УДК 621.391.825; 378

*Т.Р. Газизов*

# ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ И БЕЗОПАСНОСТЬ: ОБРАЗОВАТЕЛЬНЫЕ АСПЕКТЫ

Томский государственный университет систем управления и радиоэлектроники

## Введение

Одна из особенностей современного высшего образования – появление большого числа новых специальностей, востребованных жизнью. Например, только на радиотехническом факультете (РТФ) Томского государственного университета систем управления и радиоэлектроники (ТУСУР) за несколько лет число технических специальностей увеличилось с 2 до 12. Открытие новых специальностей требует подготовки новых специализированных дисциплин, отвечающих высоким требованиям университетского образования, таким как обучение методам решения различных задач с помощью системного подхода, использование результатов самых современных научных исследований, применение компьютерных технологий [1].

Между тем новые дисциплины должны появляться и в ходе обновления учебных программ в соответствии с новыми государственными стандартами по подготовке специалистов. Одной из новых и весьма актуальных проблем, требующих своего отражения в образовательном процессе, является проблема электромагнитных (ЭМ) помех. Она довольно широка, поскольку касается ЭМ помех как непреднамеренных, так и преднамеренных, как аппаратуре, так и людям [2, 3]. В данной работе рассматриваются образовательные аспекты этой большой проблемы в части преднамеренных электромагнитных помех (ПЭМП) аппаратуре.

## Предыстория проблемы

Под электромагнитной совместимостью (ЭМС) понимают способность прибора, устройства или системы удовлетворительно функционировать в своей ЭМ обстановке, не создавая недопустимых помех чему-либо в ней. Понимание необходимости знания основ ЭМС привело к постановке курсов по этой молодой науке в течение последнего десятилетия в большинстве технических университетов мира. Об актуальности этого процесса говорят регулярные секции «ЭМС в образовании» на каждом международном симпозиуме по ЭМС, а также тот факт, что до сих пор ЭМС общество IEEE проводит ежегодный конкурс на постановку курса по ЭМС с призовым фондом 10 000 дол.

Однако над обществом нависла новая угроза – преднамеренных электромагнитных помех, под которыми понимают преднамеренное оказание мощного ЭМ воздействия на электронные и электрические системы, нарушающего их нормальное функционирование. (ПЭМП, создаваемые в террористических целях, иногда называют ЭМ терроризмом.)

Предпосылками возникновения этой угрозы стали, с одной стороны, достижения в создании мощных источников ЭМ поля, а с другой – неуклонное уменьшение уровней сигналов электронных систем. Все более широкое внедрение в жизнь общества электронных систем, приведшее к сильной зависимости от них, а также доступность устройств для создания помех сделали эту угрозу реальностью.

В последние годы ПЭМП обращают особое внимание специалистов по ЭМС. Деятельность Международного радиосоюза (URSI) и Международной электротехнической комиссии (МЭК) инициировала важную научную и практическую работу по решению этой проблемы, о чем свидетельствует ряд докладов, представленных на различных международных конференциях и симпозиумах последних лет. Не вдаваясь в детальный обзор открытой истории проблемы [4, 5], отметим лишь некоторые ее вехи: первый доклад [6], первый обзор [7], первый семинар [8], резолюция Совета URSI по преступной деятельности с помощью ЭМ средств [9], первая отдельная секция симпозиума [10], первая книга [11], первый тематический выпуск журнала [12]. Примечательно внимание и отечественных специалистов к угрозам ПЭМП различным системам: безопасности [13], атомной энергетики [14], нефтегазодобывающей отрасли [15], авионики [16, 17].

## Серьезность проблемы

Мощность современных источников ПЭМП измеряется гигаваттами, а дальность действия может измеряться километрами [18], так что окружающая нас электроника весьма уязвима к воздействию ПЭМП. Действительно, например, типовой компьютер, который выполняет множество важных функций в инфраструктуре нашего общества, может сбоить (правда, при открытой крышке корпуса) при облучении ЭМ полем с напряженностью электри-

ческой составляющей всего 30 В/м [19]. Казалось бы, ЭМ поле легко экранируется корпусом, но выясняется, что даже среднее значение ослабления электрического поля корпусом компьютера может составить всего 2 раза [20, с. 14]. Вообще, оказывается, что для корпуса с щелями может быть много частот, на которых поле внутри корпуса больше, чем снаружи [18]; не исключение даже фюзеляж вертолета [21]. Заметим, что и внутри полностью замкнутых металлических поверхностей поле может быть больше, чем снаружи, например, в 3 раза для электрического поля в центре полой сферы на резонансной частоте [22].

