

Министерство образования и науки Российской Федерации

Томский государственный университет
систем управления и радиоэлектроники

Т.Р. Газизов, А.М. Заболоцкий, С.П. Куксенко

**Электромагнитная совместимость:
преднамеренные силовые
электромагнитные воздействия**

Учебное пособие

Томск

Издательство ТУСУРа

2018

УДК 621.391.823:621.396.6(075.8)

ББК 323.811.7я73

Г137

Рецензенты:

Гизатуллин З.М., д-р техн. наук, профессор Казанского национального исследовательского технического университета им. А.Н. Туполева-КАИ;
Шкоркин В.В., канд. техн. наук, нач. сектора АО «НПЦ «Полюс»

**Издание осуществлено при финансовой поддержке
Министерства образования и науки Российской Федерации
(проект № 8.9562.2017/8.9)**

Газизов, Тальгат Рашитович

Г137 Электромагнитная совместимость: преднамеренные силовые электромагнитные воздействия : учеб. пособие / Т.Р. Газизов, А.М. Заболоцкий, С.П. Куксенко. – Томск: Изд-во Томск. гос. ун-та систем упр. и радиоэлектроники, 2018. – 114 с.

ISBN 978-5-86889-794-8

Рассматривается актуальная в обеспечении электромагнитной совместимости проблема уменьшения преднамеренных электромагнитных помех (ПЭМП), под которыми понимают преднамеренное оказание в преступных или террористических целях мощного электромагнитного воздействия на электронные и электрические системы, нарушающего их функционирование. Представлен анализ имеющихся за рубежом теоретических и экспериментальных результатов, связанных с разработкой и использованием генераторов ПЭМП, методов и средств защиты от их деструктивного воздействия элементов электронной инфраструктуры объектов.

Для студентов, магистрантов и аспирантов, специализирующихся в области электромагнитной совместимости.

УДК 621.391.823:621.396.6(075.8)

ББК 323.811.7я73

ISBN 978-5-86889-794-8

© Газизов Т.Р., Заболоцкий А.М.,
Куксенко С.П., 2018

© Томск. гос. ун-т систем упр.
и радиоэлектроники, 2018

Введение

Радиоэлектронная аппаратура (РЭА) все больше используется в самых различных сферах инфраструктуры современного общества. Увеличение количества РЭА, часто работающей в ограниченном пространстве, приводит к росту ее плотности. Неуклонное повышение производительности РЭА во многом обеспечивается за счет увеличения верхней частоты спектра используемых сигналов.

Эти тенденции стали все чаще приводить к нарушению работы РЭА из-за взаимных электромагнитных помех, что обусловило необходимость обеспечения электромагнитной совместимости (ЭМС), способности удовлетворительно работать и не мешать работе других устройств в заданной электромагнитной обстановке. Отметим, что обеспечение ЭМС стало самостоятельным направлением в современной радиоэлектронике.

Весьма актуальна в решении задач ЭМС проблема уменьшения преднамеренных электромагнитных помех (ПЭМП)¹, под которыми по определению, принятому в международной литературе, понимают преднамеренное оказание в преступных или террористических целях мощного электромагнитного воздействия на электронные и электрические системы, нарушающего их функционирование. Предпосылками возникновения этой угрозы стали, с одной стороны, достижения в создании мощных источников электромагнитного поля, а с другой – неуклонное уменьшение уровней сигналов электронных систем. Все более широкое внедрение электронных систем в жизнь общества, приведшее к сильной зависимости от них, а также доступность устройств для

¹ Примерно для того же применяют термины: электромагнитный терроризм – В.М. Лоборев; силовое деструктивное воздействие (СДВ) – В.С. Барсуков; намеренное силовое воздействие (НСВ) – С.А. Сухоруков; функциональное поражение (ФП) – военные направления; преднамеренное силовое электромагнитное воздействие (ПДЭМВ) – ГОСТ Р 52863-2007. Видимо, правильнее использовать именно термин ПДЭМВ, но пока в России не регламентирован общий термин, здесь и далее используется термин ПЭМП, широко применяющийся ранее (дословный перевод с общепринятого Международной электротехнической комиссией и в англоязычной литературе термина Intentional Electromagnetic Interference (IEMI)). К сожалению, он не очень удачен, поскольку полностью совпадает с термином ПЭМП, широко применяемым в русскоязычной литературе по радиоэлектронной борьбе.

создания помех сделали эту угрозу реальностью. Проблема ПЭМП является новой, поэтому она еще далека от своего решения. Между тем в мире активно ведутся связанные с ней исследования.

Цель работы – представить в едином учебном пособии анализ имеющихся за рубежом теоретических и экспериментальных результатов, связанных с разработкой и использованием генераторов ПЭМП, методов и средств защиты от их деструктивного воздействия, обеспечения устойчивости к ПЭМП элементов электронной инфраструктуры объектов.

Учебное пособие предназначено для студентов, магистрантов и аспирантов, специализирующихся на электромагнитной совместимости РЭА. Отзывы можно направить по адресу talqat@tu.tusur.ru.

1. Хронология исследований

Открытое обсуждение проблемы ПЭМП началось с пленарной лекции профессора В. Лоборева на конференции АмерЭМ в 1996 г. [1]. На цюрихском симпозиуме по ЭМС в 1997 г. Комиссия E URSI при своем Комитете по ЭМ импульсу и связанными с ним явлениями, возглавляемом М. Уиком, образовала подкомитет по ЭМ терроризму под руководством Х. Уипфа. Первый обзор этой проблемы опубликован в пленарном докладе Р. Гарднера на вроцлавском симпозиуме по ЭМС 1998 г. [2]. Первый семинар «ЭМ терроризм и вредные воздействия ЭМ окружений высокой мощности» с публикацией полных докладов состоялся на Цюрихском симпозиуме по ЭМС 1999 г. [3]. Необходимо отметить, что были представлены и важные неопубликованные доклады. В частности, доклад вице-президента РАН академика В.Е. Фортова содержал много фотографий и технических характеристик готовых ЭМ устройств высокой мощности. Доклад заканчивался убедительным выводом (подчеркнутым М. Уиком при закрытии семинара), что для решения проблемы ЭМ терроризма необходимо международное сотрудничество.

Важной вехой стала резолюция Совета URSI по преступной деятельности с помощью ЭМ средств [4]. В 2000 г. «Угроза ЭМ терроризма» впервые стала отдельным разделом в списке тем Вроцлавского симпозиума по ЭМС. В 2001 г. была организована первая отдельная секция с рецензируемыми статьями Цюрихского симпозиума по ЭМС [5]. Затем доклады, связанные с ПЭМП, стали появляться на каждом симпозиуме по ЭМС и некоторых других конференциях.

Из отечественных публикаций нельзя не отметить раздел по ПЭМП «Технологии защиты систем безопасности от электромагнитного терроризма» в [6]. Первая, целиком посвященная этой проблеме книга – коллективная монография [7] – также появилась в России. Отдельная секция по ПЭМП работала на международном симпозиуме по ЭМС 2003 г. в Турции.

Важной вехой в исследованиях ПЭМП стала публикация в 2004 г. тематического выпуска IEEE Transactions on EMC [8].

Специальная секция по ПЭМП, в первом докладе которой было кратко представлено состояние дел по этой проблеме [9], состоялась на Цюрихском симпозиуме 2006 г. в Сингапуре. Наконец, на Цюрихском симпозиуме по ЭМС 2007 г. в Мюнхене впервые был представлен вводный курс по ПЭМП (Tutorial on Intentional IEMI) (рис. 1.1).

Таким образом, накопилось уже довольно много научных исследований по этой проблеме, чтобы можно было знакомить с ее основами широкий круг специалистов, проявляющих большой интерес к решению задач защиты РЭА от преднамеренных силовых электромагнитных воздействий.

TUT-2 on Monday September 24

Tutorial on Intentional EMI (IEMI)

Dr. William Radasky, Metatech Corporation (wradasky@aol.com)

13:00 – 13:40

Dr. William Radasky, Metatech Corporation, USA*

Richard Hoad, QinetiQ, UK

Introduction to Intentional Electromagnetic Interference (IEMI)

What is the definition of IEMI and what types of threat sources and situations produce IEMI?

13:40 – 15:00

Richard Hoad, QinetiQ, UK*

Dr. William Radasky, Metatech Corporation, USA

The Effect of IEMI on Equipment and Systems

Summary of test results for electronic equipment and systems when exposed to waveforms and levels that can be produced by existing threat sources.

15:00 – 15:30

Break

15:30 – 15:50

Dr. William Radasky, Metatech Corporation, USA*

Richard Hoad, QinetiQ, UK

Mitigation Concepts and Approaches for IEMI

Review of the different types of mitigation methods, including those designed to reduce the level of EM fields and voltages.

15:50 – 16:30

Richard Hoad, QinetiQ, UK*

Dr. William Radasky, Metatech Corporation, USA

Standardisation Activities in the IEC

Update of the work of the IEC to standardize the types of HPEM environments, test methods and protection methods.

16:30 – 17:00

Questions and Discussion

*Presenting author

Рис. 1.1. Программа вводного курса по ПЭМП
(EMC Zurich, Munchen, 2007)

2. Актуальность исследований

В инфраструктуре нашего общества существуют разные критичные системы, влияние ПЭМП на которые может привести к большим потерям. Одной из самых критичных является авиационная электроника, часто называемая авионикой. Поэтому стандарты, связанные с ее восприимчивостью к ЭМ помехам, становятся с годами все более строгими (табл. 2.1) [10].

Таблица 2.1
Уровни уязвимости (стандарты) в авиации

Год	Гражданские	Военные (Великобритания)	Военные (США)
1967	3,7 мВ/м, 1 ГГц	0,82 В/м, 1 ГГц	–
1968	–	–	1 В/м, 10 ГГц
1971	–	–	5 В/м, 10 ГГц 20 В/м, 40 ГГц
1980	0,1 В/м, 1 ГГц	5 В/м, 10 ГГц, период. 20 В/м, 18 ГГц модулир. 100 В/м вплоть до 200 В/м	–
1984	1 В/м, 1,215 ГГц	–	–
1986	–	–	20 В/м, 40 ГГц до 200 В/м
1989	200 В/м, 18 ГГц	–	–
1992	6,8 кВ/м, 18 ГГц	–	–

Из последующих изменений стандартов примечательны следующие. Изменение № 1 к стандарту RTCA/DO-160D от 14 декабря 2000 г. пересмотрело раздел 20 «Восприимчивость к радиочастотам» и потребовало испытаний в частотном диапазоне до 18 ГГц вплоть до 7200 В/м (рис. 2.1) [11]. Изменение 3 от 5 декабря 2002 г. добавило испытания периодическими пачками импульсов [12].

Показателен рост уровней восприимчивости, устанавливаемый военными стандартами (которые используются в авионике).

Например, со времени создания MIL-STD-461 уровни восприимчивости к излучаемым эмиссиям возросли на 46 дБ при росте на 32 дБ с выходом MIL-STD-461C. Отражая реалии жизни, каждый пересмотр MIL-STD-461 увеличивал уровни восприимчивости к излучаемым эмиссиям, уменьшая уровни излучаемых эмиссий (рис. 2.2) [13].

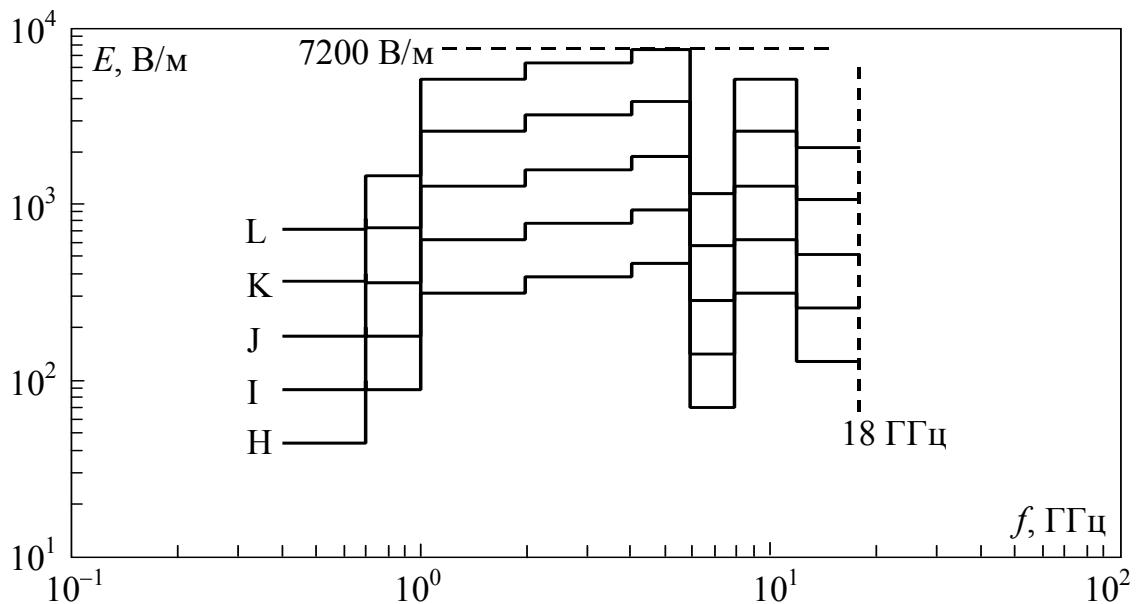


Рис. 2.1. Испытательные уровни (для радиочастотного импульса) и категории восприимчивости к излучениям

Тем не менее в этой области существуют проблемы, являющиеся возможными причинами авиакатастроф. Например, несмотря на строгие требования, многие старые самолеты, соответствующие требованиям стандарта EUROCAE ED-14B 1984 г. (максимальный уровень напряженности поля 1 В/м в полосе частот до 1,215 ГГц), продолжают летать сегодня, поскольку имеют срок нормативной эксплуатации 20–30 лет [10]. Высокая актуальность указанных проблем подтверждается исследованиями в этой области: как национальными (например, программа Германии (BWB) из двух фаз (1995–2000, 2001–2005) по оценке угроз микроволн высокой мощности бортовой аппаратуре [14]), так и международными (например, Европейский проект EM-HAZ «Методы и технологии для безопасности и защиты летательных аппаратов от электромагнитных угроз» [15]).

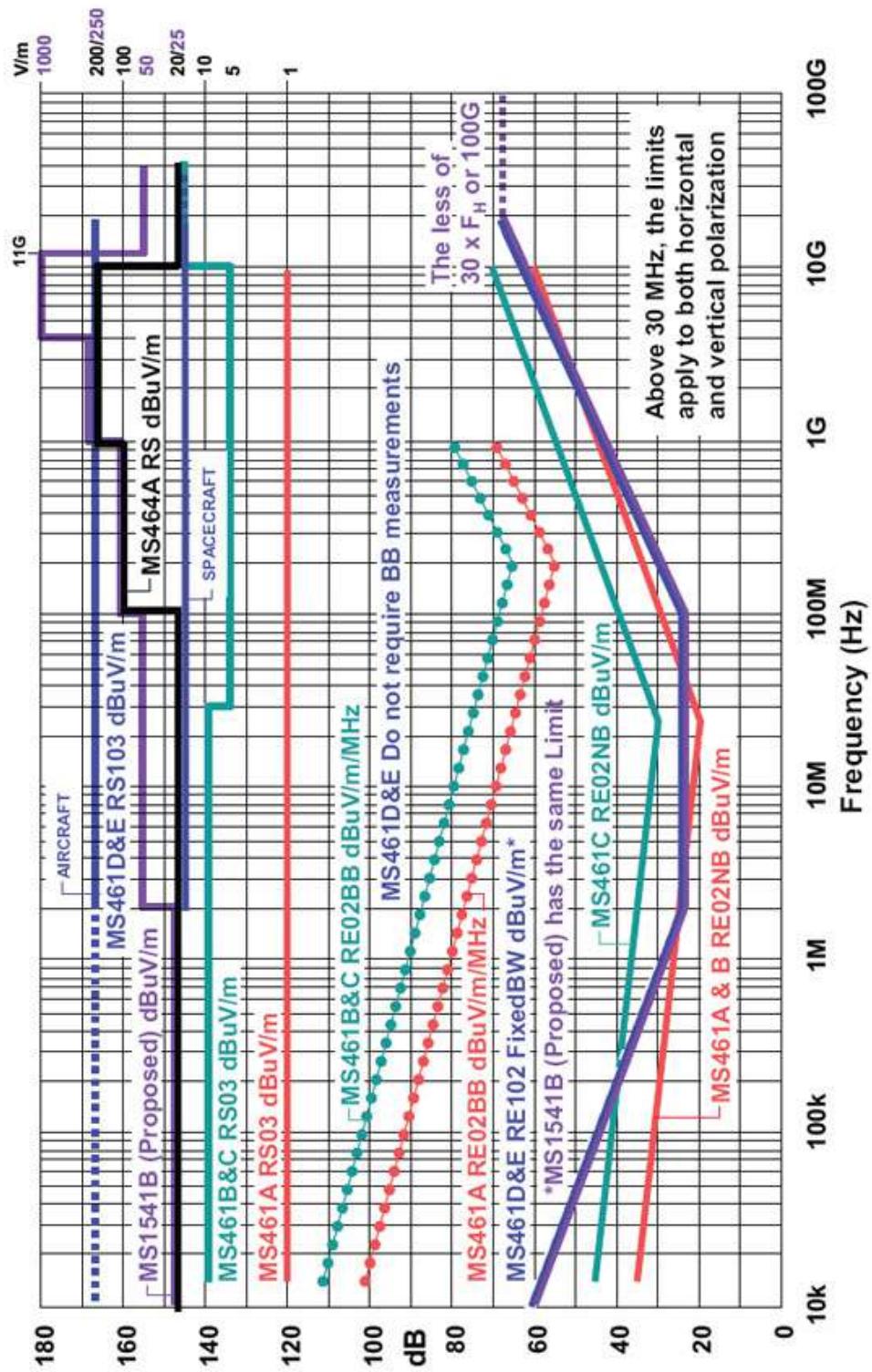


Рис. 2.2. Сравнение уровней стандартов MIL-STD-461A, B, C; 461D, E; 464A; 1541B

Сделаны весьма многозначительные выводы даже для военной авионики. Например, согласно заключению авторитетных производителей бортовых радаров в России [16], существующие бортовые радиолокационные системы практически беззащитны к воздействию мощного короткоимпульсного СВЧ-излучения.

Другим аспектом в свете чрезвычайно актуальной и нерешенной проблемы терроризма может стать электромагнитный 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 всё более трудной задачей» [17].

Яркой иллюстрацией актуальности подобных исследований и пристального к ним внимания является диссертация французского ученого Палетта, титульный лист которой показан на рис. 2.3,*a*. Прежде всего обращает на себя внимание список оппонентов, включающий, пожалуй, самых известных сегодня в ЭМС-сообществе ученых: Канаверо (главный редактор IEEE Transactions on EMC), Яноз (организатор многих симпозиумов по ЭМС, соавтор известной монографии по ЭМС), Баум (личность, ставшая легендарной в области ЭМС). Весьма примечательна и тематика работы: она посвящена исследованию влияния внешнего электромагнитного поля на бортовую кабельную разводку самолета, т.е. одно из наиболее опасных из всех возможных проявлений проблемы ПЭМП. Впечатляют и значительные средства, вкладываемые в такие исследования: работа выполнялась в рамках совместного проекта Франции и США, а сложнейшее экспериментальное моделирование осуществлялось на самолете типа «Боинг» (рис. 2.3,*b,в*).

В международных организациях ведется активная работа по проблеме ПЭМП. Как уже отмечалось, URSI инициировал эту деятельность, а МЭК организовала активную работу по созданию ряда новых стандартов, связанных с ПЭМП. Эта работа идет по обычной схеме координации МЭК и ее подкомитетов с другими организациями (рис. 2.4 [18]).

