ ЭЛЕКТРОННОЙ ТЕХНИКИ К ЭЛЕКТРОМАГНИТНЫМ ИМПУЛЬСАМ ПРЕДНАМЕРЕННОГО ВОЗДЕЙСТВИЯ

Комнатный Д.В., к.т.н.
Гомельский государственный технический университет им. П.О. Сухого

e-mail: toe4031@gstu.by

В статье рассматривается проблема прогнозирования устойчивости электронной техники к электромагнитным импульсам преднамеренного воздействия (ЭИПВ). Эти воздействия могут осуществляться злоумышленниками с целью создания чрезвычайных ситуаций. В этом заключается угроза электромагнитного терроризма, проявления которого возможны и в Республике Беларусь. В статье проанализированы пути распространения ЭИПВ и показана их аналогия с путями проникновения электростатического разряда в электронную технику. Также выполнено сравнение энергии в спектре биэкспоненциального импульса разряда статического электричества и гауссова ЭИПВ. Сравнение показало, что биэкспоненциальный импульс является более опасным. Сделан вывод, что по устойчивости электронной аппаратуры к электростатическому разряду можно косвенно судить о ее устойчивости к ЭИПВ. Это дает возможность сократить цикл испытаний электронной техники на устойчивость к ЭИПВ и получить экономический эффект.

The problem of electronic technique immunity prediction for electromagnetic impulse of purpose action (EIPA) is considered in the article. Theses actions can be realized by plotters with the goal to create the extraordinary situations. The danger of electromagnetic terrorism concludes in this fact. The demonstrations of this danger are possible in the Republic of Belarus too. The ways of EIPA propagation are analyzed in the article, and the analogy with the penetration ways of electrostatic discharges into electronic technique is shown. Also the comparison of spectrum energy in biexponential impulse of static electricity discharge and Gauss impulse of EIPA is fulfilled. The comparison show, that biexponential impulse is more dangerous. The conclusion is made, that one can indirectly destine about EIPA immunity on electronic hardware electrostatic discharge immunity. This gives the opportunity to reduce the testing cycle of electronic technique immunity to EIPA and to result the economical effect.

(Поступила в редакцию 28 апреля 2011 г.)

Введение

В настоящее время имеется возможность создания генераторов электромагнитных импульсов длительностью порядка единиц наносекунд и высокой амплитуды, в связи с чем появилась реальная опасность использования этих импульсов, как импульсов преднамеренного воздействия на электронное и компьютерное оборудование информационно-управляющих систем, в том числе и ответственных технологических процессов. Целью воздействия является дезорганизация работы органов управления и производственных объектов, вплоть до создания чрезвычайных ситуаций (аварии на электростанциях, железных дорогах, химических заводах). В этом и заключается «электромагнитный терроризм», возможностью проявления которого нельзя пренебрегать в современных условиях [1], в том числе и в Республике Беларусь.

Основным способом борьбы с этой опасностью является проектирование технических средств, устойчивых к воздействию ЭИПВ, и подтверждение этой устойчивости путем натурных испытаний. Вместе с тем, современные требования к электронной и микропроцессорной технике включают в себя требование устойчивости к широкому набору электромагнитных помех, в частности к электростатическому разряду (ЭСР). Проверка, удовлетворяет ли данное техническое средство требованиям электромагнитной совместимости, осуществляется также

путем натурных испытаний. Импульсы ЭСР имеют длительность порядка наносекунд и достаточно высокую амплитуду [2]. В этом свойства импульсов ЭСР и ЭИПВ оказываются сходными. В свою очередь, отмеченное обстоятельство дает основания для углубленного сравнительного анализа механизмов распространения воздействия обоих типов помех.

Основная часть

По [3, 4] наиболее вероятным является применение ЭИПВ в форме двойной экспоненты и в форме гауссовой кривой. Эти импульсы генерируются на замаскированной установке, размещенной поблизости от атакуемого объекта, и распространяются в пространстве. Простейшей легко маскируемой антенной является протяженный штырь, создающий волны цилиндрического типа, поэтому для дальнейшего анализа рассматривается этот тип волн. Его математическая запись имеет вид [5]:

$$\xi(R,t)=\frac{1}{\sqrt{R}}E\left(t-\frac{R}{c}\right)e^{-\gamma R}, \qquad (1)$$

где $\xi(R,t)$ – мгновенное значение напряженности поля, В/м;

R – расстояние, м;

t – время, с;

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

c – скорость света, м/с;

γ – коэффициент затухания, $м^{-1}$.