Очевидно, что ПЭМП не посредством излучения, а по проводникам могут повлиять гораздо сильнее. Оказывается, что короткие импульсы могут легко распространиться по сети питания здания от трансформаторной станции до блока питания компьютера [23]. Часто полагают, что компьютер защищен традиционным устройством бесперебойного питания, однако выясняется, что и оно весьма подвержено деструктивному воздействию [13]. Грамотное построение защиты при укорочении импульсов, воздействующих по проводникам, оказывается нетривиальным делом: напряжение срабатывания традиционных газовых разрядников возрастает, например, с 250 до 800 В, а с определенного порога разряд и вовсе не наступает; те же тенденции, хотя и в меньшей степени, имеют место и для металлооксидных варисторов; проблема, казалось бы, снимается быстродействующими защитными диодами, но их предельные токи составляют всего несколько ампер [24].

Проблема ПЭМП оказалась очень серьезной даже для военной электроники. Например, согласно авторитетным производителям бортовых радаров в России [25], существующие бортовые радиолокационные системы практически беззащитны к воздействию мощного короткоимпульсного СВЧ излучения. Другим аспектом в свете чрезвычайно актуальной и нерешенной проблемы терроризма может стать ЭМ терроризм. Как тут не процитировать индийских военных ученых: «Технология – великий нивелировщик, который может полностью изменить расстановку сил. Даже самое "сильное" государство сталкивается с опасностью "получить щелчок" от разных мафий и террористических организаций. Поддерживать технологический перевес против терроризма становится все более трудной задачей» [26].

Следовательно, необходимо осознать, что решение проблемы ПЭМП крайне сложно, если возможно вообще. Однако можно и, видимо, очень нужно говорить об ослаблении влияния ПЭМП. И представляется, что не последние, если не главные, роли в этой работе отведены просвещению и образованию: угроза, к которой все будут готовы, потеряет свою силу. По мнению автора, внедрение аспектов, связанных с ПЭМП, в сознание будущих инженеров так же необходимо, как уже выполняющееся внедрение аспектов экологии и безопасности жизнедеятельности в сознание студентов и школьников.

## Просвещение

Действительно, всю связанную с ПЭМП работу URSI и МЭК, о которой уже упоминалось, в определенном смысле можно отнести к просветительской. Сначала URSI на своей Генеральной ассамблее 1999 г. для широкого круга специалистов всего мира впервые дал определение проблеме ПЭМП и сформулировал, какую работу необходимо начать для ее решения. Затем представители этих авторитетных организаций развернули активную деятельность по освещению этой проблемы буквально на каждом международном симпозиуме по ЭМС: пленарные доклады, семинары, открытые заседания соответствующей комиссии URSI, заседания отдельных секций с докладами и полной их публикацией. Следующим шагом стали анализ проведенных исследований и разработка на его основе ряда новых стандартов МЭК, связанных с мощными ЭМ воздействиями: теперь весь опыт, накопленный в мире, концентрируется и представляется экспертами высшей квалификации в доступном для всех виде.

Автор полностью разделяет озабоченность специалистов по ЭМС проблемой ПЭМП и поэтому также включился в эту просветительскую работу. Так, тема ПЭМП стала предметом 11 докладов автора на отечественных и зарубежных конференциях и симпозиумах за 2000–2003 гг.: доклады полностью опубликованы, лично представлены автором и вызвали большой интерес аудитории. Кроме того, для отечественных специалистов различных служб безопасности и студентов вузов соответствующих специальностей издана книга [11], включающая 29 научных работ по ПЭМП, отобранных из зарубежной печати за 1998–2001 гг. и переведенных автором на русский язык. Эти работы, собранные воедино, дают полное представление о сути проблемы, знакомят с результатами самых свежих исследований ее различных аспектов и позволяют выработать подходы к ее решению. Наконец, в ТУСУРе организуются открытые семинары с лекциями зарубежных ученых, известных своими исследованиями по ЭМ помехам. Первый такой семинар состоялся 9 июля 2001 г. На нем выступили с лекциями профессора Мишель Яноз (Швейцария) и Вальтер Ван Лук (Бельгия). На следующем семинаре, который планируется на февраль 2004 г., профессор Яноз, уже в качестве заслуженного лектора ЭМС общества IEEE, проведет цикл лекций, посвященный влиянию мощных ЭМ воздействий на различные системы.