THESE DE DOCTORAT
DE L'UNIVERSITE PARIS XI - ORSAY

Specialite : Electronique

Presentee par

Laurent PALETTA

Pour obtenir le grade de

DOCTEUR EN SCIENCES DE L'UNIVERSITE PARIS XI ORSAY
DEMARCHE TOPOLOGIQUE POUR L'ETUDE DES
COUPLAGES ELECTROMAGNETIQUES SUR DES SYSTEMES DE CABLAGES
INDUSTRIELS DE GRANDE DIMENSION

Soutenue publiquement le 28 Septembre 1998
devant le Jury suivant

President	M. Jean-Charles Bolomey	Professeur, UFR Sciences d'Orsay -
Supelec		
Rapporteurs	M. Flavio Canavero	Professeur, Ecole Polytechnique de
Turin		
	M. Michel Ianoz	Professeur, Ecole Polytechnique de
Lausanne		
Directeur de these	M. Jean-Philippe Parmantier	Ingenieur, ONERA
Examinateurs	M. Carl Edward Baum	Senior Scientist, Air Force Research
Lab.		
	M. Philippe Dumas	Ingenieur de Recherche, RENAULT

a



Figure IV-31 : Avion EMPTAC en dessous du simulateur Ellipticus (Kirtland - Air Force Base - Nouveau Mexique)

b

Рис. 2.3. Диссертация Палетта: *a* – титульный лист;

b – испытательный самолет

(начало, окончание см. на с. 12)

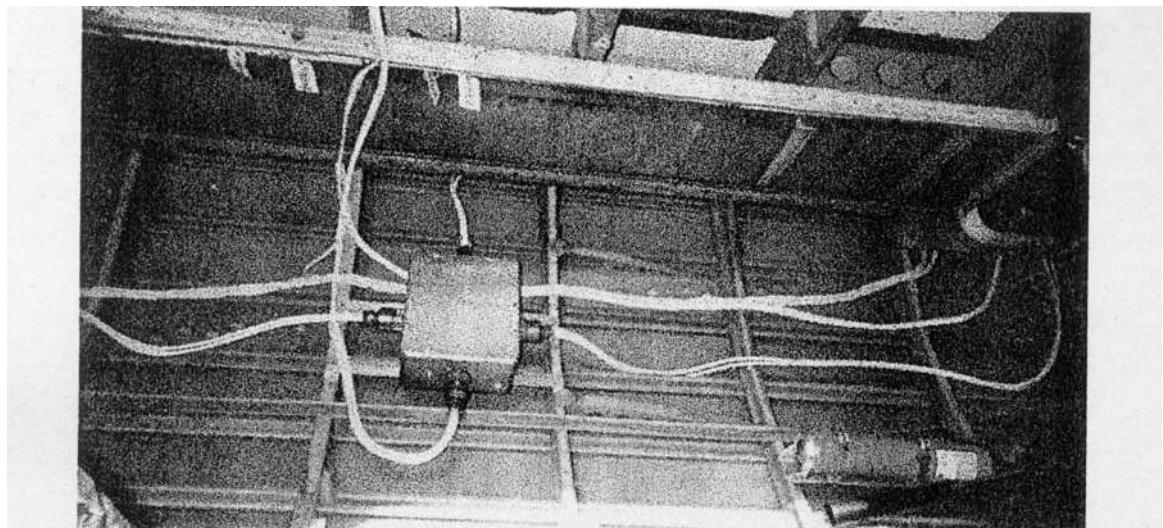


Figure III-32 : Câblage non blindé installé dans la soute avant faradisée de l'avion EMPTAC

6

Рис. 2.3. Диссертация Палетта: 6 – фрагмент кабельной разводки
(окончание, начало см. на с. 11)

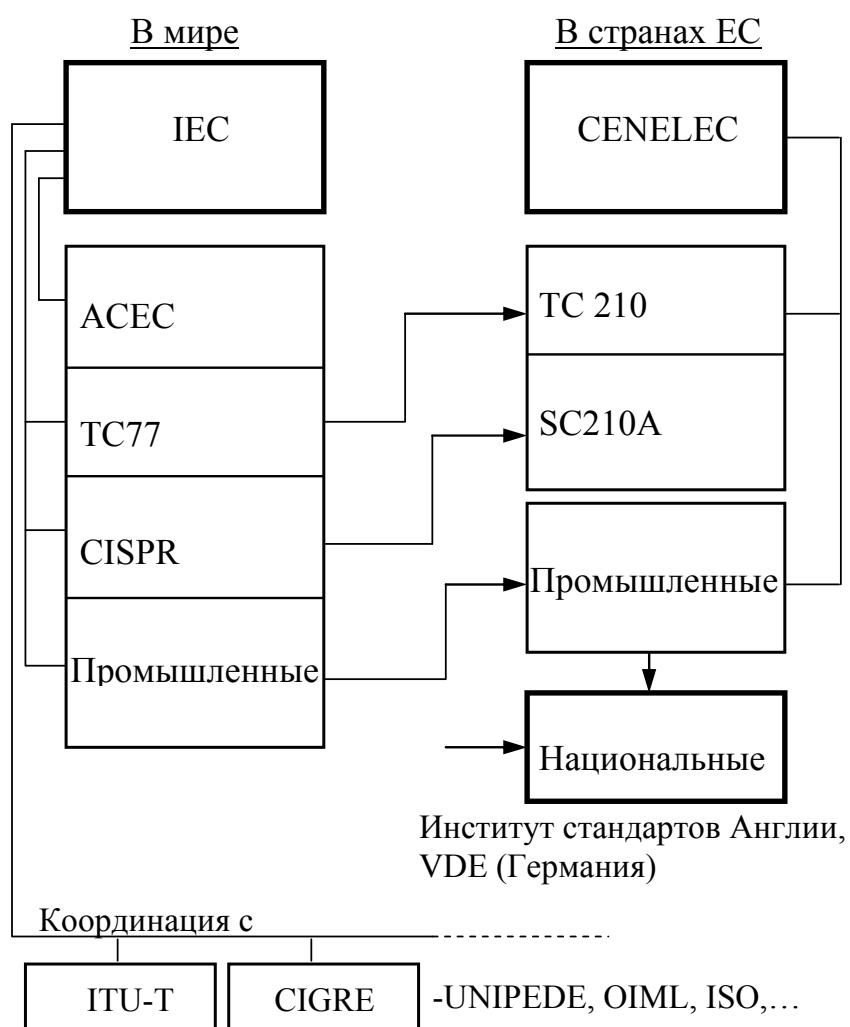


Рис. 2.4. Организация международной деятельности
в области стандартов по ЭМС

Доклады о состоянии работ по стандартизации в области ПЭМП регулярно делают на симпозиумах по ЭМС Мануэль Уик и Уильям Радаски, председатель ТК77 в МЭК (например, [19]).

Специфика проблемы ПЭМП заставляет пересматривать, казалось бы, давно установленные понятия. Так, стандартом IEC 61000-2-13 [20] введена новая процедура определения спектра сигнала по 90 % энергии между двумя частотами: нижней и верхней. Для однозначности определения эта процедура требует выбирать минимальное значение отношения этих частот, называемое отношением полосы (band-ratio). На рис. 2.5 проиллюстрирован пример определения нижней и верхней частот, а также показана ширина полосы, которая была бы определена, как это принято в связи ($f_3 - f_1$), что явно не учитет многие из важных более высоких частот, которые могут иметь существенное влияние на восприимчивость электронного оборудования.

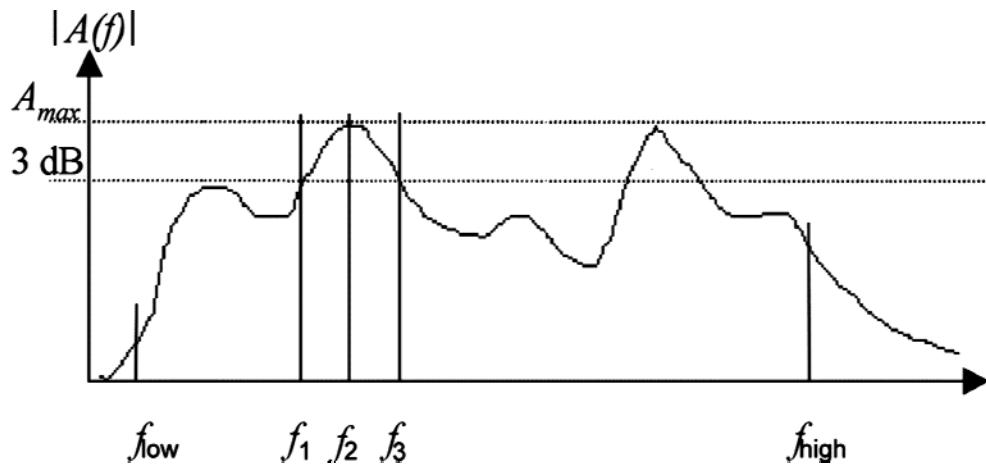


Рис. 2.5. Сигнал с многочисленными пиками интенсивности спектра

Установлены три «широкополосных» категории: мезополосная (средняя полоса), субгиперполосная и гиперполосная (табл. 2.2) [20].

Поскольку нарушение работы оборудования из-за электромагнитных воздействий может оказывать влияние на безопасность человека, то разрабатываются соответствующие стандарты и в этой сфере [21]. Например, актуальная проблема безопасности и ЭМС обсуждалась на семинаре IEEE в 2006 г. [22].

Таблица 2.2
Определения для классификации ширины полосы

Категория полосы	Процентная ширина полосы (pbw)	Отношение полосы (br)
Узкополосная	$\leq 1 \%$	$br \leq 1,01$
Мезополосная	$1 \% < pbw \leq 100 \%$	$1,01 < br \leq 3$
Субгиперполосная	$100 \% < pbw \leq 163,4 \%$	$3 < br \leq 10$
Гиперполосная	$163,4 \% < pbw \leq 200 \%$	$br > 10$

Для защиты от ПЭМП полезны непрерывно совершенствующиеся военные стандарты. Так, в [23] предложен новый подход к распределению требований стандарта MIL-STD-464 для функционирования авиационных систем при разряде молнии через фюзеляж самолета. Вопросы стандартизации, прямо или косвенно касающиеся ПЭМП, затрагиваются во многих работах.

3. Источники электромагнитного излучения

Согласно обобщенным данным на 1998 г. [24]) узкополосные источники электромагнитного излучения способны генерировать в антенне в полосе частот 0,5–10 ГГц пиковую мощность 0,1–20 ГВт, создавая на расстоянии 100 м электрические поля 20–300 кВ/м. Аналогичные характеристики для широкополосных (0,1–50 ГГц) источников составляют 2–20 ГВт и 4–20 кВ/м.

Что касается узкополосной генерации, например, от виркаторов получена мощность 0,17–40 ГВт в сантиметровом и дециметровом диапазонах [6], а мощность современных релятивистских генераторов оценивается в 20–80 ГВт [25]. Для генерации широкополосных импульсов разработаны различные технологии: от гигантского одиночного импульса контролируемого взрыва до большого числа импульсов с высокой частотой повторения. В частности, для одиночного импульса взрывомагнитных генераторов достигнута генерация тока в десятки мегаампер и пиковой мощности в десятки тераватт [6]. На основе разряда в газе высокого давления возможна генерация миллиона импульсов с частотой повторения в несколько килогерц при напряжении более 5 МВ и мощности в сотни гигаватт в наносекундном диапазоне. Для кремниевых приборов, основанных на эффектах сверхбыстрого восстановления напряжения и обратимого пробоя, достигнуты напряжения до 100 кВ при времени фронта импульса менее 1 нс (пиковая мощность до 100 МВт) и до 20 кВ при 100 пс (более 10 МВт). Благодаря таким особенностям этих приборов, как дешевизна, почти неограниченный ресурс и высокая стабильность, стала возможной разработка простых и компактных генераторов импульсов пиковой мощностью в сотни киловатт с частотой повторения вплоть до нескольких мегагерц. Чрезвычайно малый джиттер этих импульсов позволяет суммировать мощность большого числа генераторов [26].

Пример информационного оружия (дальность поражения 800 м в секторе 24°) – микроволновой генератор пиковой мощностью около 1 ГВт (265 кВ; 3,5 кА) с зеркальной антенной диамет-

ром 3 м. Другой пример – фазированная антенная решётка из 144 твердотельных излучателей импульсов длительностью менее 1 нс, имеющая общую мощность 1 ГВт и работающая на несколько целей [6]. Генератор импульсов (± 200 кВ; 3,5 нс; 100 Гц) импульсной мощностью 3,2 ГВт способен работать в течение 20 мин с перерывами 1,5 ч, создавая 1,3 ГВт импульсного поля вертикальной поляризации [27]. Новая антенна для решеток, управляемых подобным генератором, излучает мощные и более короткие (менее 1 нс) импульсы [28].

Для малогабаритных переносных источников ПЭМП характеристики и в конечном счете цена определяются возможностями источника, запасающего энергию. Кейс из электролитических конденсаторов, запасающих $2 \text{ МДж}/\text{м}^3$ энергии, стоимостью \$10000–\$15000 может вывести из строя до 20 компьютеров, а установка на ионисторах ($10 \text{ МДж}/\text{м}^3$, \$50000) может быть достаточной для вывода из строя всех компьютеров большого вычислительного центра [6]. Наконец, электромагнитную бомбу в кейсе с дальностью действия 500 м можно купить по Интернету за \$100000 [29]. Что касается возможных размеров, то генератор, например на 50 кВ и 2 кДж, может весить менее 50 кг [30].

В [31] сообщается о возможностях (для создания надежных, компактных переносных систем высокой мощности) значительного улучшения характеристик электронных приборов с поперечным полем (tapered MILO), полученных ранее: КПД 15 % на частоте 1 ГГц, 2 ГВт радиочастотной мощности, 250 Дж на импульс при источнике 500 кВт .

Приведём характеристики уже работающих систем. Так, весьма показательна оценка напряженности ЭМ поля, созданного подвижной станцией спутниковой связи SNG (рис. 3.1) [10]. Из нее следует, что пролетающий в луче самолет будет около 0,15 с находиться в поле 42 В/м, а это может быть одного порядка с уровнями уязвимости оборудования.

В 1997–1999 гг. в Исследовательской лаборатории BBC США разработана система (с импульсной излучающей полуантенной) для излучения импульсов длительностью (по уровням 0,5) 100 пс, мощностью 1 МВт, с частотой повторения 600 Гц и показателем поля на расстоянии 5,3 МВ [32].

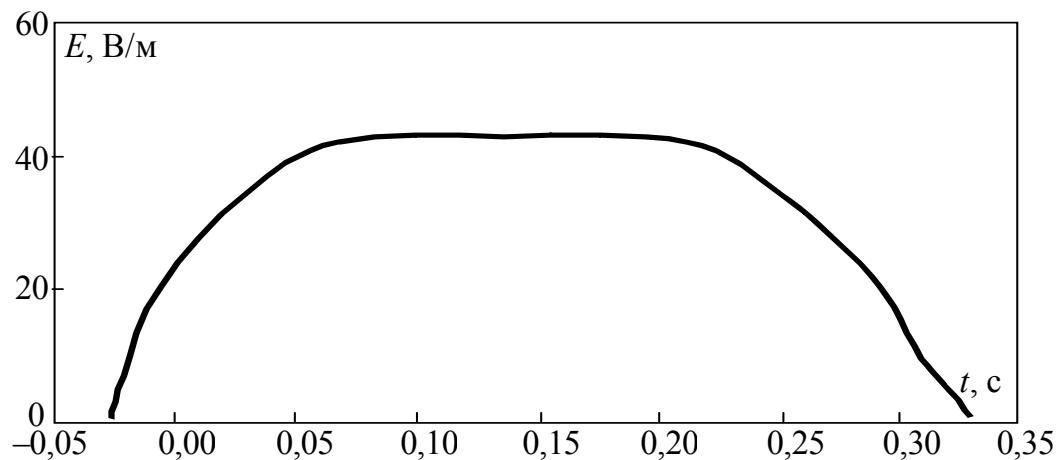


Рис. 3.1. Моделирование поля на высоте 300 м, создаваемого пролетающему самолету станцией SNG при угле высоты луча 30 градусов

О преодолении ограничения, налагаемого пробоем, за счет оптимизации формы и длительности импульса, а также параметров каждого излучателя и включения их в решетку (рис. 3.2) сообщается в [33].

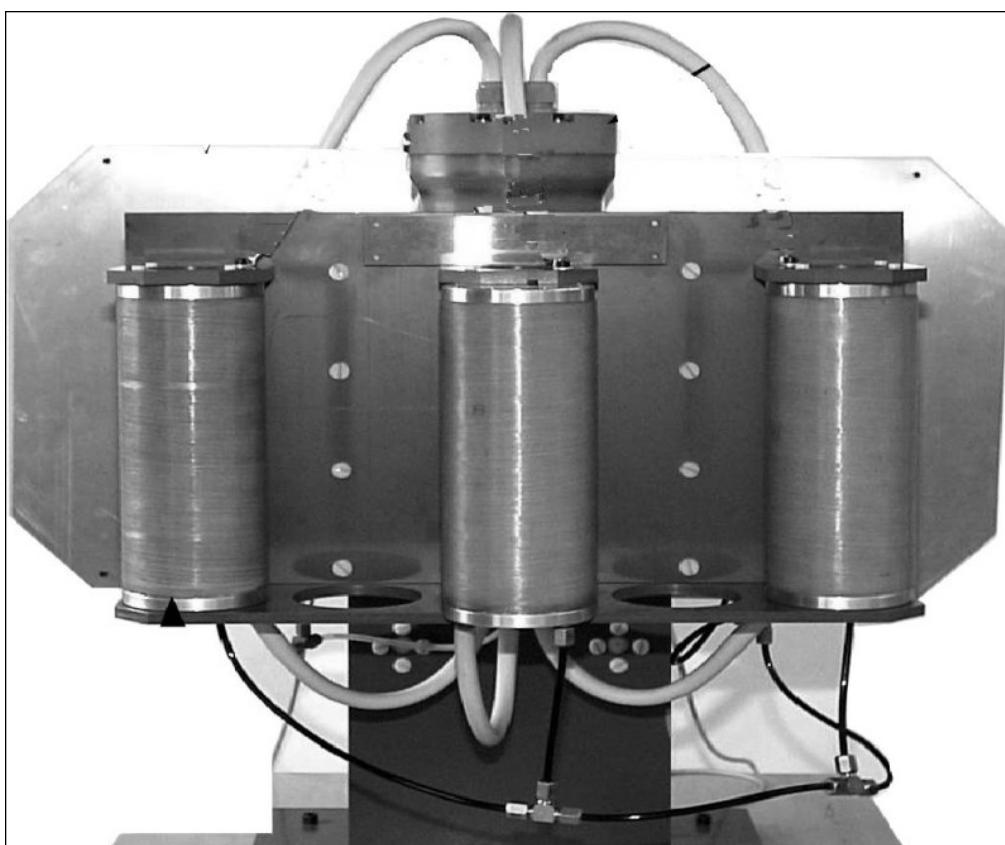


Рис. 3.2. Оптимизированная по размеру решетка источников (DIEHL Munitionssysteme)

Компактные, надежные радиочастотные источники высокой мощности, разрабатываемые в Германии (DIEHL) для потенциального применения в качестве радиочастотного оружия и нацеленные на доведение до коммерческих образцов, описаны в [34]. В состав типовых проектов входит DS350, мощный лабораторный источник для испытаний на электромагнитные воздействия, серия компактных источников DS110 и сверхширокополосные глушилки с ультравысокой частотой повторения. Системы DS110A с решеткой предназначены для применений на более дальние расстояния, где использование радиочастотных источников с одной антенной ограничено атмосферным пробоем в области антенны. DS350 показал способность создавать поле напряженностью более 300 кВ/м на расстоянии 1 м, работая на частотах 50–100 МГц. На частоте 50 МГц получена излучаемая импульсная энергия 30 Дж. Эта система не была оптимизирована для компактности, а представляет собой надежную модульную лабораторную испытательную систему. К ней удобно подключать разные антенны, что обеспечивает максимальную гибкость как в испытаниях на воздействие, так и в разработке антенн. Имеется серия компактных источников DS110, встроенных в портфель, или цилиндрической геометрии. Измерения излучаемого поля показывают возможность получения напряженностей 100–160 кВ/м на расстоянии 1 м в виде затухающей синусоиды частотой 350 МГц примерной длительностью 6 нс. Простым добавлением рефлектора было получено пиковое излучаемое поле, нормированное к 1 м, напряженностью более 300 кВ/м.