Формула (1) показывает, что форма импульса в однородной изотропной среде не искажается, а амплитуда уменьшается по сложной зависимости от расстояния. Уровень ослабления в воздушной среде является малым. По данным исследования [6], стены зданий оказывают крайне малое воздействие на ЭИПВ, если не приняты специальные меры по экранированию здания. Следовательно, импульс приходит к поражаемому объекту неизмененной формы, но сниженной амплитуды. Достигнув неоднородности, например отверстия, в корпусе изделия электронной техники, ЭИПВ наводит в ней импульс напряжения. Неоднородность становится паразитной антенной, которая излучает помеховое электромагнитное поле внутрь корпуса и наводит помехи в узлах изделия.

Импульс ЭСР с реального объекта или имитированный генератором можно считать имеющим форму двойной экспоненты [2]. ЭСР характеризуется высокими напряжениями и малыми токами. Импульсы ЭСР производятся на те же неоднородности в корпусе электронной аппаратуры, которые являются каналами для проникновения ЭИПВ [7]. Возбуждаемые импульсом напряжения ЭСР неоднородности также становятся источниками помехового электромагнитного излучения в корпусе изделия.

Таким образом, видно, что механизмы воздействия обоих типов помех на электронные изделия крайне сходны. При этом излучение при возбуждении неоднородности в корпусе ЭСР может быть даже выше, чем при возбуждении от ЭИПВ. Это объясняется тем, что в первом случае разряд происходит непосредственно в неоднородность, тогда как во втором случае импульс приходит к отверстию ослабленным за счет расстояния.

Уровень помех, создаваемых внутри корпуса электронного изделия, определяется энергией импульсов ЭСР и ЭИПВ, воздействующих на паразитный излучатель в корпусе. Для сравнения опасности рассматриваемых в статье помех для электронной аппаратуры необходимо сравнить энергию указанных выше импульсов, которые имеют различную форму и воздействуют на одну и ту же паразитную антенну. На основании результатов работ [5] и [8] по эквивалентности импульсов сравниваемые импульсы должны иметь одинаковую длительность, одинаковое значение максимума амплитуды спектра и анализироваться в одинаковой полосе частот.

На рис. 1 показан квадрат амплитудного спектра биэкспоненциального импульса со следующими параметрами: амплитуда импульса имеет значение 6000 В, длительность – $6 \cdot 10^{-8}$ с, параметры экспонент $\alpha_1 = 9{,}324 \cdot 10^7$ с$^{-1}$, $\alpha_2 = 3{,}871 \cdot 10^8$ с$^{-1}$. Такой импульс моделирует импульс испытательного генератора ЭСР при испытании по третьей степени жесткости. Квадрат спектра определяется по формуле [9]

$$S^2(\omega) = \frac{U^2(\alpha_2 - \alpha_1)^2}{(\alpha_1\alpha_2 - \omega^2)^2 + \omega^2(\alpha_2 + \alpha_1)^2}, \quad (2)$$

где S – спектр импульса, В·с;

ω – круговая частота, рад/с;

U – напряжение импульса, В;

α_1, α_2 – временные параметры импульса, с$^{-1}$.