## Образование

Нельзя не отметить бурный всплеск интереса в обществе к вопросам безопасности, который уже отразился на образовательном процессе. Например, 5 из 12 упоминавшихся технических специальностей РТФ ТУСУРа связаны с безопасностью аппаратуры. Успешно проводится ежегодный всероссийский конкурс студентов и аспирантов по информационной безопасности SIBINFO. Открыт и работает Региональный учебно-научный центр Восточной Сибири и Дальнего Востока по проблемам информационной безопасности в системе высшей школы. Внимание ВАК к подготовке специалистов высшей квалификации в этом направлении отразилось в новых паспортах специальностей диссертационных советов. Например, среди областей исследования специальности 05.12.04 отдельной строкой прописана «разработка методов разрушения информации с помощью помех и ее защиты в радиосистемах различного назначения», а в формулу специальности 05.12.07 включено «решение задач электромагнитной совместимости». Защищаются докторские диссертации по этой тематике [27, 28].

Однако специфика проблемы ПЭМП, в силу ее новизны, еще не успела найти должного отражения в высшем образовании. Между тем, учитывая высокую актуальность проблемы и пятилетний период подготовки специалистов, этот процесс не должен затягиваться. Автор рассматривает его как доведение работы URSI и МЭК до учебных классов и аудиторий и как доцент ТУСУРа пытается внести в нее свой посильный вклад. Так, различные факты и численные данные, касающиеся проблемы ПЭМП, включаются (насколько это уместно и возможно) в стандартные университетские курсы по ЭМС и САПР. Кроме того, организована трехмесячная дипломная практика лучших студентов в ЭМС группе Федерального технологического института г. Лозанны, известной своими исследованиями влияния мощных ЭМ воздействий на различные системы. Наконец, автором готовится новый университетский курс «Электромагнитная совместимость и безопасность радиоэлектронной аппаратуры», включенный в учебный план трех специальностей РТФ ТУСУРа.

Нельзя не отметить одну из основных трудностей, выявившихся при постановке этого нового и достаточно сложного курса – недостаток базовых знаний студентов по основам ЭМС. Действительно, ЭМ помехи, которые из-за сложности часто оставались белым пятном даже в радиотехническом образовании, требуют к себе гораздо больше внимания в высшей школе. По мнению автора, например, включение раздела по ЭМС в каждый дипломный проект технических специальностей аналогично разделам по безопасности жизнедеятельности и экономике – давно назревшая необходимость. Кроме того, объединение усилий вуза в рамках единой кафедры ЭМС – совершенно естественный шаг в этом направлении. Наконец, включение специальности «Электромагнитная совместимость» в перечень инженерных специальностей Минобразования РФ стало бы мощным импульсом в этой работе. К сожалению, последнее, по-видимому, до сих пор затрудняется из-за междисциплинарного характера ЭМС. Между тем накопленный в мире объем знаний в этой области, его классификация и систематизация убедительно говорят об ЭМС как большом самостоятельном направлении.