Для испытательных целей представляет интерес DS110B, источник с перестройкой частоты в диапазоне 100–300 МГц. Испытана и его новая, длинноимпульсная версия DS110B-LP, специально предназначенная для испытательных применений с различными антennами для оптимизации воздействия на цели. Глушитель с высокой частотой повторения HRR-8G – последний в серии источников, способных эффективно подавлять сигналы связи в диапазоне 20–500 МГц, используя сверхширокополосные импульсы с частотой повторения более 1 МГц. Мощная решетка из трех антенн DS110A3 показала стабильные импульсы поля, нормированного к 1 м, напряженностью более 600 кВ/м. К досто-

инствам этой системы относится не только более высокая напряженность поля, но также улучшенная направленность на цели, которая предотвращает излучение в нежелательных направлениях. Ведется разработка систем с 6 и более антеннами для получения еще более высоких напряженностей. DS110A3 встроена в небольшой трейлер, чтобы разыгрывать сценарии с подвижным радиочастотным оружием. (Можно предположить, что именно эта решетка показана на рис. 3.2.)

В [35] сообщается о разработке компактной электромагнитной системы для прекращения движения транспортных средств, состоящей из подвижного перестраиваемого мощного источника и направленной антенны. Она способна генерировать энергию, достаточную для отключения или повреждения модуля управления или микропроцессора транспортного средства. Примечательно использование поиска «уязвимых частот», состоящего из систематического исследования откликов микропроцессора в широком диапазоне частот (300–2000 МГц) посредством двух различных тестовых режимов: непрерывной волны и широкополосного измерения, применяя 46-сантиметровую импульсную излучающую антенну.

В [36] описан действенный способ преодоления ослабления поля расстоянием. Как известно, чтобы иметь большую напряженность поля около цели, используют различные типы микроволнового оружия: прямое оружие, электромагнитное излучение которого проходит через атмосферу, и непрямое оружие, когда источник электромагнитного излучения выстреливается к цели и происходит эмиссия излучения в ближнем окружении цели. Во втором варианте электромагнитная энергия не поглощается в атмосфере, поэтому уровни излучения у цели могут быть максимизированы. Оригинальной системой является парашют из проводящего материала, который действует как антенна рефлекторного типа, в комбинации с электромагнитным источником для эмиссии коротких импульсов. Система таких парашютов может быть сброшена над целевой территорией и воздействовать на все системы в пределах их дальности действия. В этой же работе приводится диаграмма направленности парашютной антенны (рис. 3.3), а в [37] сообщается о разработке импульсной излу-

чающей 2-метровой тканной антенны, интегрированной в стандартный парашют и встроенной в 150-миллиметровый артиллерийский снаряд (рис. 3.4).

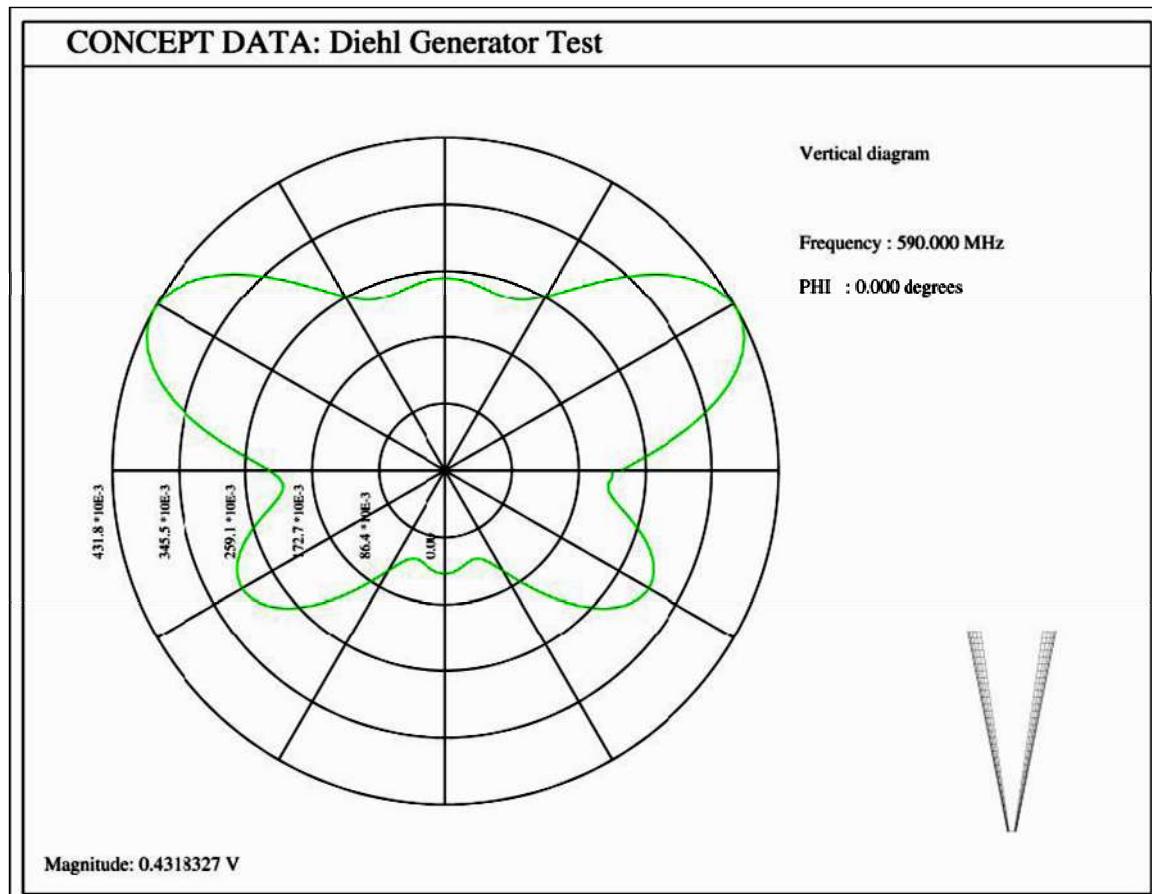


Рис. 3.3. Диаграмма направленности парашютной антенны



Рис. 3.4. Испытательная установка (*a*) для парашютной импульсной излучающей антенны (*b*)

В [38] представлен образец сверхширокополосной рупорной антенны с линзой (рис. 3.5), которая позволяет излучать чистый импульс со значительно меньшими, чем у рефлекторной импульсной излучающей антенны, боковыми лепестками. Более того, усиление этой антенны с 30-сантиметровой линзой оказалось больше, чем у 46-сантиметровой импульсной излучающей антенны.

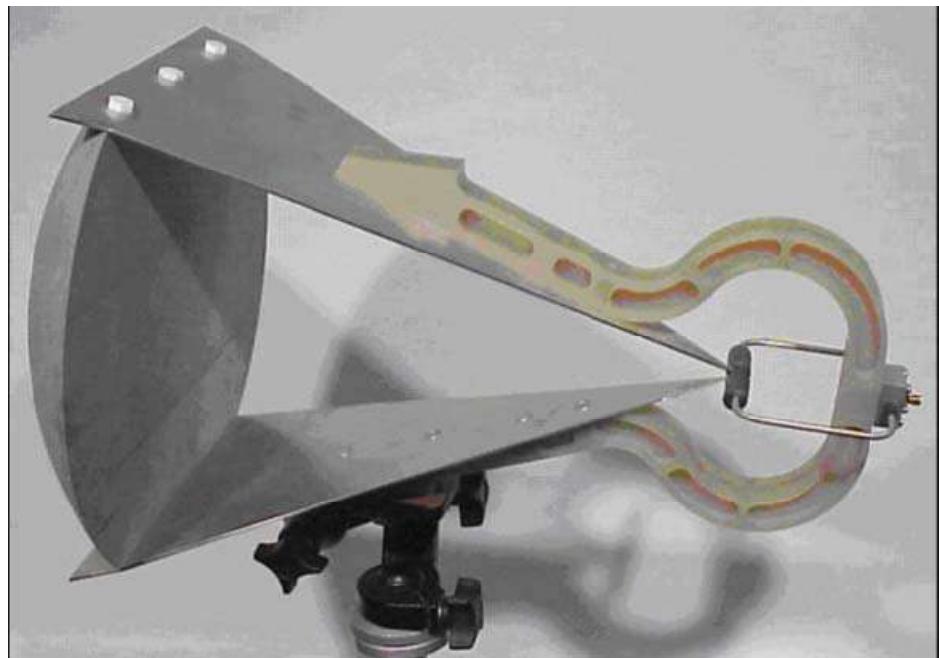


Рис. 3.5. Образец сверхширокополосного линзового ТЕМ-рупора

В [39] на основании проведенных экспериментов утверждается, что для нанесения максимального повреждения с минимальными затратами должно использоваться импульсное, а не непрерывное воздействие в области микроволновых частот. Сообщается также, что, исходя из этого вывода, была построена самая быстрая для своего времени испытательная установка с временем фронта 100 пс и уровнями поля 100 кВ/м, а позже была создана установка с временем фронта 10 пс и уровнями поля 1000 кВ/м.

В [40] сообщается о генераторе, способном выдавать мощность 100 МВт в наносекундных импульсах с фронтами порядка 200 пс. Такие устройства имеют компактную прямую геометрию и коммутируются лавинным GaAs фотопроводящим полупроводниковым ключом, который срабатывает от решетки маломощных

лазерных диодов. Однако при высоких напряженностях ключи на GaAs обладают небольшим числом срабатываний (менее 105), что привело к использованию в них карбида кремния (SiC) как отличного кандидата для высокочастотных электронных приборов высокой мощности, которые работают в среде с высокой температурой и сильным излучением (рис. 3.6) [41].

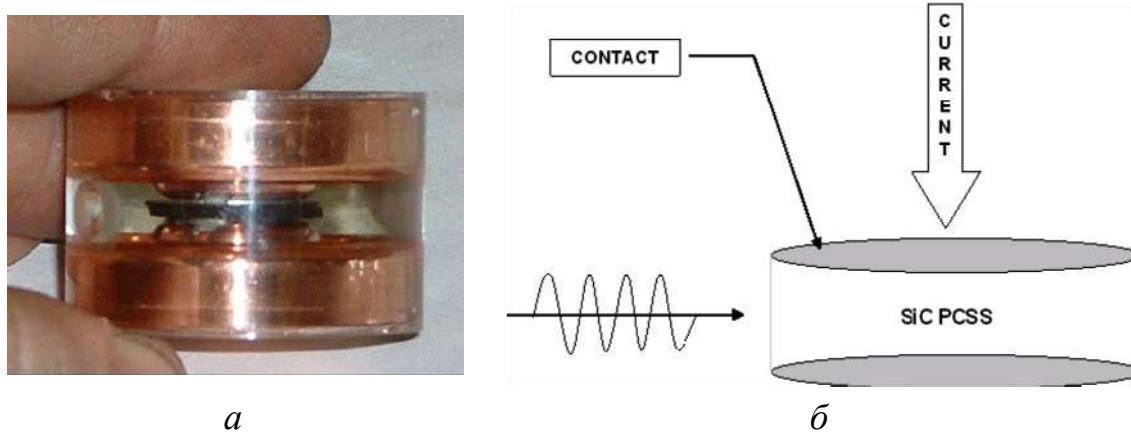


Рис. 3.6. Корпус фотопроводящего ключа на карбиде кремния (SiC)
для применений с высоким уровнем поля (а)
и иллюстрация процесса проводимости в нем (б)

Соответствие типов генераторов полосам частот выглядит следующим образом [9]. Узкополосная категория покрывается главным образом симуляторами микроволн высокой мощности. Они довольно велики по размеру, и их источники энергии обычно размещаются в больших трейлерах. Они способны генерировать поля пиковыми уровнями более 10 кВ/м в импульсах длительностью в микросекунду на расстоянии в десятки метров. Мезополосные генераторы вырабатывают сигналы наподобие затухающих синусоид, которые можно согласовать с резонансами кабелей оборудования. Эти импульсы не требуют большой энергии в частотном диапазоне выше 500 МГц, поэтому их источник энергии может быть достаточно небольшим. Наилучший пример источника этого типа – источник импульсов в портфеле, разработанный Diehl Systems в Германии и продемонстрированный на конференции EUROEM летом 2004 г. в Магдебурге. Он способен вырабатывать пиковый импульс 100 кВ/м на расстоянии 1 м при частоте затухающей синусоиды 350 МГц. Частота повторения со-

ставляет 5 импульсов в минуту для времени жизни батареи 1 ч. Это устройство может легко переноситься внутри здания и размещаться близко к чувствительному электронному оборудованию. Для гиперполосного и субгиперполосного случаев большинство сигналов генерируется импульсными излучающими антеннами. Эта конструкция антенн способна к очень малым временам нарастания, что приводит к более высоким отношениям полосы. В табл. 3.1 описано несколько примеров таких генераторов [20]. Все они являются гиперполосными генераторами, поскольку отношение полосы у них более чем 10. Субгиперполосная категория ($3 \leq br \leq 10$) в основном содержит другие варианты генераторов импульсных излучающих антенн, которые не оптимизированы на такие короткие фронты, как 100 пс. Эти генераторы могут быть подобными описанным, но не требуют такого же уровня допусков, необходимого для достижения исключительно коротких фронтов.

В [42] рассматриваются примеры потенциальных источников микроволн высокой мощности и излучающих систем, приводятся многочисленные характеристики и фотографии (рис. 3.7).

Эволюция развития импульсных излучающих антенн кратко представлена в [43]. Много данных по узкополосным генераторам микроволн высокой мощности приведено во вводном курсе [44].

В [45] описывается новая точная, стабильная и транспортируемая антенная система для испытаний на восприимчивость к излучениям, создающая поле напряженностью 200 В/м в диапазоне от 2 до 40 ГГц с помощью фокусирующей и легко управляемой антенной системы с усилителями на полупроводниковых приборах (рис. 3.8).

В [46] приводятся характеристики станций исследования ионосферы (рис. 3.9) и детальные характеристики станции, созданной по американской программе НААРР (рис. 3.10); в заключении делается вывод, что она является очень мощным инструментом для исследований, но будет использоваться для определенных (совершенно секретных) военных целей.

Таблица 3.1

Примеры импульсных излучающих антенн

Название, страна	Генератор	Антенна	Ближнее поле	Дальнее поле	r_E	Отношение полосы, br	Полоса
Опытный образец антенны, излучающей импульсы, США	± 60 кВ, 100 пс/20 нс, 200 Гц, пачка импульсов	$\varnothing 3,66$ м, ($F/D=0,33$)	23 кВ/м при $r=2$ м	4,2 кВ/м при $r=304$ м	1280 кВ	100	Гипер
Усовершенствованный опытный образец антенны, излучающей импульсы, США	$\sim \pm 75$ кВ, 85 пс/20 нс, ~ 400 Гц	$\varnothing 1,83$ м, ($F/D=0,33$)	41,6 кВ/м при $r=16,6$ м	27,6 кВ/м при $r=25$ м	690 кВ	50	Гипер
Антенна, излучающая импульсы, Швейцария	2,8 кВ, 100 пс/4 нс, 800 Гц	$\varnothing 1,8$ м, ($F/D=0,28$)	1,4 кВ/м при $r=5$ м	220 В/м при $r=41$ м	10 кВ	50	Гипер
Антенна, излучающая импульсы, Нидерланды	9 кВ, 100 пс/4 нс, 800 Гц	$\varnothing 0,9$ м, ($F/D=0,37$)	7 кВ/м при $r=1$ м	—	34 кВ	25	Гипер
Антенна, излучающая импульсы, Германия	9 кВ, 100 пс/4 нс, 800 Гц	$\varnothing 0,9$ м, ($F/D=0,37$)	7 кВ/м при $r=1$ м	—	34 кВ	25	Гипер



Рис. 3.7. Импульсная излучающая антенна от ТНО (Нидерланды) (а) и компактный радиочастотный источник DS 110 от DIEHL (Германия) (б)

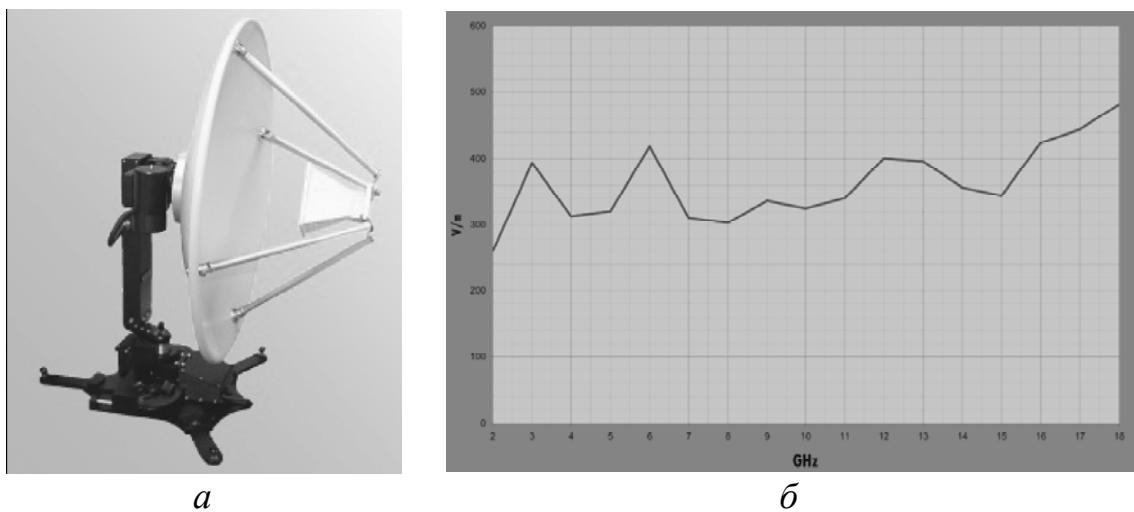


Рис. 3.8. Вид антенной системы (а) и типовая напряженность поля на расстоянии 1 м (б)

В [47] рассмотрена возможность влияния излучений от неструктурированных сетей на морские и авиационные радиослужбы на основе перекрытия частот их работы (рис. 3.11). Можно полагать, что этот путь потенциально пригоден для создания ПЭМП.