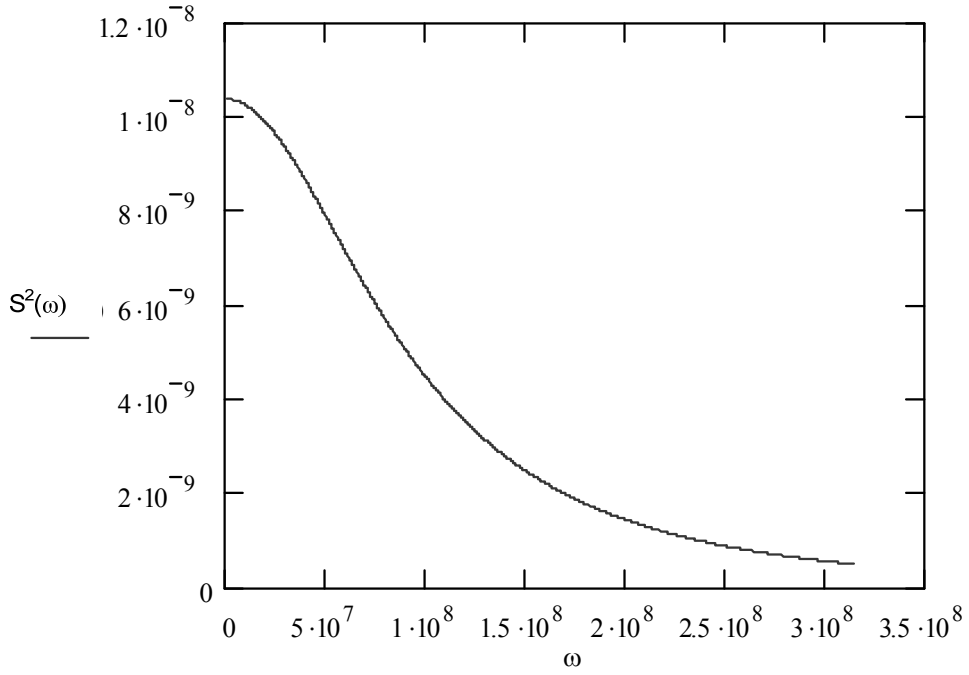

Рисунок 1 – Квадрат спектра биэкспоненциального импульса

На рисунке 2 приведен квадрат амплитудного спектра гауссова импульса той же длительности с амплитудой 1000 В, что обеспечивает амплитуду спектра, близкую к амплитуде спектра биэкспоненциального импульса. Квадрат спектра гауссова импульса G рассчитывается по выражению [9]

$$G(\omega) = \pi A^2 \tau^2 \left(\exp - \left(\frac{\omega\tau}{2} \right)^2 \right)^2, \quad (3)$$

где A – амплитуда импульса, В.

τ – длительность импульса, с.

Анализ рис. 1 и 2 показывает, что в полосе частот $0 \ldots 3 \cdot 10^8$ рад/с огибающая спектра биэкспоненциального импульса охватывает большую площадь, чем огибающая спектра гауссова импульса. Поэтому энергия спектра биэкспоненциального импульса больше. Этот вывод следует также из расчета энергии обоих импульсов по известной теореме Рэлея [9].

Значение энергии биэкспоненциального импульса составляет 0,363 Дж, а значение энергии гауссова импульса – 0,075 Дж.

Следовательно из двух имеющих близкие параметры импульсов более опасным является биэкспоненциальный. Устойчивая к этому импульсу электронная аппаратура будет устойчива и к гауссову импульсу преднамеренного воздействия, имеющему сходные параметры. Устойчивость к ЭИПВ с другими параметрами можно оценить, используя масштабные коэффициенты.