## Литература


1. Газизов Т.Р. Автоматизированное проектирование бытовой радиоэлектронной аппаратуры с учетом электромагнитной совместимости // Мат-лы Всерос. науч.-практ. конф. «Интеграция учебного процесса и фундаментальных научных исследований в университетах: инновационные стратегии и технологии»: В 2 т. Т. 1 / Под ред. А.С. Ревушкина. Томск, 2000.
2. Газизов Т.Р. Неумышленные и преднамеренные электромагнитные помехи техническим объектам и людям // Мат-лы VI Всерос. науч.-практ. конф. «Проблемы информационной безопасности общества и личности». Томск, 22–24 мая 2002 г. Томск, 2002.
3. Gazizov T.R. EMC and safety: gaps in education // Proc. of the Int. Symp. on EMC. Sorrento, Italy, 9–13 Sept. 2002. № 2.
4. Газизов Т.Р. Информационная война и электромагнитный терроризм // Мат-лы межрегион. науч.-практ. конф. «Проблемы информационной безопасности общества и личности». Томск, 24–26 мая 2000 г. Томск, 2002.
5. Газизов Т.Р. Исследования проблемы электромагнитного терроризма // Мат-лы межрегион. науч.-практ. конф. «Проблемы информационной безопасности общества и личности». Томск, 6–8 июня 2001 г. Томск, 2001.
6. Loborev V.M. The modern research problems.– Plenary Lecture, AMEREM Conf. Albuquerque, NM, May 1996.
7. Gardner R.L. Electromagnetic terrorism. A real danger // Proc. of the 14th Int. Wroclaw Symp. on EMC.Wroclaw, Poland, 23–25 June 1998.
8. Workshop W4: Electromagnetic terrorism and adverse effects of high power electromagnetic (HPE) environments // Supplement to Proc. of the 13th Int. Zurich Symp. on EMC. Zurich, Switzerland, 16–18 Febr. 1999.
9. URSI resolution on «Criminal activities using electromagnetic tools» // The Radio Science Bull. № 290, Sept. 1999.
10. Radasky W.A. et al. Intentional electromagnetic interference (EMI) – Test data and implications // Proc. of the 14th Int. Zurich Symp. on EMC. Zurich, Switzerland, 20–22 Febr. 2001.
11. Электромагнитный терроризм на рубеже тысячелетий / Под ред. Т.Р. Газизова. Томск, 2002.
12. Special issue on high power electromagnetic (HPEM) disturbances and intentional EMI. – IEEE Trans. on Electromagn. Compat. V. 46. № 2, May 2004.
13. Барсуков В.С. Безопасность: технологии, средства, услуги. М., 2001.
14. Никифоров Н.В. Антитеррористические технологии обеспечения электромагнитной безопасности // Технологии электромагнитной совместимости. 2002. № 2.

15. Газизов Т.Р. Потенциальные угрозы электромагнитного терроризма критичным электронным системам // Мат-лы III науч.-практ. конф. «Современные средства и системы автоматизации – гарантия высокой эффективности производства». Томск, 14–15 нояб. 2002 г. Томск, 2003.
16. Газизов Т.Р. Оценка возможности угроз электромагнитного терроризма авионике // Тр. II Всерос. науч.-техн. конф. по проблемам создания перспективной авионики. Томск, 15–17 апр. 2003 г. Томск, 2003.
17. Газизов Т.Р. Вопросы разработки авионики, защищенной от электромагнитного терроризма // Там же.
18. Ianoz M., Wipf H. Modeling and simulation methods to assess EM terrorism effects // Supplement to Proc. of the 13th Int. Zurich Symp. on EMC. Zurich, Switzerland, 16–18 Febr. 1999.
19. Lo Vetri J. et al. Microwave Interaction With a Personal Computer: Experiment and Modeling // Ibid.
20. Seow T.S. et al. Microwave Testing of a Computer: a Representative Example of the Susceptibility of Commercial System // Digest of EUROEM2000, Edinburgh, Scotland, 30 May – 2 June 2000.
21. Zielinski R.J. Risk of Interference to Aircraft from VSAT, SNG and SIT Terminals // Proc. of the 15th Int. Wroclaw Symp. on EMC. Wroclaw, Poland, 27–30 June 2000.
22. Jakobus U. Application of numerical techniques based on the method of moments to the solution of a variety of real-world EMC problems // The Int. Journal for EMC. ITEM 2001.
23. Fortov V.E. et al. A computer code for estimating pulsed electromagnetic disturbances penetrating into building power and earthing circuits // Proc. of the 14th Int. Zurich Symp. on EMC. Zurich, Switzerland, 20–22 Febr. 2001.
24. Messier M.A. et al. Response of telecom protection to three IEC waveforms // Proc. of the 15th Int. Zurich Symp. on EMC. Zurich, Switzerland, 18–20 Febr. 2003.
25. Канащенков А.И. и др. Облик перспективных бортовых радиолокационных систем. Возможности и ограничения. М., 2002.
26. Debnath R., Karve V.W. A soft systems methodology-system dynamics (SSM-SD) based approach to re-engineering EMI/EMC regulations and standards to counter future terrorist threats // Proc. 15th Int. Wroclaw Symp. on EMC. 27–30 June 2000. Late Papers.
27. Степанов П.В. Методология предупреждения угроз информационной безопасности техническими средствами в телекоммуникационной инфраструктуре интеллектуального здания: Автореф. дис. ... д-ра техн. наук. М., 2001.
28. Кириллов В.Ю. Электромагнитная совместимость элементов и устройств бортовых систем летательных аппаратов при воздействии электростатических разрядов: Автореф. дис. ... д-ра техн. наук. М., 2002.