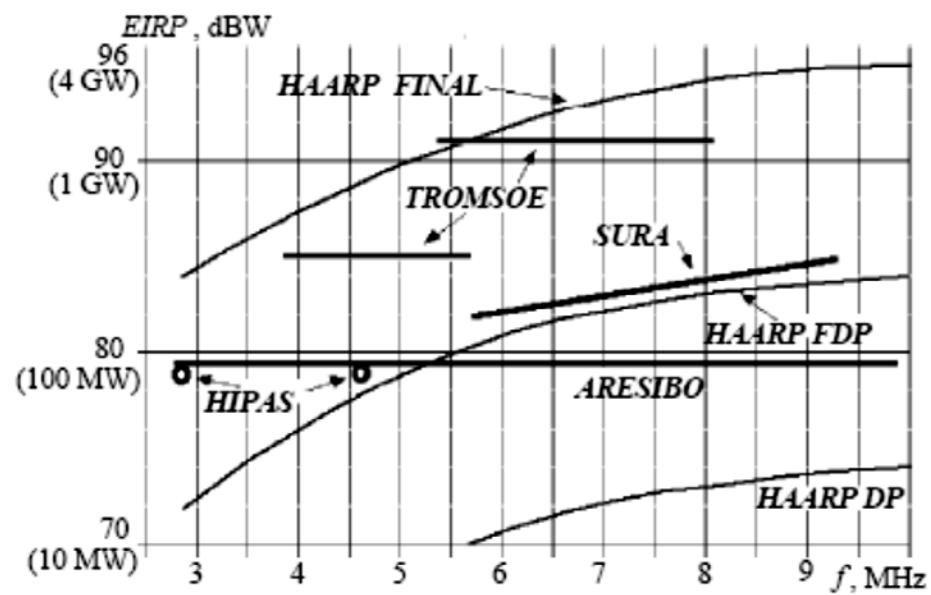


Рис. 3.9. Характеристики станций исследования ионосферы

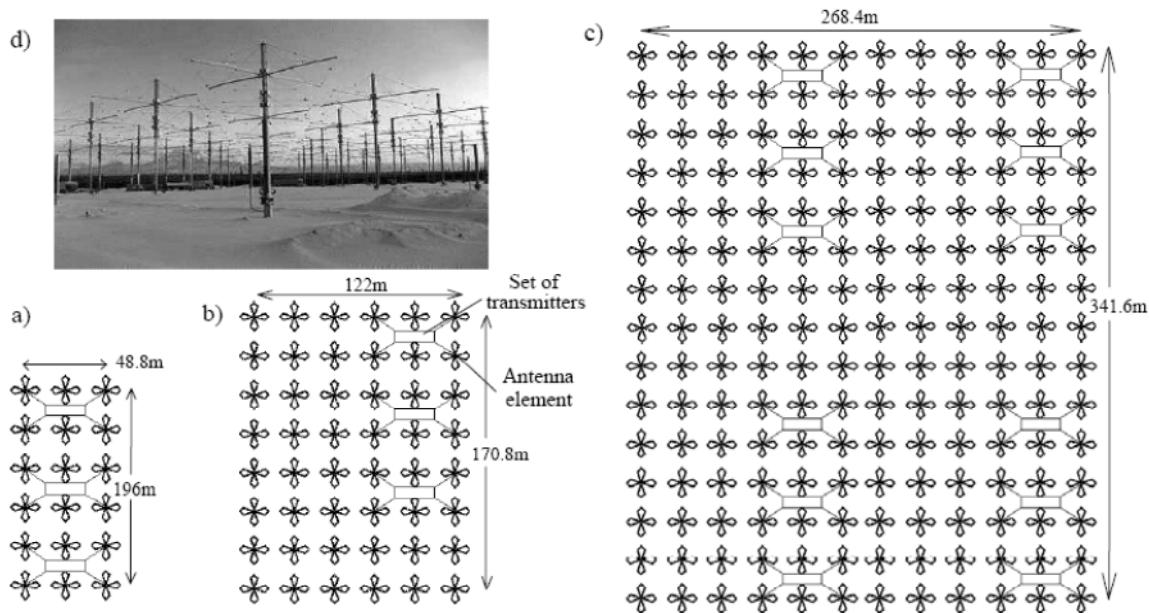


Рис. 3.10. Антенна HAARP: *a* – образец на стадии разработки; *b* – окончательный образец на стадии разработки; *c* – окончательная антенна; *d* – вид окончательного образца на стадии разработки

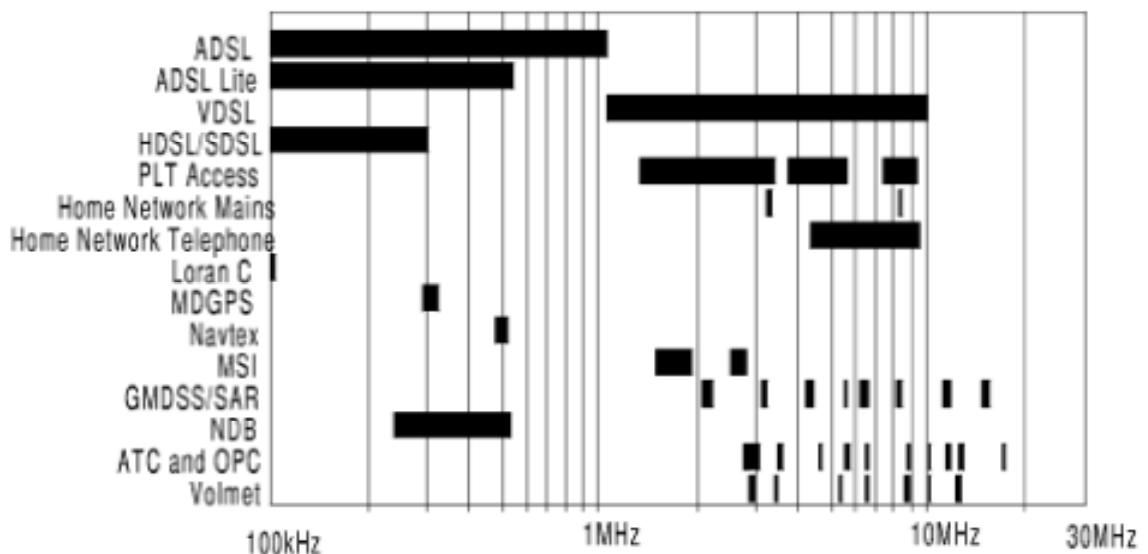


Рис. 3.11. Перекрытие частот неструктурированных сетей и морских и авиационных радиослужб

4. Электромагнитная уязвимость систем и компонентов

4.1. Компьютеры

Полезные косвенные оценки вероятности сбоя и повреждения реальных систем можно сделать исходя из уровней уязвимости типового оборудования. Поскольку в состав многих систем входит персональный компьютер (ПК), то весьма важно знать уровни уязвимости ПК к ЭМ воздействиям. Экспериментально определенные уровни уязвимости электронных устройств и систем опубликованы во многих работах. Испытания ПК при облучении материнской платы показали, что на них могут влиять узкополосные поля всего лишь в 30 В/м. Параметры ЭМ излучений, вызывающих нарушения работы различных ПК (с открытой крышкой), приведены в табл. 4.1 [48]. Как видно, уровень уязвимости ПК, не защищённого ЭМ экраном, сильно зависит от параметров микроволнового ЭМ воздействия и может составлять всего 30 В/м.

Последующие испытания [49] показали, что уровень восприимчивости зависит от быстродействия микропроцессора: более старые и медленные микропроцессоры более чувствительны к сбою. Это объясняется тем, что быстродействующие процессоры требовали конструирования лучших по электромагнитному экранированию компьютерных корпусов, чтобы пройти испытания на соответствие требованиям ЭМС на помехоэмиссию. Причина в том, что создаваемые компьютером сигналы частотой более 1 ГГц легко проникают через большие отверстия, типичные для корпусов ранних компьютеров. Примечательно, что даже для новых компьютеров на частотах около 500 МГц возможны уровни сбоя всего 500 В/м [9].

Сводные результаты по уровням сбоя компьютеров для воздействий [9]:

узкополосные (на 1 ГГц)	500 В/м;
мезополосные (оценка)	10 кВ/м;
гиперполосные	2 кВ/м.

Таблица 4.1

Описание испытываемых ПК, воздействующего поля и наблюдаемых эффектов

Тип ПК	Частота несущей, ГГц	Воздействующее поле			Наблюдаемые эффекты
		Напряженность и модуляция электрического поля В/м	Модуляция	Поляризация	
133 МГц Pentium	2,713	30	НВ	Y	Z
	2,770	50	AM	Y	Z
	1,133	50	AM, имп.	Y	Z
	2,675	50, 75	AM, имп.	Y	Z
	2,887	75	AM	Y	Z
233 МГц Pentium2	1,070	100	Имп.	X	Z
	1,460	100	AM, НВ, имп.	X	Z
	1,480	100	НВ	Y	Z
300 МГц Pentium2	1,040	45	Имп.	Y	Z
	1,400	100	НВ	X	Z
	1,510	100	AM	X	-Z
	1,515	100	AM	X	Z
	1,510	75	Имп.	Y	Z
	1,750	75	Имп.	Y	Z
	1,430–1,550	50	Имп.	X	-Z
	1,690	85	Имп.	Y	Z

Уровни повреждения для импульсных сигналов начинаются со значений, которые лишь в 2–3 раза больше уровней сбоя. Для узкополосных сигналов уровни повреждения во много раз выше уровней сбоя.

В [50] приведен обзор двух весьма обстоятельных исследований восприимчивости, выполненных в ЭМС-группе фирмы QinetiQ, Англия. В первом оценивался порог восприимчивости коммерческого компьютерного оборудования к мощным электромагнитным излучениям в реверберационной камере (рис. 4.1), а во втором – к импульсным излучениям в проводном имитаторе (рис. 4.2).

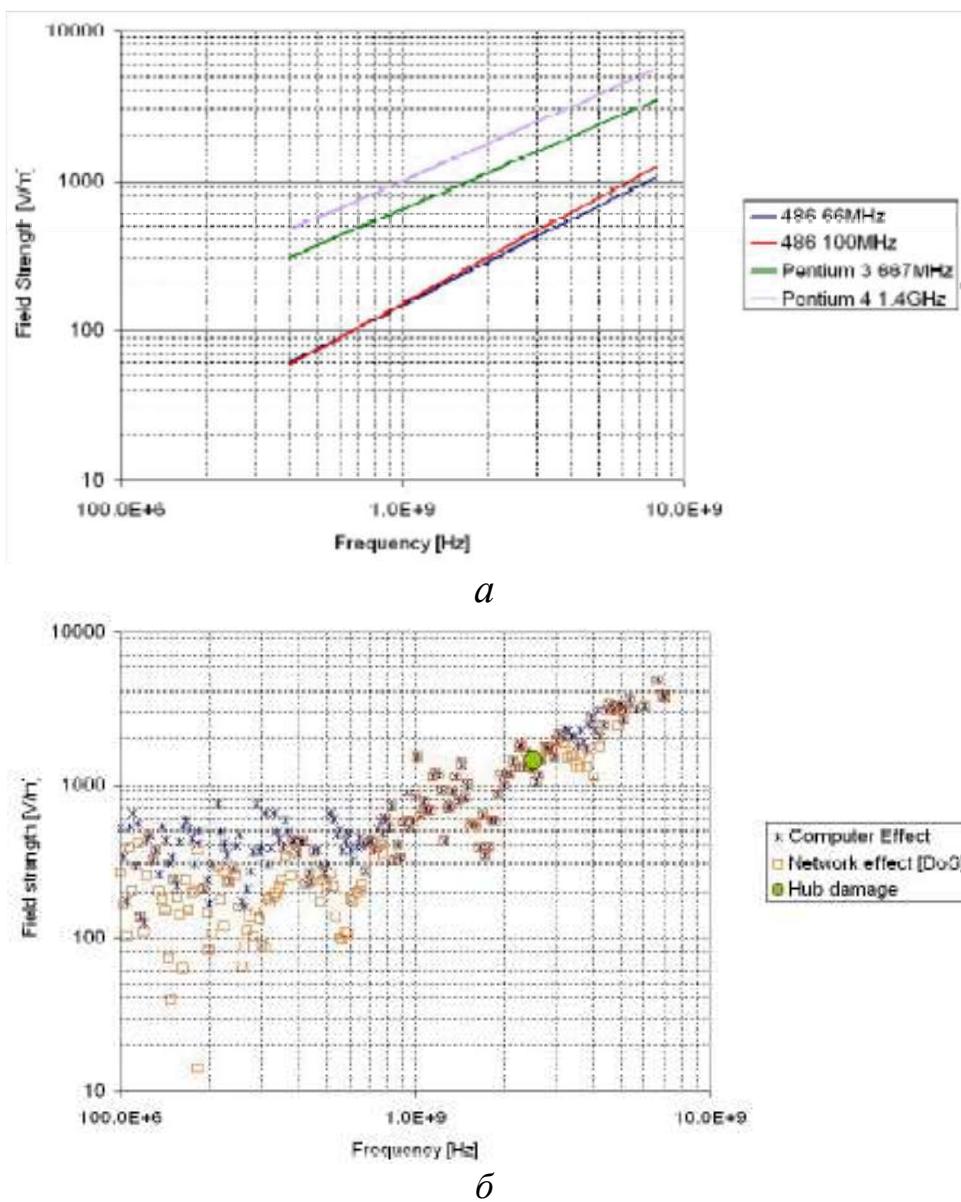
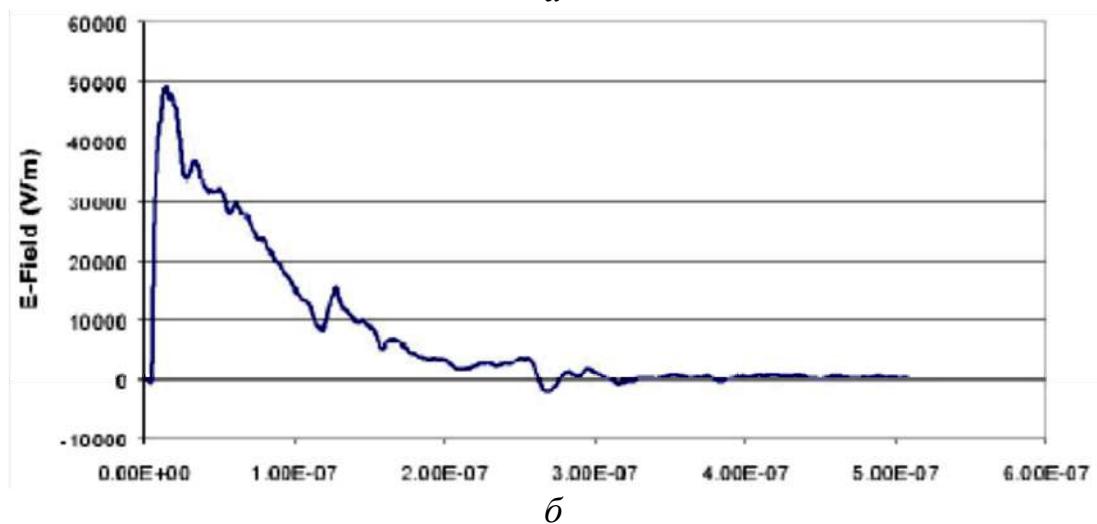


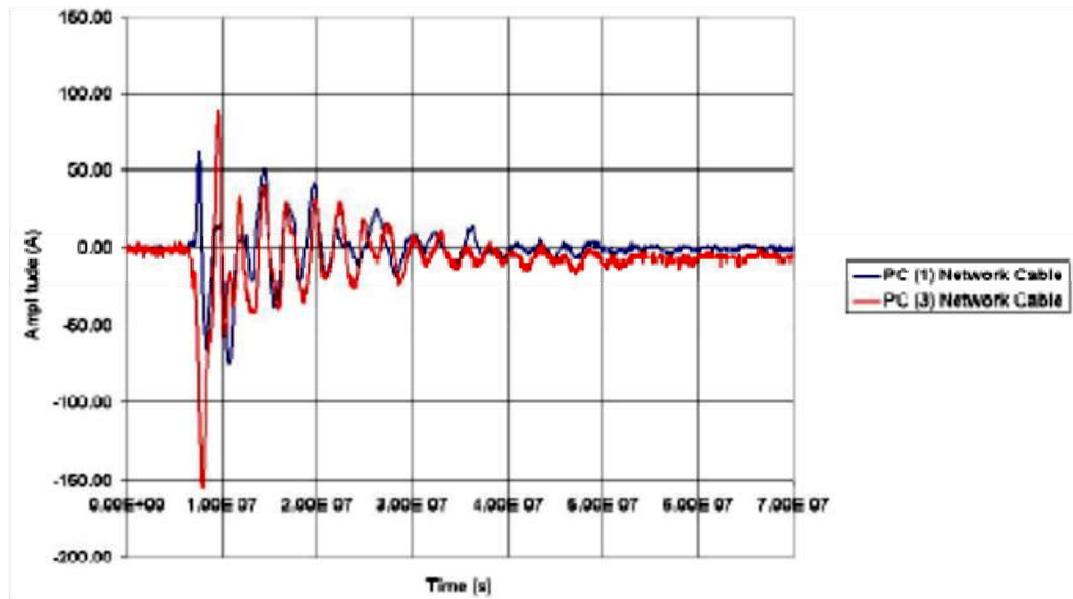
Рис. 4.1. Порог сбоя четырех компьютеров: *a* – только тренды; *б* – восприимчивость сети



a



b



c

Рис. 4.2. Импульсный имитатор QinetiQ (*a*), типичный измеренный импульс поля в имитаторе (*б*), наведенные в кабелях токи при 45 кВ/м (*в*) (начало, окончание см. на с. 32)

	8kV/m	15kV/m	22kV/m	30kV/m	45kV/m
PC (1)	0/5	0/5	5/5	6/6	5/5
CPU (P3 667)	0/5	0/5	0/5	6/6	5/5
Monitor (CRT)	0/5	0/5	0/5	0/6	0/5
Keyboard	1/5	1/5	5/5	1/6	1/5
Mouse	0/5	0/5	5/5	0/6	0/5
Network Interface	0/5	0/5	0/5	0/6	1/2
PC (2)	0/5	0/5	2/5	4/6	5/5
CPU (P3 667)	0/5	0/5	2/5	4/6	5/5
Monitor (CRT)	0/5	0/5	0/5	0/6	0/5
Keyboard	0/5	0/5	0/5	0/6	0/5
Mouse	0/5	0/5	0/5	0/6	0/5
Network Interface	0/5	0/5	0/5	0/6	0/5
PC (3)	0/5	0/5	2/5	1/6	1/5
CPU (P3 667)	0/5	0/5	0/5	0/6	1/5
Monitor (CRT)	0/5	0/5	1/5	0/6	0/5
Keyboard	0/5	0/5	1/5	1/6	0/5
Mouse	0/5	0/5	0/5	1/6	0/5
Network Interface	0/5	0/5	0/5	0/6	1/5
Hub	0/5	0/5	0/5	0/6	2/5
 Damage or Combination of Damage and User Intervention Upset Requiring User Intervention					

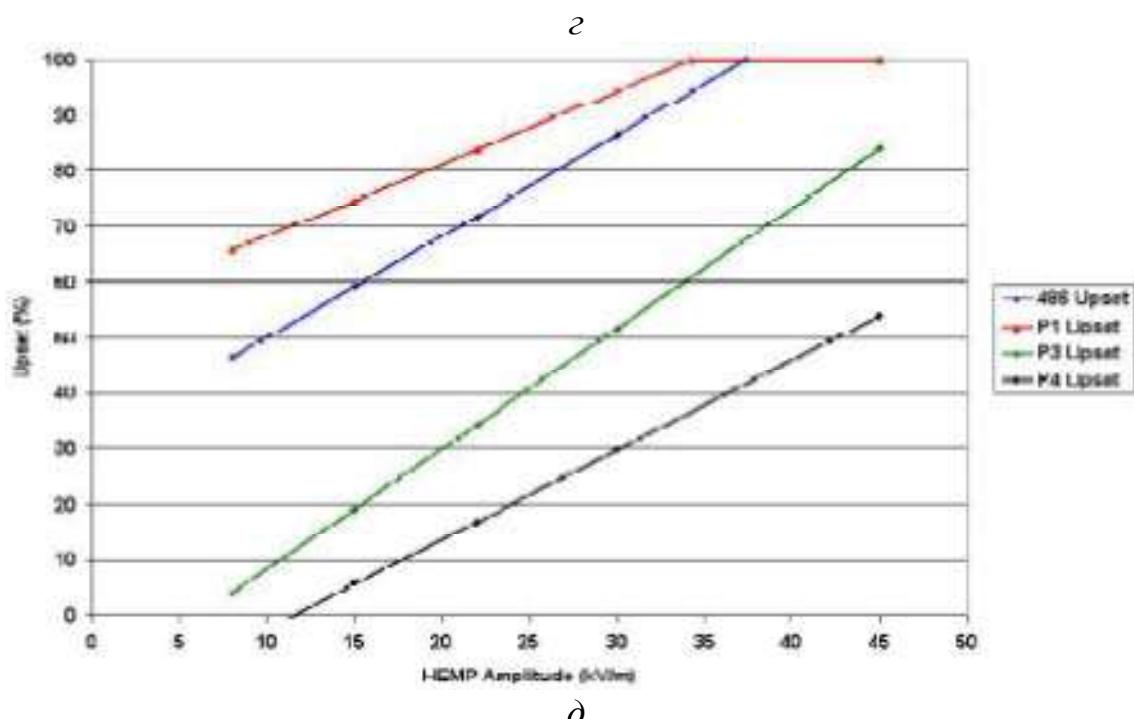


Рис. 4.2. Сравнение восприимчивости компьютеров (ε), средний процент сбоя сетей четырех компьютеров: только тренды (δ)
(окончание, начало см. на с. 31)

Статистически значимые результаты (25–50 повторений каждого испытания) экспериментальных исследований восприимчивости одноплатного компьютера Crystal CS5OO с микропроцессором AMD 386-SX (рис. 4.3), выполненных в Mission Research Corporation, приведены в [51]. Испытания (рис. 4.4) проводились микроволновыми импульсами в диапазоне параметров импульса: длительность 100–10000 нс, частота повторения 0,01–1,5 МГц, число импульсов 1–100. Предложена простая аналитическая модель вероятности отсутствия сбоя, коррелирующая с экспериментальными данными (рис. 4.5), которая позволяет выполнить аналитические оценки в случае ограниченного числа испытаний.

Manufacturer	Crystal Group
CPU	AMD 386-SX
CPU Clock Speed	40 MHz
Hard Drive Capacity	520 MB
RAM	4MB
Floppy Drive	1.44MB
Video Card	None (Modified BIOS)
Operating System	DOS 5.0
Terminal Program	CTTY (Part of DOS)
Communications Ports	2 Serial Communications Ports
Keyboard Port	Keyboard Port available, but not used.