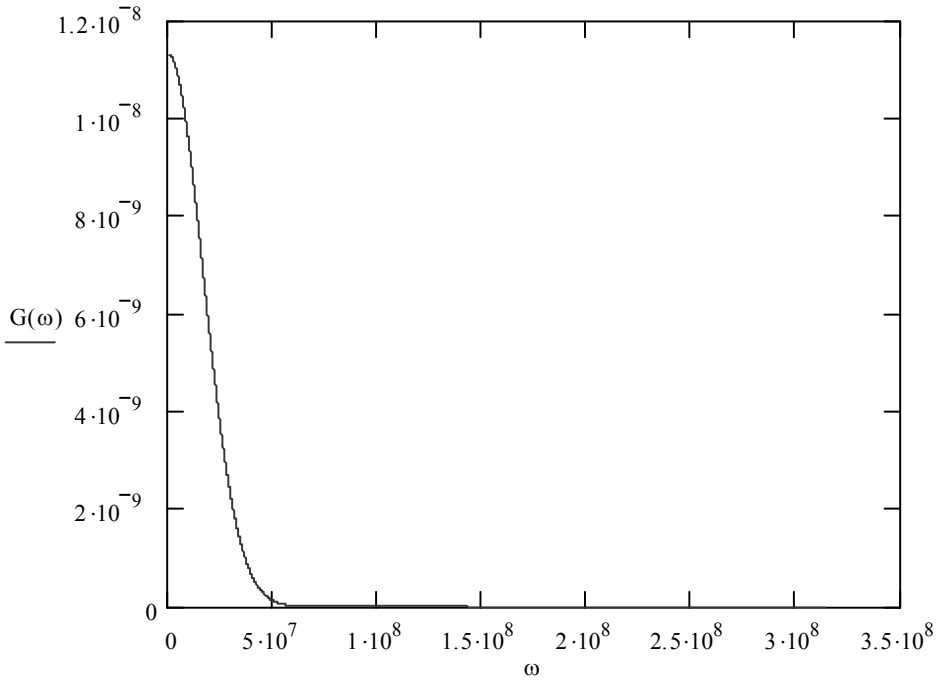

Рисунок 2 – Квадрат спектра гауссова импульса

Выводы

Сказанное позволяет сделать вывод, что по устойчивости изделия электронной техники к ЭСР можно косвенно судить и об устойчивости того же изделия к ЭИПВ, распространяющимся по свободному пространству. Испытания на устойчивость к ЭСР производятся для всех типов электронного оборудования информационно-управляющих систем. Следовательно, добившись устойчивости к ЭСР конструктивными мерами и подтвердив ее данными испытаний, можно увеличить и устойчивость того же технического средства к ЭИПВ. Таким образом, достигается значительная экономия средств на проведение мероприятий по обеспечению устойчивости к ЭИПВ, ускоряется разработка и внедрение новой техники. Кроме этого обеспечивается достаточный уровень устойчивости этой техники к современным угрозам, что повышает ее конкурентоспособность и привлекательность для потребителя. Все это принесет значительные экономические преимущества производителям электронной техники, а также преимущества в вопросах обеспечения безопасности государства.

Литература

1. Электромагнитный терроризм на рубеже тысячелетий / М. Бакстром [и др.] ; под ред. Т.Р. Газизова. – Томск : Изд-во Томского университета, 2002. – 206 с.

2. Хабигер, Э. Электромагнитная совместимость. Основы ее применения в технике. – М . Энергоатомиздат, 1995. – 304 с.

3. Гизатуллин, З.И. Технология прогнозирования и повышения электромагнитной совместимости цифровых электронных средств при внешних высокочастотных импульсных воздействиях / З.И. Гизатуллин // Технологии ЭМС. – 2010. – № 3 (34). – С. 22–29.

4. Гизатуллин, Р.И. Прогнозирование защиты информации в цифровых электронных средствах при преднамеренном электромагнитном воздействии по цепи питания / Р.И. Гизатуллин // Технологии ЭМС. – 2010. – № 3 (34). – С. 64–72.

5. Аполлонский, С.М. Расчеты электромагнитных полей / С.М. Аполлонский, А.Н. Горский. – М. : Маршрут, 2006. – 982 с.

6. Гайнутдинов, Р.М. Прогнозирование электромагнитной обстановки в здании при преднамеренном воздействии сверхширокополосного электромагнитного импульса / Р.М. Гайнутдинов // Технологии ЭМС. – 2010. – № 3 (34). – С. 53–63.

7. ГОСТ Р 513 17.4.2-99. Устойчивость к электростатическим разрядам. Требования и методы испытаний. – Взамен ГОСТ 29191.–91 ; введ. 1999–12–24. – М. : Изд-во стандартов, 2000. – 26 с.

8. Бочков, К.А. Импульсы помех в эквивалентном представлении / К.А. Бочков, Ю.Ф. Березняцкий, Н.В. Рязанцева // Проблемы и перспективы развития устройств автоматики, связи и вычислительной техники на железнодорожном транспорте : сб. науч. тр. / РГУ ПС. – Ростов-на-Дону : РГУ ПС, 1999. – С. 103–107.

9. Баскаков, С.И. Радиотехнические цепи и сигналы / С.И. Баскаков. – М. : Высш. шк., 2005. – 462 с.