Рис. 4.3. Характеристики испытываемого компьютера

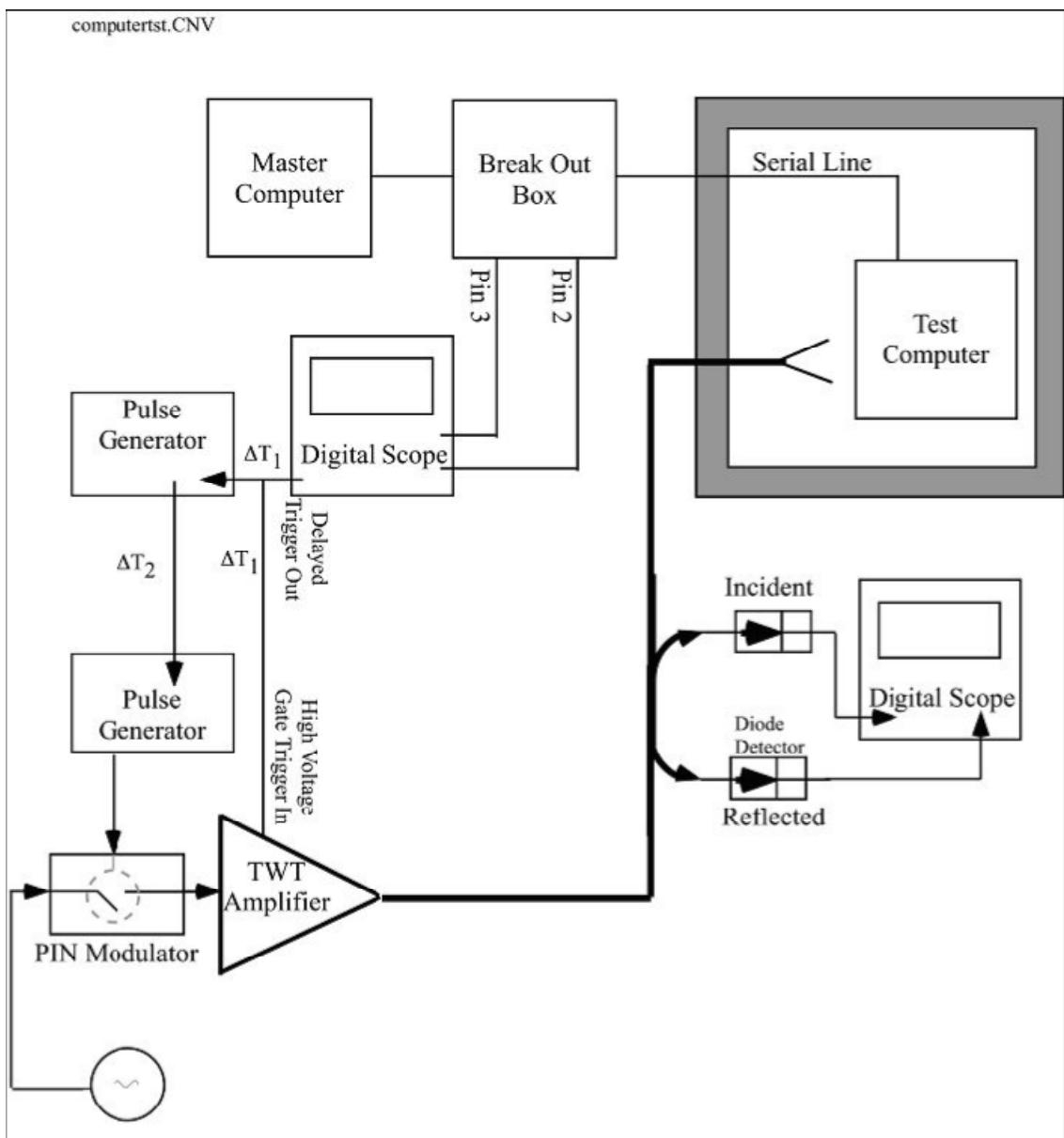


Рис. 4.4. Испытательная установка для измерения вероятности выхода из строя компьютера

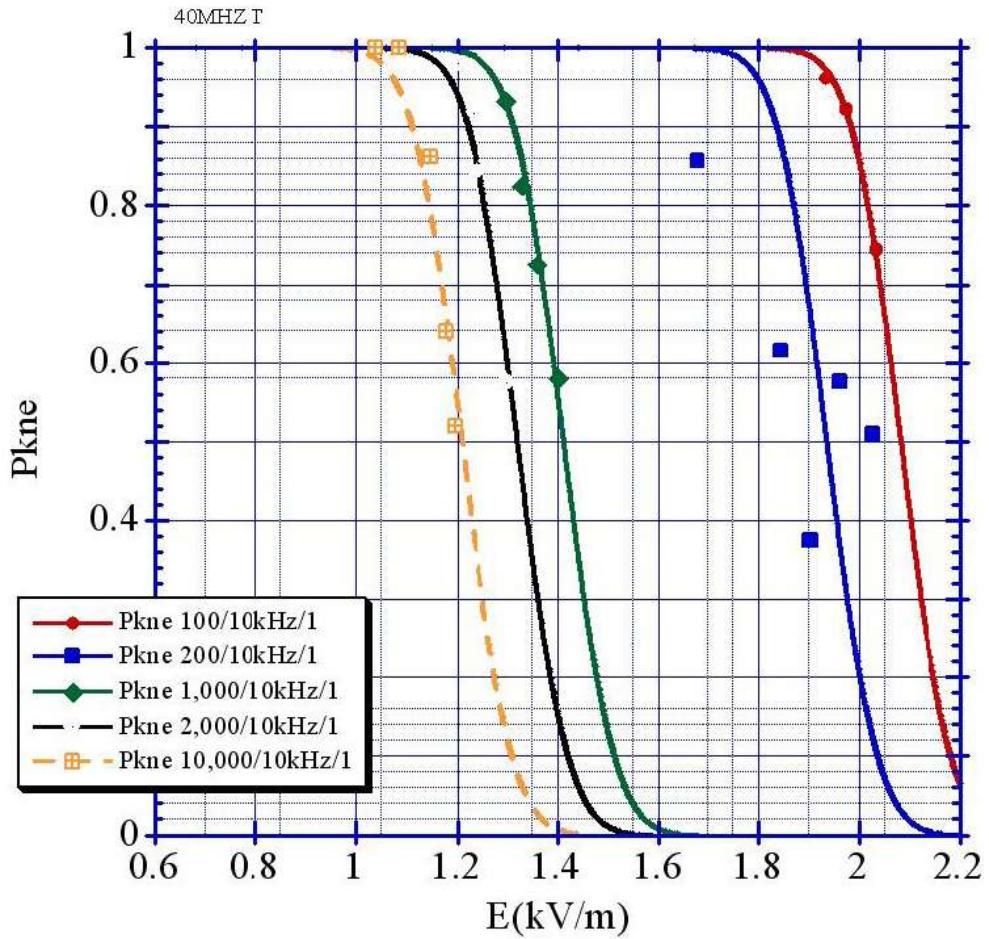


Рис. 4.5. Сравнение результатов испытаний и модели

В [52] приведены результаты экспериментального исследования восприимчивости компьютеров и их компонентов к низкочастотным воздействиям.

4.2. Автомобиль

Весьма важной и неотъемлемой составляющей жизни человека стал автомобиль, функционирование многих систем которого зачастую становится критичным. Нередко именно на автомобиль устанавливают радиоэлектронную аппаратуру, от функционирования которой зависит его безопасность для людей. В этой связи результаты мощного ЭМ воздействия на автомобиль (рис. 4.6) представляют особый интерес для оценки дальности возможного саботажа. Результаты такой оценки для двух источников разной мощности без экрана и с экраном с эффективностью экранирования (ЭЭ) 30 дБ приведены в табл. 4.2. Как видно,

автомобиль, подвергаемый мощному микроволновому облучению от источника размером с кейс (100 кВт), получает сбой на расстоянии 50 м, а от источника размером с фургон (10 МВт) – сбой на расстоянии 500 м и повреждение на расстоянии 15 м [53]. Испытания автомобиля фиксированными частотами в диапазоне 1,3–15 ГГц показали сбой (остановку двигателя) при 500 В/м на 1,3 ГГц и перманентные повреждения при 15 кВ/м на 1,3 ГГц, а при 24 кВ/м на 2,86 ГГц.

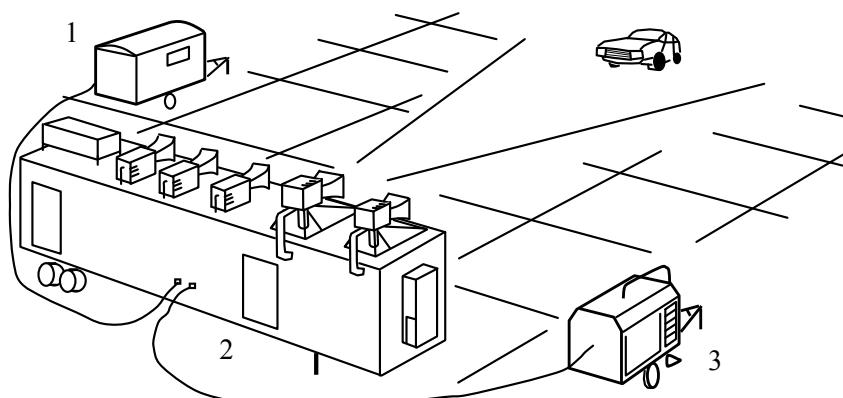


Рис. 4.6. Микроволновая испытательная установка для автомобиля: 1 – кабина дистанционного управления; 2 – система генерации микроволн; 3 – дизель-генератор

Таблица 4.2

Оценка дальности действия для саботажа
по результатам испытаний автомобиля на воздействие МВМ

Источник	Результат на дальности, м		
	15	50	500
МВМ фургон $P=10 \text{ МВт}$	Долговременное повреждение	Временный сбой**	Временный сбой**
МВМ кейс * $P=100 \text{ кВт}$	Временный сбой**	Временный сбой**	Нет влияния
МВМ фургон $\mathcal{E}=30 \text{ дБ}$	Временный сбой**	Нет влияния	Нет влияния
МВМ кейс * $\mathcal{E}=30 \text{ дБ}$	Нет влияния	Нет влияния	Нет влияния

* Может вызвать долговременное повреждение вблизи жертвы.
** Может вызвать долговременное повреждение.

Обращает внимание сопоставимость по уровням (500 В/м) сбоев компьютера и автомобиля. Для частот ниже 1,3 ГГц воз-

можно снижение уровня сбоя для автомобиля, если к нему применимы тенденции, показанные для компьютеров.

В [54] обстоятельно описано экспериментальное и компьютерное моделирование влияния мощных электромагнитных излучений на работу цифровой электроники, а именно таймера, используемого для управления последовательностью сигналов свечей зажигания в автомобиле. Наблюдались мягкие и жесткие сбои и идентифицировались важные параметры цепей и воздействующего сигнала, влияющие на сбои.

4.3. Макет корпуса ракеты GENEC

Результаты детального экспериментального исследования восприимчивости электроники внутри макета корпуса ракеты GENEC (рис. 4.7), причем двумя методами: на открытой территории и в реверберационной камере, представлены в [55]. Облучение проводилось микроволновыми импульсами частотой 2,86 ГГц длительностью 5 мкс с частотой повторения 30 Гц. Минимальная напряженность поля для нарушения работы электроники составила около 1 кВ/м.

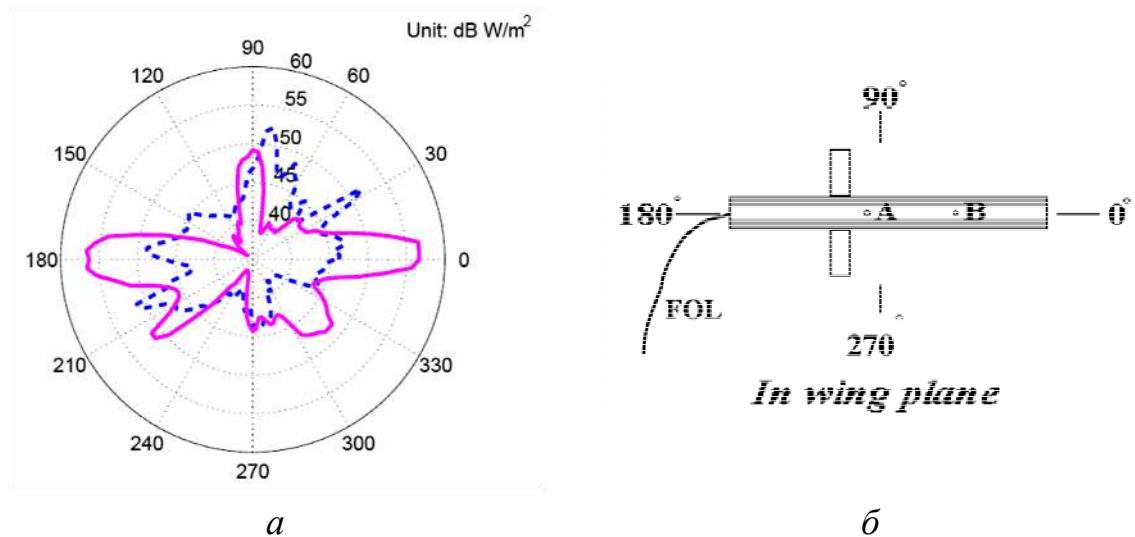


Рис. 4.7. Ориентация ракеты GENEC (а); минимальная плотность мощности, необходимая для влияния на электронику внутри GENEC, в зависимости от угла облучения (б). Корпус GENEC облучался в плоскости крыльев при поляризации электрического поля, параллельной (пунктирная) и перпендикулярной (сплошная) плоскости крыльев

Результаты расширенных экспериментальных исследований угловых диаграмм восприимчивости GENEC к слабым и сильным микроволновым излучениям детально описаны в [56], где приведены детали эксперимента и диаграммы для широкого диапазона частот (рис. 4.8).

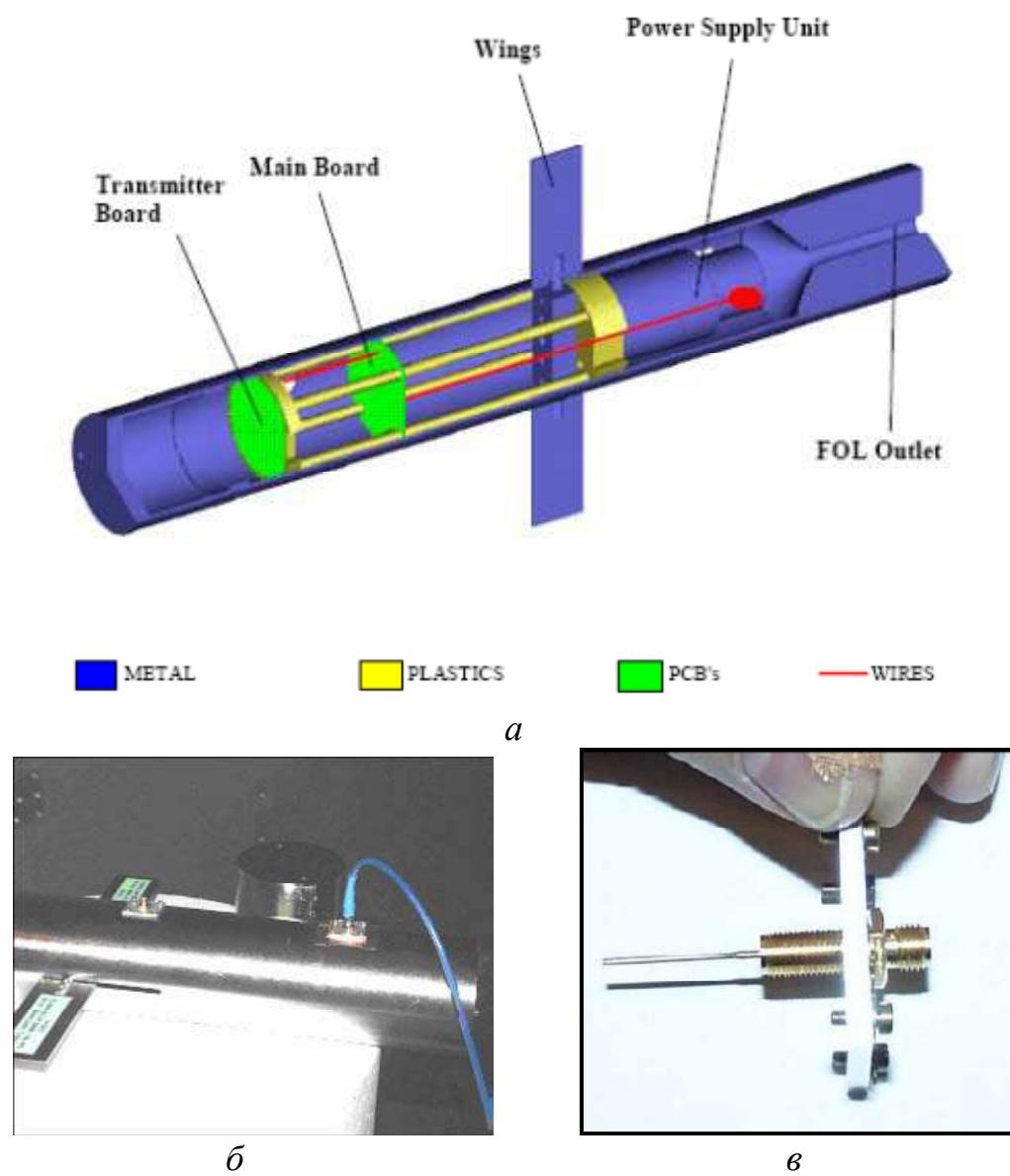


Рис. 4.8. Ракета GENEC (FOL – Fiber Optic Lead) (а). Крылья, щель и места двух датчиков с одним присоединенным (б). Крупный вид датчика поля и его разъема; часть слева от металлической пластины находится внутри GENEC (в) (начало, окончание см. на с. 39)

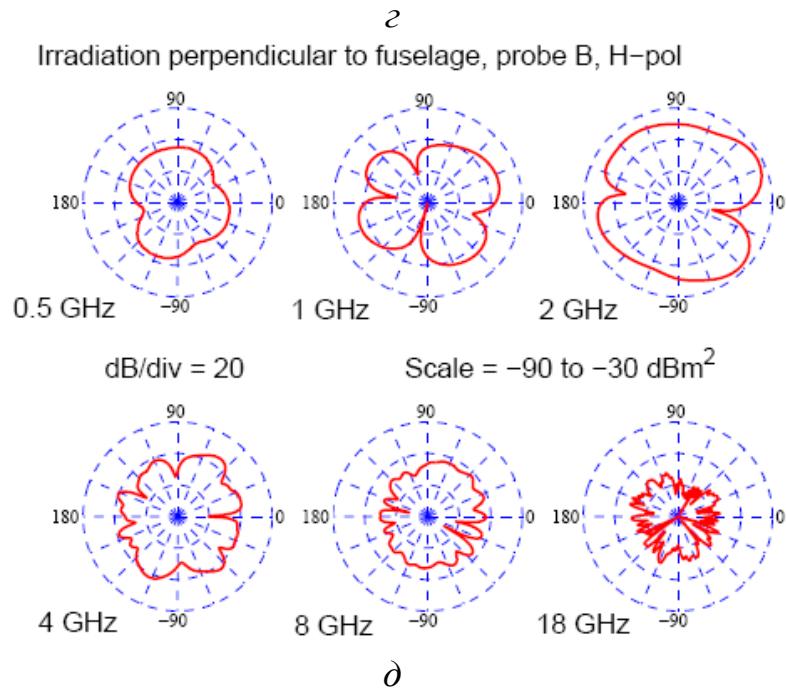


Рис. 4.8. Облучение в плоскости крыльев

GENEC антенной S-диапазона. Все соединения с GENEC сделаны оптоволокном для отсутствия воздействия от излучаемого поля. Поворотное устройство позволяет вращать GENEC на 360° (φ). Угловые диаграммы приема при измерениях на слабом уровне (δ) (окончание, начало см. на с. 38)

Восприимчивость наиболее уязвимой цепи, цепи сброса логических компонентов на плате, состоящей из памяти, микрокон-

троллера и EPLD приборов и помещенной в металлический макет корпуса ракеты GENEC (часть французско-германского сотрудничества), исследована теоретически, численно и экспериментально в [57]. Выявлено, что для GENEC первая частота отсечки 1,6 ГГц для прохождения внешнего воздействия внутрь корпуса через крылья и щели ракеты очень близка к частоте первого внутреннего резонанса корпуса ракеты. Таким образом, на частотах около 1,6 ГГц напряженность поля внутри ракеты и вблизи платы достаточно высока для индукции значительного паразитного сигнала на печатных проводниках платы, причем анализ трассировки платы показал, что линия сброса является источником сильной наводки.

Результаты компьютерного и экспериментального моделирования воздействия внешнего поля внутри обобщенного корпуса ракеты GENEC (рис. 4.9) приведены в [58] (рис. 4.10).

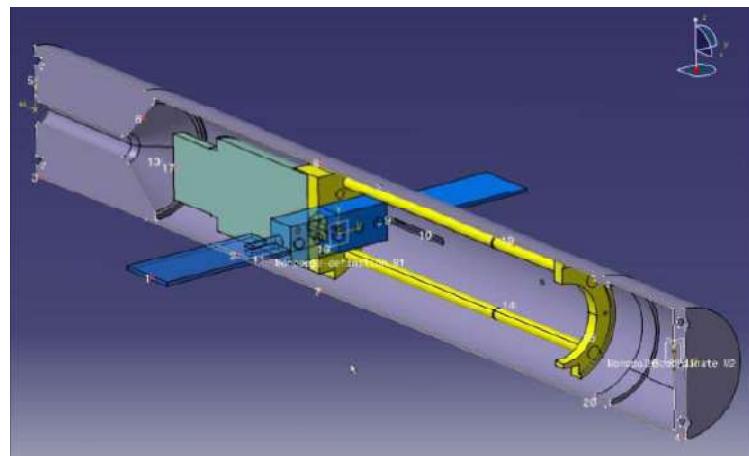


Рис. 4.9. Усеченный вид объекта GENEC, использованный в моделировании

В [59] разработаны 2 печатные платы, которые вставлялись в обобщенный корпус ракеты GENEC для исследований по восприимчивости к воздействиям. Одна плата аналого-цифровая, с ТТЛ и КМОП компонентами с напряжением питания 5 В, другая – микроконтроллер на 3,3 В. Обе платы подвергались мощным электромагнитным воздействиям различных типов, включающим немодулированные непрерывные колебания и сверхширокополосные. Экспериментальные результаты показали нарушение работы от сбоев до замираний и повреждения (рис. 4.11).

GENEC Configuration 1: 17_3

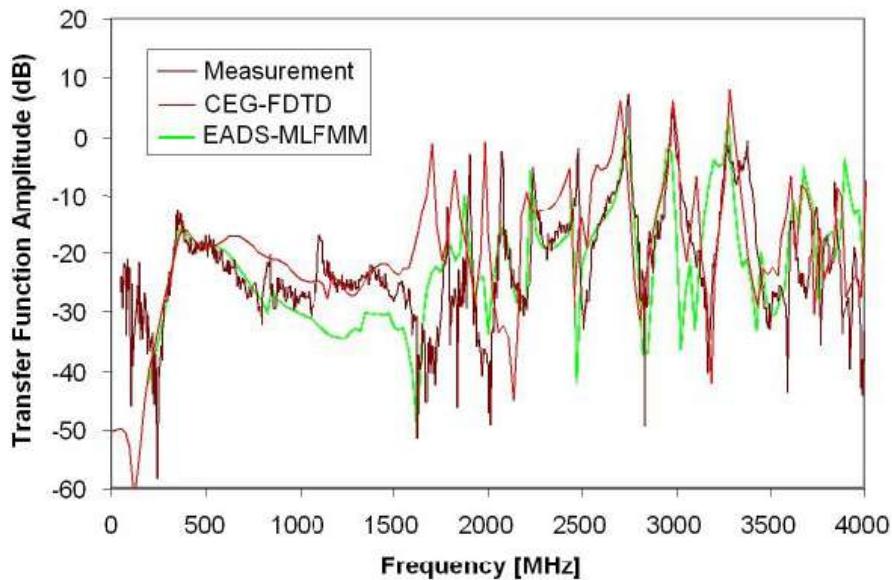


Рис. 4.10. Пример передаточной функции электрического поля для волны из свободного пространства до тестовой точки внутри GENEC. Сравнение результатов моделирования в CEG (Centre des Etudes de Gramat), кодом Protheus/MLFMA и измерений

В работе также представлен процесс наводки, как теоретически, так и экспериментально. Кроме того, показаны результаты определения передаточных функций для непрерывных и сверхширокополосных колебаний. Они использованы при разработке метода оценки наводки на печатную плату для наихудшего случая.

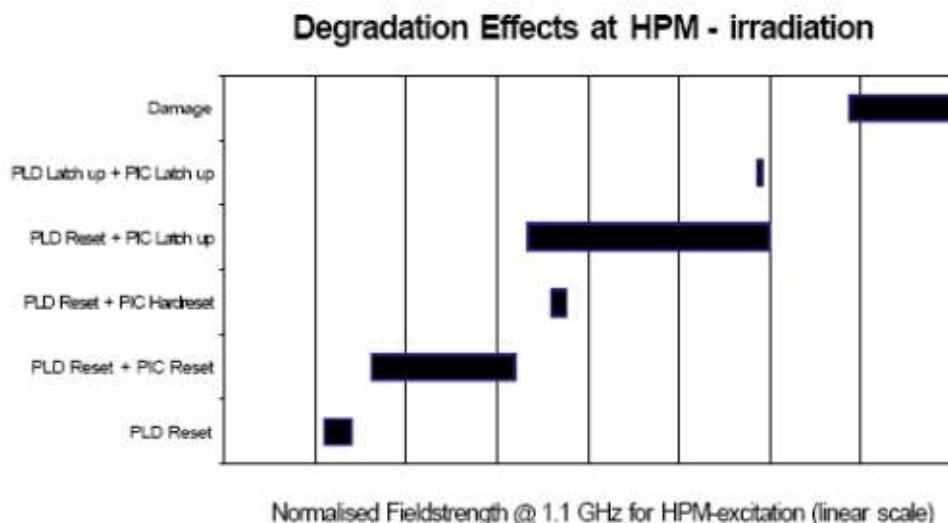


Рис. 4.11. Деградационные эффекты при воздействии мощных микроволн (начало, окончание см. на с. 42)

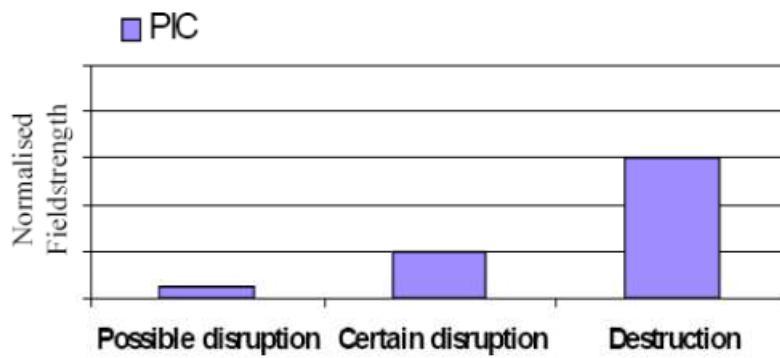


Рис. 4.11. Тенденции в напряженности поля от первых сбоев до выхода из строя PIC-микроконтроллера. Разница в напряженности поля от первых сбоев до разрушения примерно в 10 раз (окончание, начало см. на с. 41)

4.4. Электроэнергетика

В [60] приводятся результаты экспериментального исследования восприимчивости шкафа с микропроцессорными реле высоковольтных подстанций к воздействию электромагнитного импульса.

В [61] выполнена обзорная оценка стойкости сети электропитания (рис. 4.12) к воздействию геомагнитных бурь и преднамеченных электромагнитных воздействий (рис. 4.13).

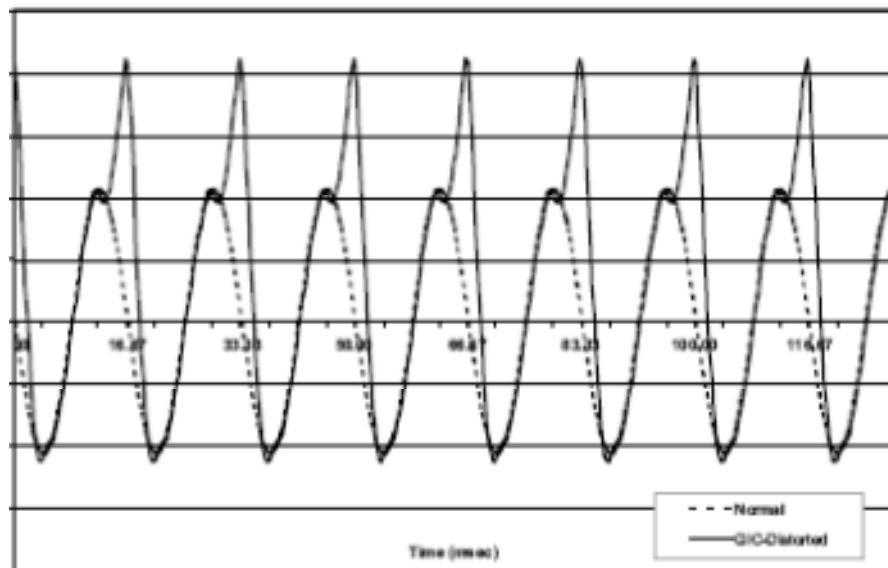


Рис. 4.12. Трансформатор 500 кВ: нормальный переменный ток (---); переменный ток, искаженный четными и нечетными гармониками из-за полупериодного насыщения трансформатора, вызванного геомагнитно наведенными токами (—)

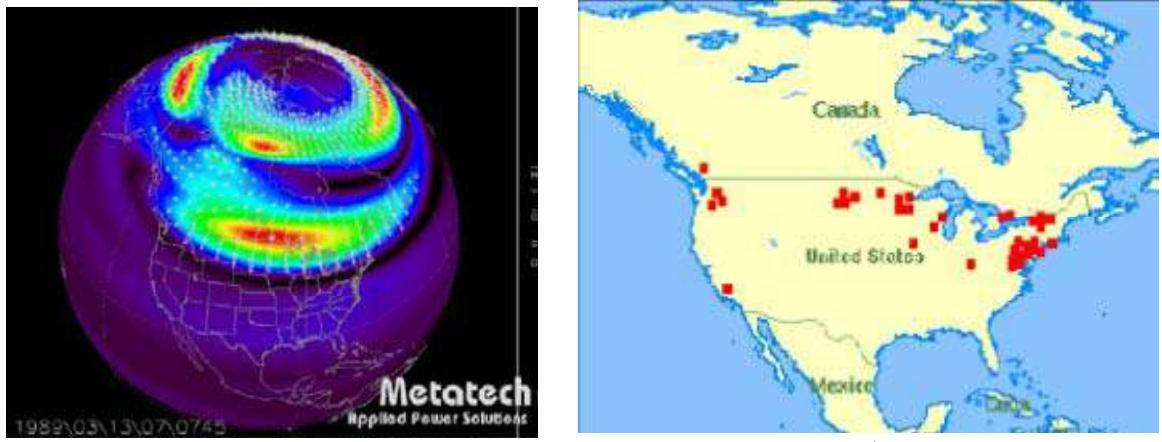


Рис. 4.13. Карта погоды, с контурами производной от магнитных полей в момент аварии сети питания (Hydro-Quebec, 7:45 UT or 2:45 EST, March 13, 1989) (а). Зафиксированные влияния на сеть питания в Северной Америке, March 13, 1989, time 16:00–17:23 EST (21:00–22:23 UT) (б)

В [62] описывается обстоятельное исследование критического напряжения пробоя для изоляторов класса 15 кВ при воздействии не только имитирующих молнию импульсов 1,2/50 мкс, но и импульсов 60/200 нс (рис. 4.14). Аналогичные исследования представлены в [63].

В [64] исследуется восприимчивость конкретных типов электронной аппаратуры управления электропитанием (рис. 4.15, 4.16) к кондуктивным помехам, вызванным электромагнитным импульсом высотного ядерного взрыва.

В [65] показано, что электромагнитные помехи от защитных разрядников влияют (снижая скорость передачи вплоть до срыва) на работу схем мониторинга и контроля переключателя среднего напряжения, использующих технологии Bluetooth и 802.11b.

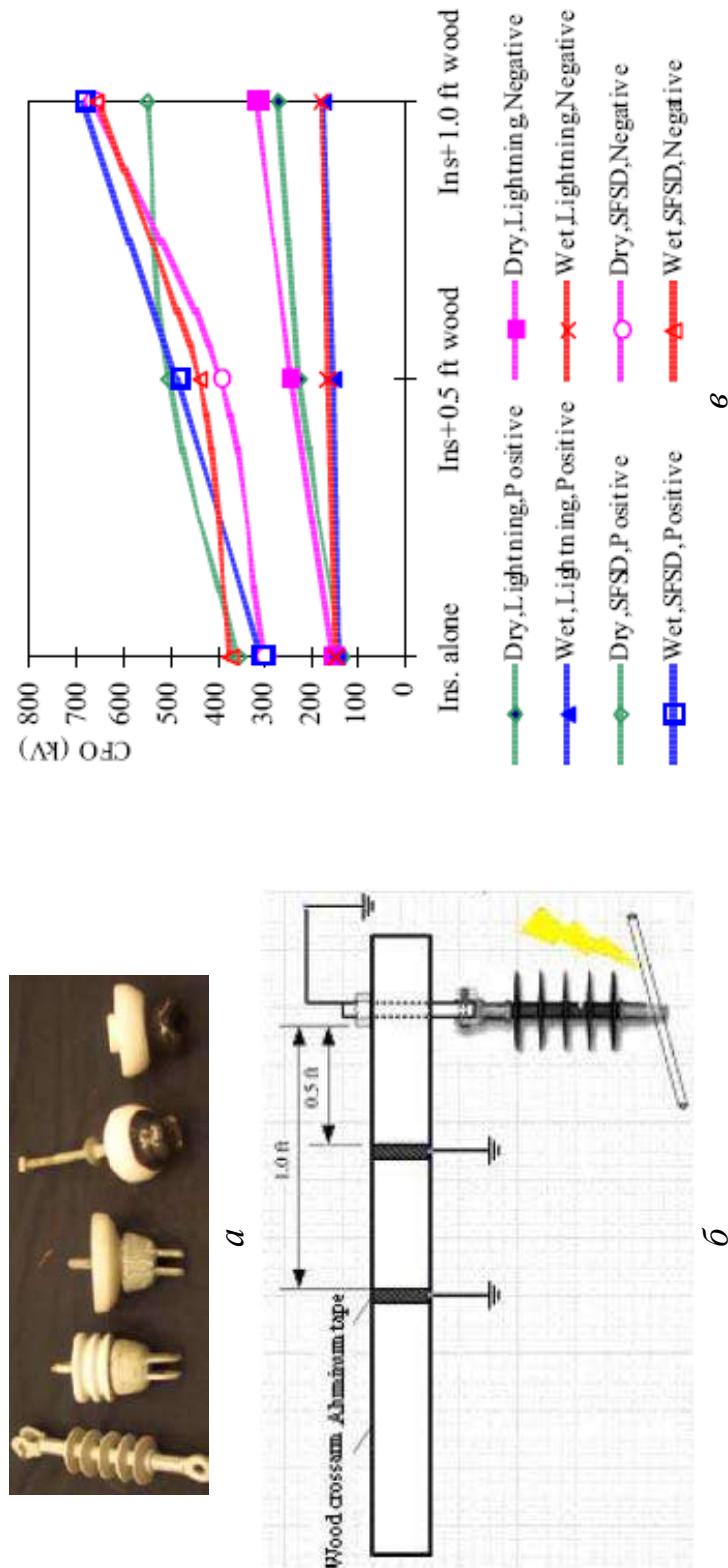


Рис. 4.14. Изоляторы слева направо (названия в оригинале): 15кВ Class Polymer Suspension Insulator, ANSI 52-9 15кВ Class Suspension Insulator; ANSI 52-1 15кВ Class Suspension Insulator; ANSI 55-3 15кВ Class Pin Insulator; ANSI 55-4 15кВ Class Pin Insulator (а).
Схема эксперимента для полимерного изолятора 15 кВ с деревянным бруском (б).
Критическое напряжение пробоя для изолятора 15 кВ из полимерной сuspензии
с деревянным бруском при различных условиях испытаний (в)

Permanent Damage to SEL-2701 Ethernet at 1.2 kV.
Shot 3491 (2.0 kV) waveforms

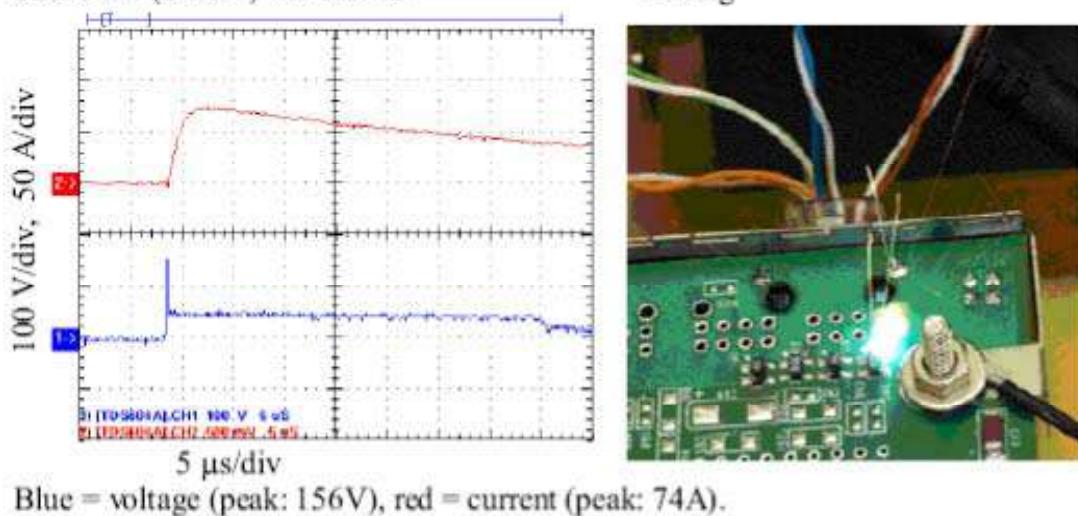


Рис. 4.15. Образец воздействия медленного импульса на SEL2701 Ethernet порт. На графике показаны формы напряжения (снизу) и тока (сверху). (Этот порт был уже поврежден прежде импульсом напряжения малого уровня и показано дальнейшее повреждение данным воздействием.)

Permanent Damage, Shot 74, 4.5 kV Pulse, MicroLogix 1000 Analog Input

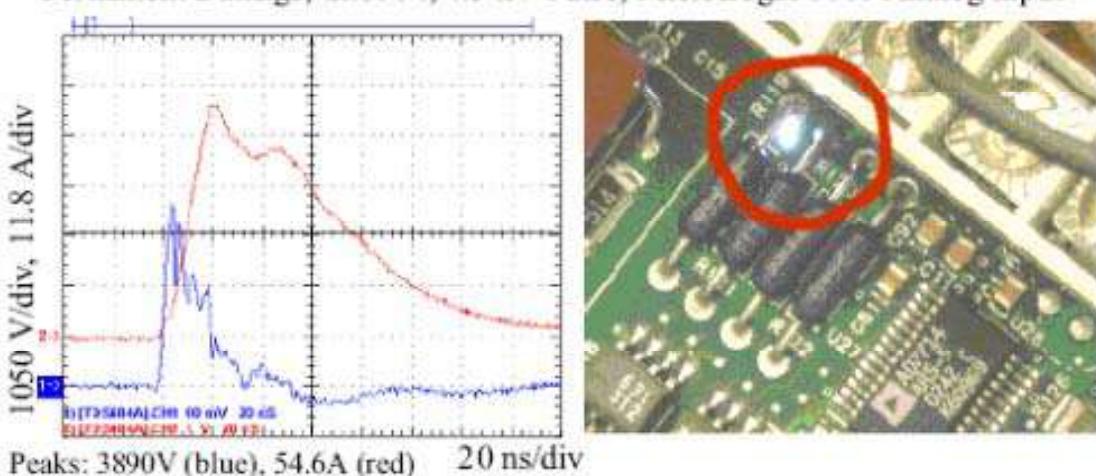


Рис. 4.16. Образец воздействия на MicroLogix 1000, вызвавшего повреждение. Напряжение снизу, ток сверху. (Было искрение, но это не защищило аналоговые входы компонентов схемы.)

4.5. Авионика

В [66] представлены результаты исследования отчетов по фактам помех в самолетах, вызванных, предположительно, переносными электронными устройствами (рис. 4.17). Эти отчеты

классифицированы и проанализированы по типам самолетов, их подвергшимся влиянию системам, деталям событий и фазам полета. Собранные за 1993–2006 гг. 204 отчета показали, что около трети событий имеют определенное отношение к переносным электронным устройствам и что растет число аномалий, связанных с работой автопилота. Большинство проблем связывают с сотовыми телефонами. Вероятность помех возрастает на малой высоте, а значит, они могут вызываться радиоволнами с земли.

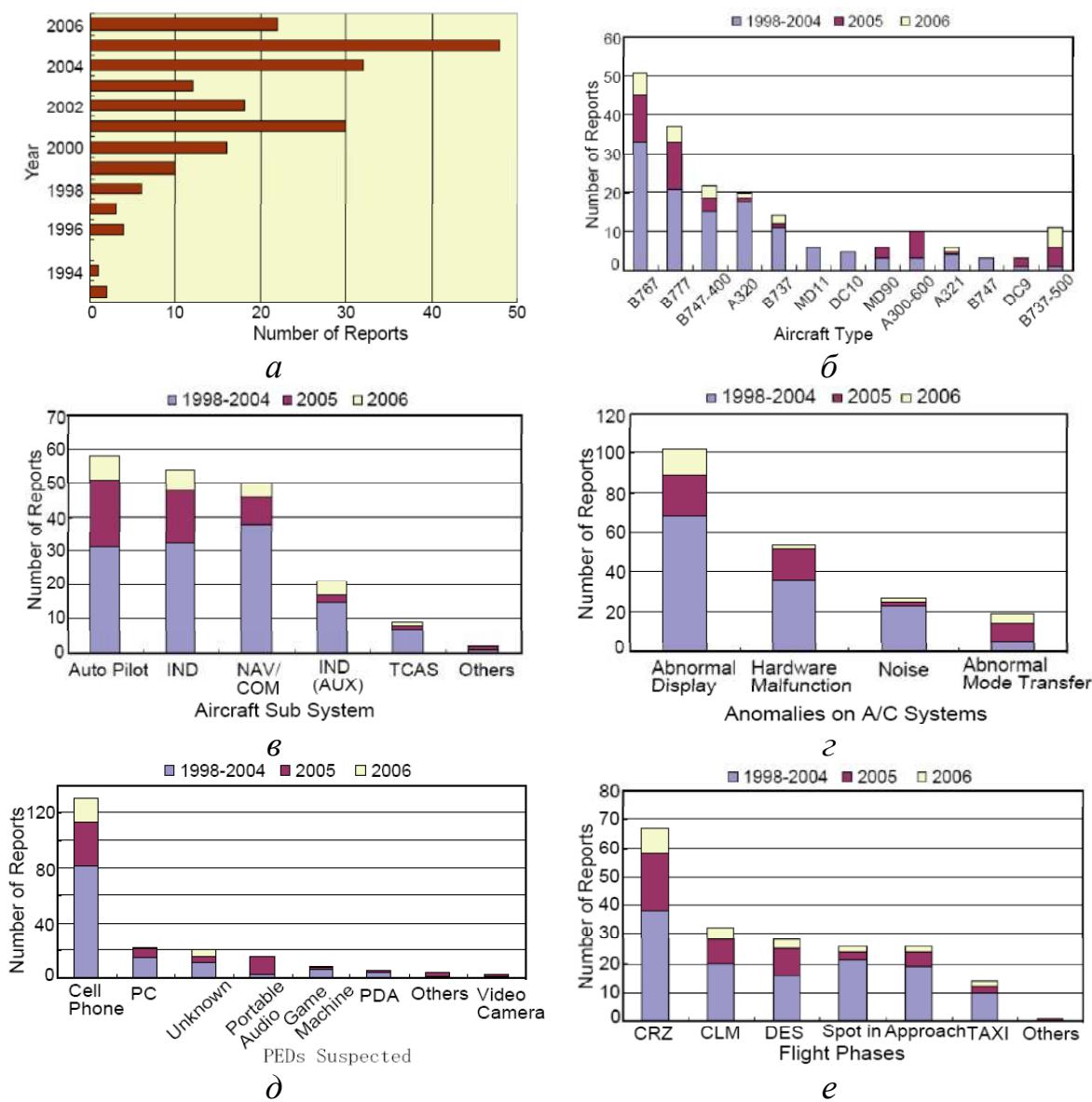


Рис. 4.17. Число отчетов об электромагнитных помехах в самолетах: по годам (a); по типам самолетов (б); по подсистемам самолета (в); по видам аномалий (г); по предполагаемым источникам (д); по фазам полета (е)

В работе германских специалистов EUROCOPTER [67] приводятся результаты исследования влияния переносных электронных устройств на авионику вертолета. Сделаны следующие выводы: сигнальные линии защищены; не исключены помехи связным VHF/FM приемникам; в целом защищены навигационные приемники, кроме VOR, DME и GPS; GPS особенно подвержена влиянию мобильных телефонов GSM и UMTS.

В [68] представлены результаты расследования причин взрыва и падения в Атлантический океан самолета (Boeing 747 Series 100 рейса TWA-800 17 июля 1996 г., через 14 минут после вылета из Нью-Йорка в Париж) с позиции возможности воспламенения топлива от электромагнитных помех, вызванных переносными электронными приборами пассажиров (рис. 4.18).

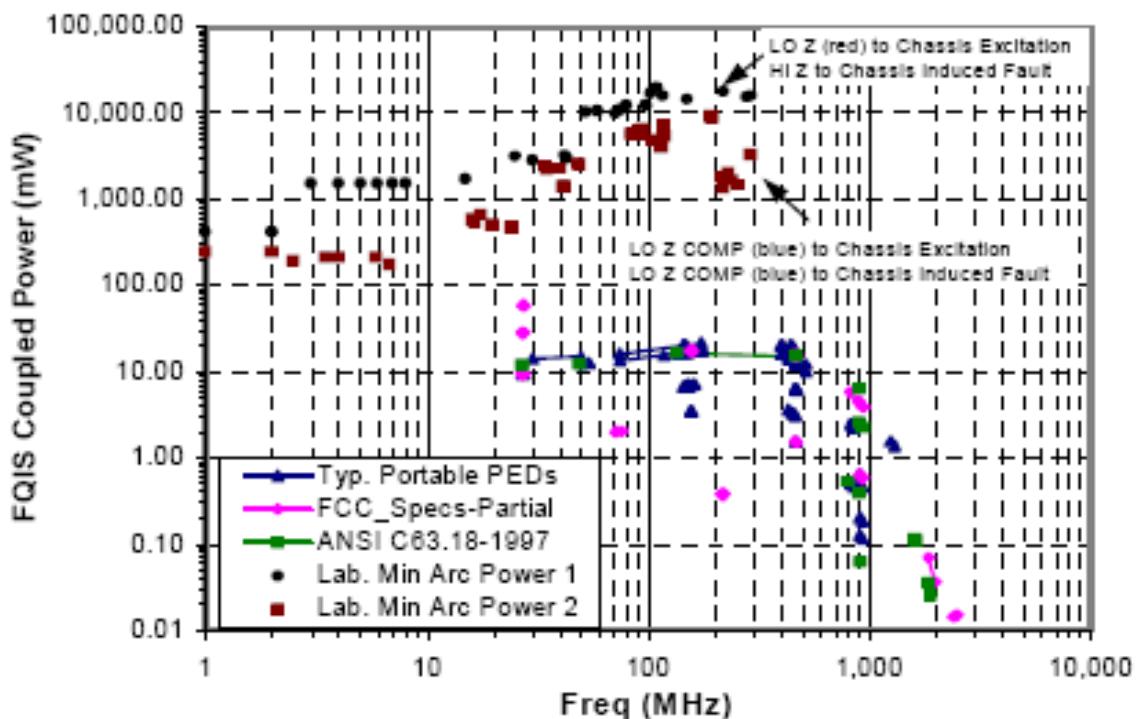


Рис. 4.18. Угрозы переносных электронных приборов разводке системы датчика количества топлива. Также показаны минимальные уровни наблюдаемого искрения при различных воздействиях и наведенных повреждениях

Прямые измерения уровней уязвимости реального бортового оборудования показывают в основном около нескольких сотен вольт на метр, тогда как около 5 % оборудования имеет уровень менее 100 В/м [10]. Кроме того, некоторые косвенные оценки

уязвимости авионики могут дать много меньшие уровни. Например, в соответствии с оценкой, использованной в [24], рассматривая сотовый телефон как причину 80 % обнаруженных воздействий на авионику и учитывая уровень его излучения несколько вольт на метр на нескольких метрах, можно оценивать уязвимость авионики также в несколько вольт на метр. Однако известна статистика NASA [15] по числу зафиксированных случаев воздействий от источников: 25 – сотовый телефон; 25 – ноутбук; 14 – неизвестный источник; 13 – электронная игра; 13 – магнитофон; 12 – радио; 7 – CD-плеер; 3 – пейджер; 2 – цифровой видеоплеер; по 1 – диктофон, калькулятор, телевизор, органайзер. Максимальные измеренные уровни излучения некоторых из них показаны на рис. 4.19 [15]. Таким образом, применение аналогичной оценки снижает уровень уязвимости авионики до 100 мВ/м (табл. 4.3). Но это очень низкие уровни, свидетельствующие о том, что оценка уязвимости авионики по максимальному уровню излучения приборов, приводящему к сбою оборудования, может быть некорректной.

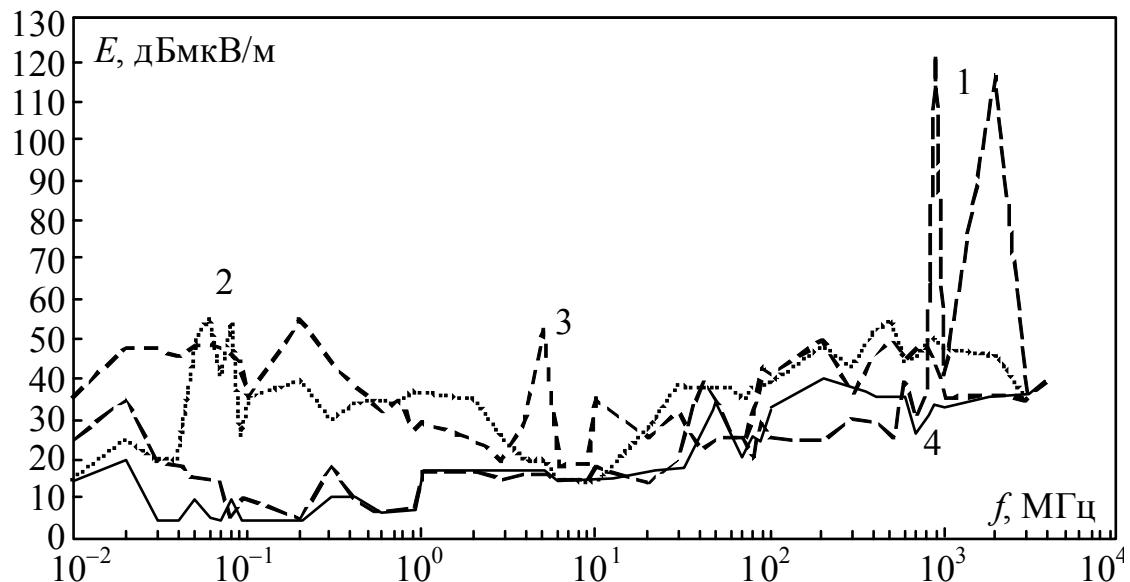


Рис. 4.19. Максимальные измеренные уровни излучения (с 1 м) сотовых телефонов (1); ноутбуков (2); камер (3); плееров (4)

Таблица 4.3

Число инцидентов из-за переносных электронных приборов и их максимальные уровни излучения, измеренные на расстоянии 1 м, в диапазоне 10 кГц–4 ГГц

Параметр	Тип переносных электронных приборов			
	Мобильные телефоны	Ноутбуки	CD-плееры	Всего
Число / % инцидентов	25/21	25/21	7/6	118/100
Максимальное излучение, В/м	≈ 1	$< 10^{-3}$	$\approx 10^{-4}$	—

Возникает естественный вопрос: как могут такие низкие уровни излучения нарушить работу авионики? Трудно ответить однозначно. Несомненный факт состоит в том, что появляются условия, при которых создаются уровни поля, приводящие к сбою оборудования.

4.6. Компоненты

Проводились исследования восприимчивости отдельных составляющих компьютерных систем к импульсному ЭМ воздействию [69]. Вероятность сбоя при облучении материнской платы ПК показана для различных импульсов на рис. 4.20, а для различных материнских плат на рис. 4.21.

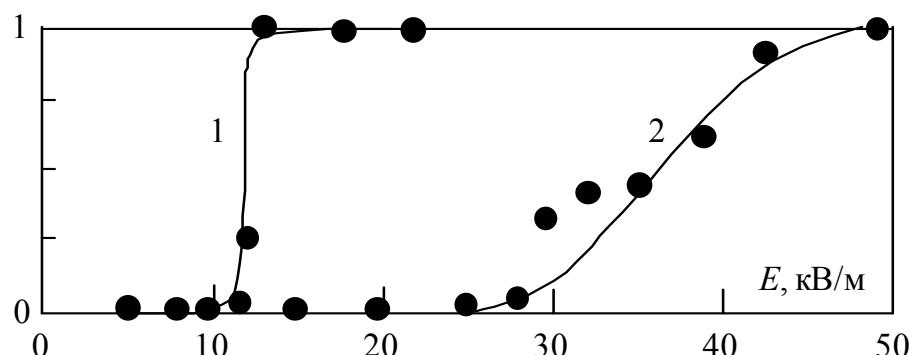


Рис. 4.20. Вероятность сбоя платы Rocky-518 HV с процессором Pentium MMX 233 МГц при облучении импульсами с временем нарастания–длительности: 100 пс–2,5 нс (1); 1,5 нс–80 нс (2)

В [70] приведены результаты испытаний двух микропроцессорных плат с процессорами Pentium и AMD 486. Кроме того, для

измерения передаточных функций была разработана обобщенная плата. Эти платы испытывались в симуляторах: на двух установках непрерывного воздействия и трёх импульсных установках с различными формами импульса.

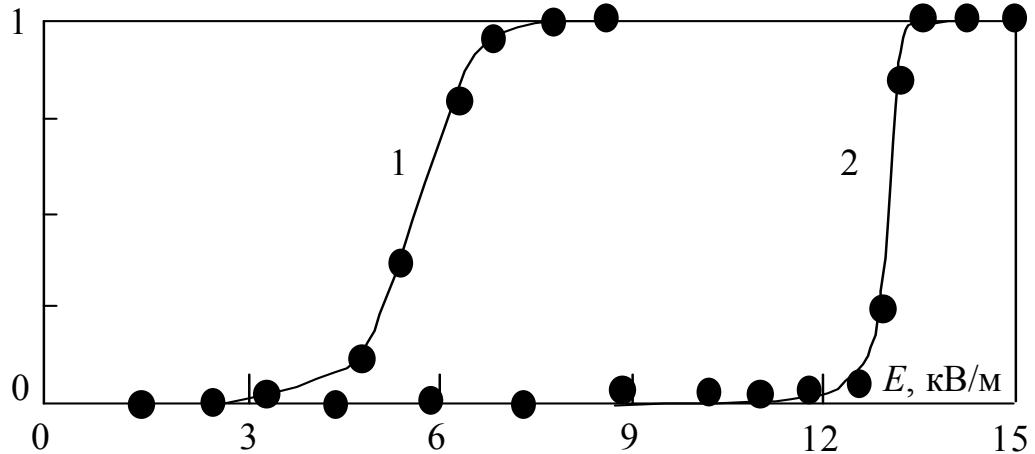


Рис. 4.21. Вероятность сбоя при облучении импульсом с временем нарастания 100 пс и длительностью 2,5 нс материнских плат SSC-5x86H DX4-S CPU 100 MHz (1) и Rocky-518 HV Pentium MMX CPU 233 MHz (2)

При оценке непрерывного воздействия частотой от 150 МГц до 2 ГГц на эти платы результаты сбоев были сведены к низкому, среднему и наивысшему уровням. Сравнивались результаты различных типов мощного микроволнового воздействия, включая вариации по длительности и частоте повторения импульсов. Две платы подвергались импульсным воздействиям: получены данные для низких и высоких частот повторения. Используя эти данные, авторы рассмотрели чувствительность плат и сравнили результаты непрерывного и импульсного воздействий. Выявлено, что эффекты уязвимости начались при непрерывных воздействиях в области 100 В/м, а при воздействии сверхширокополосных импульсов в области нескольких киловольт на метр.

В [71] рассмотрено влияние различных состояний функционирования и программы на эффекты пробоя электронных устройств (сдвиговых регистров, микроконтроллеров и персональных компьютеров) под воздействием узкополосных и сверхширокополосных импульсов (рис. 4.22).

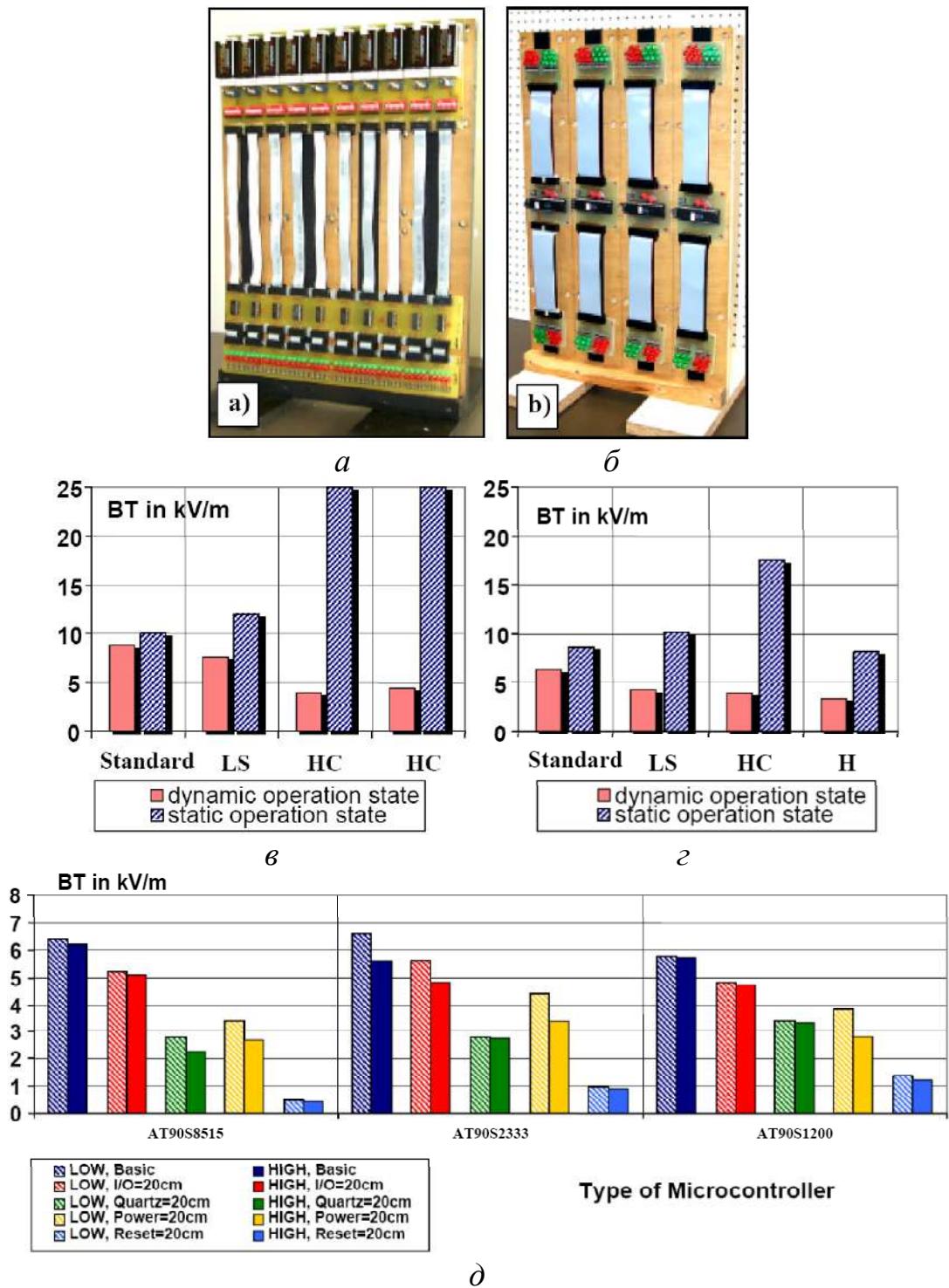


Рис. 4.22. Тестовые установки для сдвиговых регистров (а) и микроконтроллеров (б). Порог пробоя (ВТ): сдвиговых регистров четырёх различных технологий в динамическом и статическом режимах работы при длине входных линий 0 см (в) и 20 см (г); трёх микроконтроллерных систем в состояниях портов LOW и HIGH, измеренный в испытательных установках (тактовая частота 1 МГц) (д) (начало, окончание см. на с. 52)

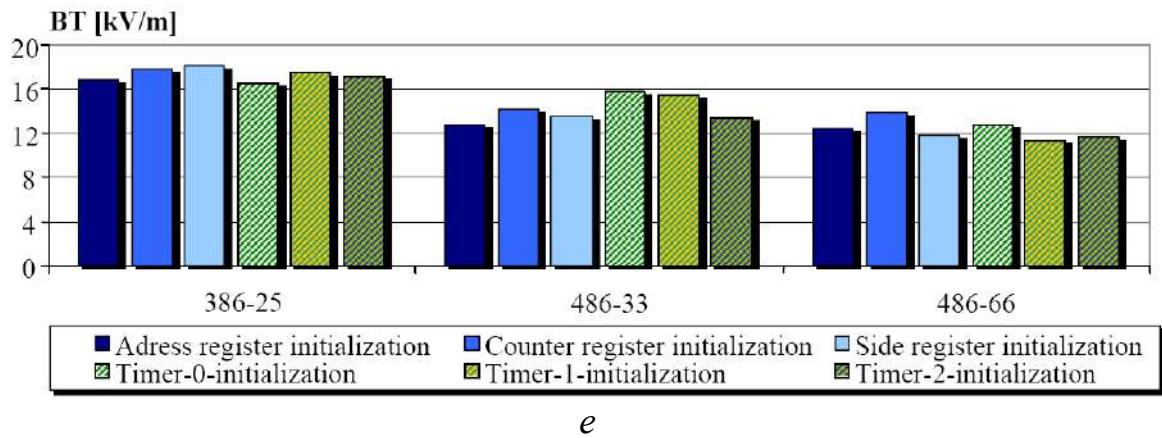


Рис. 4.22. Порог пробоя (ВТ) трех систем персональных компьютеров в шести состояниях программы (e)
(окончание, начало см. на с. 51)

В [72] исследовано влияние сверхширокополосного излучения на работу микроконтроллера с различной длиной подводящих линий (рис. 4.23).

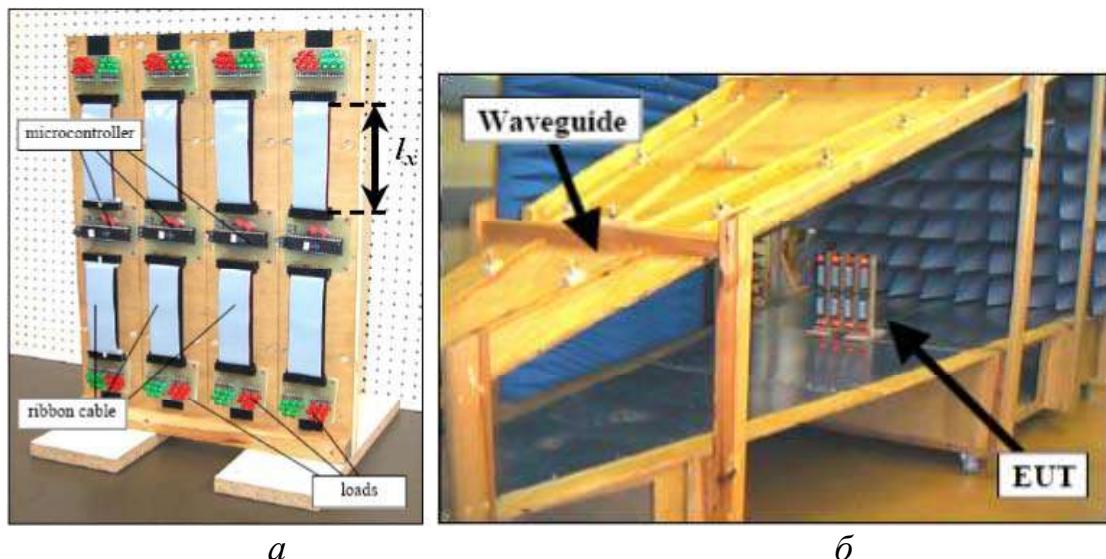


Рис. 4.23. Испытательная структура микроконтроллера:
крупно (а) и в ТЕМ-волноводе (б)
(начало, продолжение см. на с. 53)

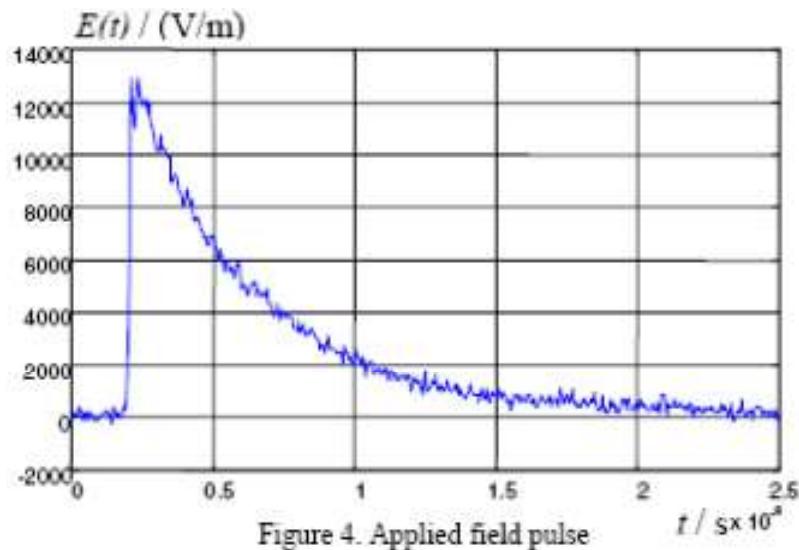
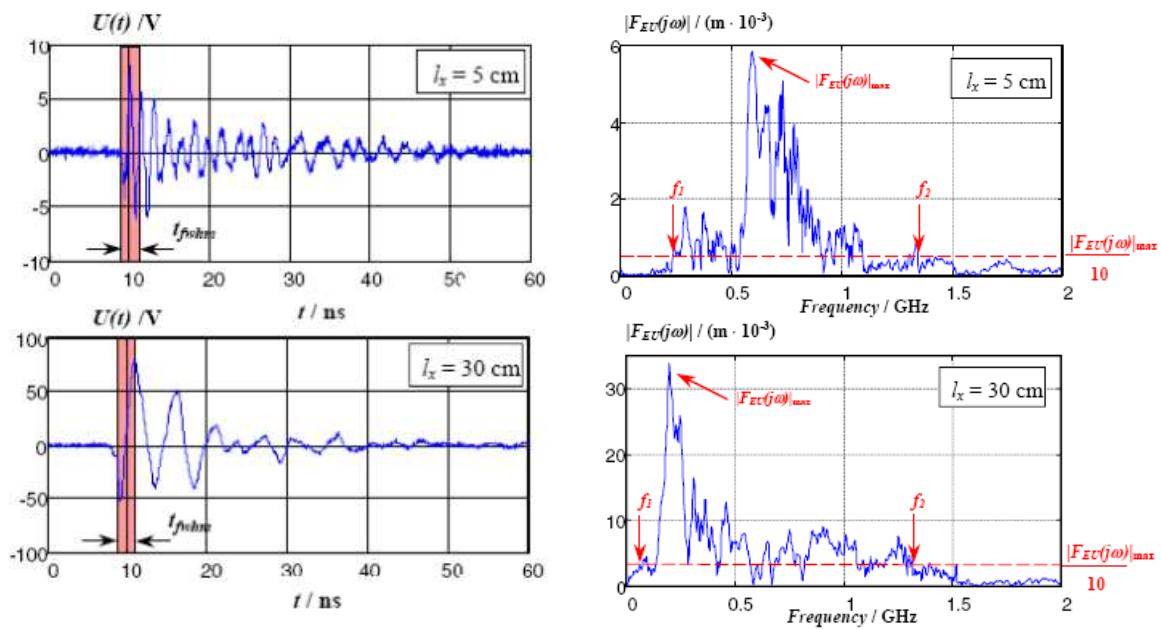


Figure 4. Applied field pulse

б



г

Рис. 4.23. Испытательная структура микроконтроллера:
форма импульса воздействующего поля (*б*); формы импульса
и передаточные функции наводки при разных длинах
гибкого кабеля (*г*) (продолжение, начало см. на с. 52,
окончание – на с. 54)

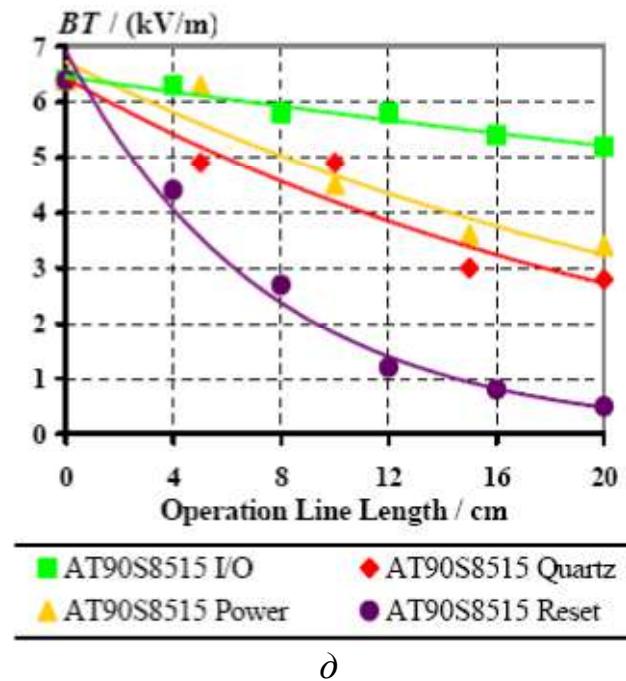


Рис. 4.23. Испытательная структура микроконтроллера:
пороги пробоя микроконтроллеров при разной длине линий (d)
(окончание, начало см. на с. 52)

В [73] выполнено исследование деструктивных эффектов (экспериментально, а также моделированием) в полупроводниковой логике (И-НЕ и НЕ), возникающих вследствие излучаемых и кондуктивных воздействий (рис. 4.24).

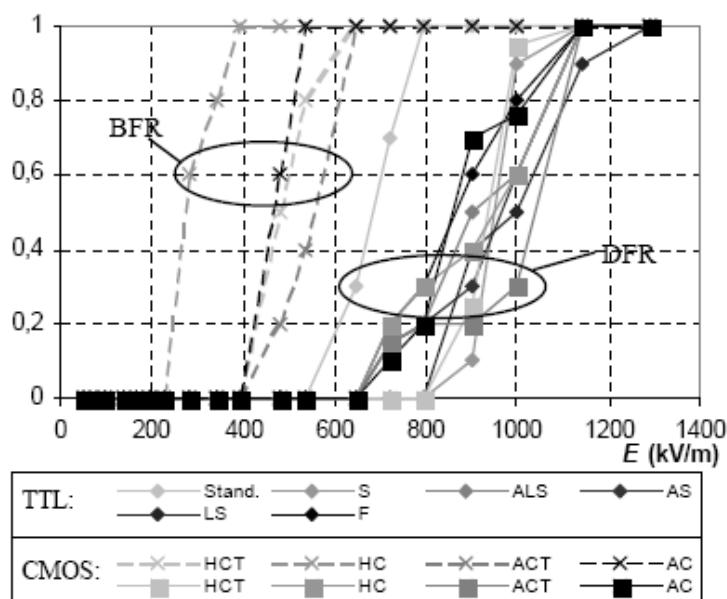
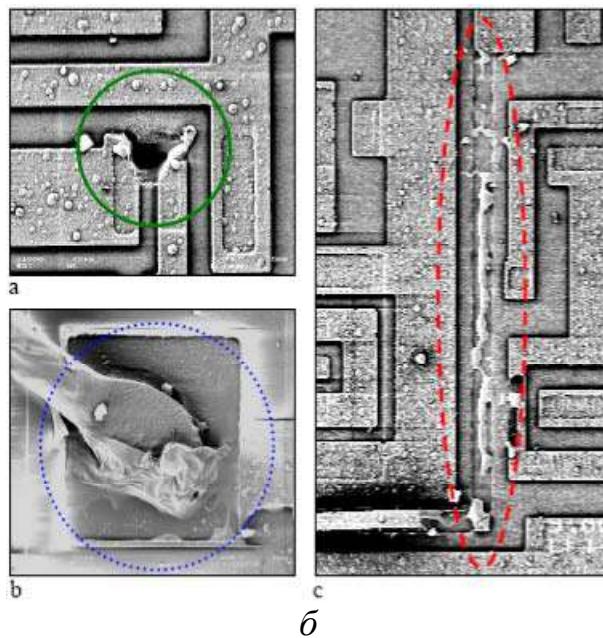
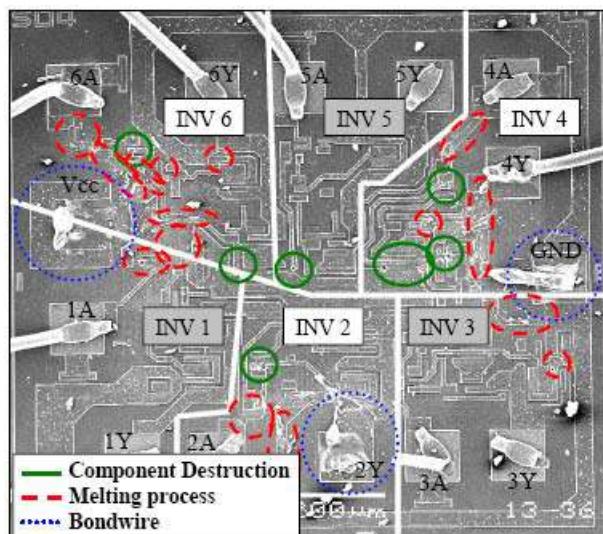


Рис. 4.24. Статистический анализ ТТЛ- и КМОП-вентилей
(начало, продолжение см. на 55)



б



б

Inverter 6	Inverter 5	Inverter 4
IN: L OUT: H	IN: H OUT: L	IN: L OUT: H
Inverter 1	Inverter 2	Inverter 3
IN: H OUT: L	IN: L OUT: H	IN: H OUT: L

г

Рис. 4.24. Деструктивные эффекты в ТТЛ-схемах (*б*);
ТТЛ-инвертор на диодах Шоттки после воздействия
электромагнитного импульса амплитудой 1090 кВ/м (*в*);
состояние системы во время воздействия импульса (*г*)
(продолжение, начало см. на с. 54, окончание – на с. 56)

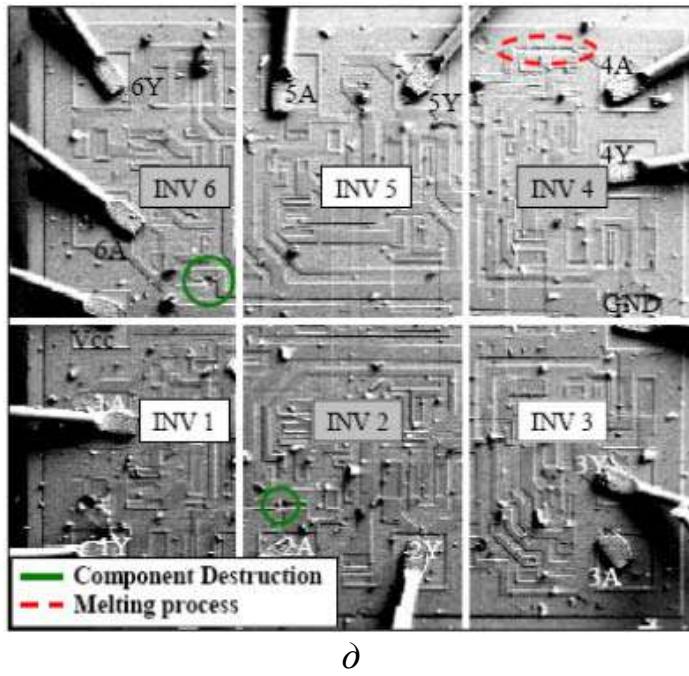


Рис. 4.24. Стандартный ТТЛ-инвертор после кондуктивного воздействия импульсом (δ) (окончание, начало см. на с. 54)

Уровни импульсного ЭМ поля со временем нарастания 2 нс и результаты его воздействия на различные сетевые кабели, подключенные к компьютеру, приведены в табл. 4.4 [69]. Результаты исследования уязвимости при кондуктивном воздействии на кабельные входы различных сетевых плат приведены в табл. 4.5 [5]. Немонотонная зависимость вероятности сбоя от числа воздействующих импульсов отмечена в [5], но ее причины не выявлены.

В [74] предложен новый метод измерения для оценки восприимчивости ИС к таким кондуктивным помехам, как импульсы EFT. Метод использован для оценки восприимчивости 8-битного микроконтроллера.

В работе французских военных, посвященной созданию электромагнитного оружия [75], рассматриваются результаты микроволнового воздействия на печатные платы в реверберационной камере. Исследовались три типа воздействий: непрерывные волны, импульсные волны и амплитудная модуляция (частоты модуляции: 100 кГц, 1 МГц, 10 МГц). Обнаружено, как и ожидалось, что непрерывное воздействие является самым действенным, а добавление амплитудной модуляции к непрерывному сигналу не оказывало влияния на пороговый уровень.

Таблица 4.4

Уровни излучения и результаты его воздействия
на различные кабели

Уровень	Результат воздействия
RG58 (10Base-2)	
>12 кВ/м	Разрушение аппаратного обеспечения
12 кВ/м	Зависание: выход связи из строя, отказы компьютеров
≤6 кВ/м	Нарушение работы, подавление: число потерянных блоков возрастает, готовность канала к связи снижается с ростом частоты повторения импульсов
≤0,53 кВ/м	Битовая ошибка: наводится импульс того же уровня, что и сигнал
S-UTP (10Base-T)	
>12 кВ/м	Разрушение аппаратного обеспечения
≥6 кВ/м	Зависание: отказы компьютеров
<6 кВ/м	Нет ошибок
S-UTP (100Base-TX)	
>12 кВ/м	Разрушение аппаратного обеспечения
12 кВ/м	Зависание: отказы компьютеров
≤6 кВ/м	Нарушение работы, подавление
≤2 кВ/м	Нет ошибок

Таблица 4.5

Число сбоев/испытаний при кондуктивном воздействии
EFT-импульсов (фронт 5 нс, ширина 50 нс) различного
напряжения на кабельные входы разных сетевых плат

10Base-T						
Частота выбросов (импульсы)	1000 В	1500 В	2000 В	3000 В	4000 В	4500 В
1000 кГц (20000)	0/7	2/5	1/5			
100 кГц (2000)	7/9		сбой при каждом испытании			
10 кГц (200)	6/8	1/3				
1 кГц (20)	0/6	2/5	3/5	6/8		
Одна серия	0/2	×	0/3	1/3	0/3	
10Base-2						
Частота выбросов	500 В	1000 В	1500 В	2000 В	2500 В	3000 В
Одна серия	1/6	3/6	3/6	4/6	сбой при каждом испытании	

Установлена энергетическая неэффективность непрерывного излучения и отмечено, что при переходе к микроволновым импульсам для оптимизации порогового уровня эффектов электроники возможно использование двух параметров импульса: частоты повторения и длительности. Например, увеличение частоты повторения от 1 до 10 кГц может уменьшить напряженность поля, требуемую для сбоя схемы, на 25 дБ, а среднюю мощность – на 15 дБ. Выявлены два различных поведения поля на границе длительности импульса около 3 мкс. Так, при длительности более 3 мкс уровень поля для сбоя почти не изменяется с ростом длительности: выигрыш лишь в 2 дБ между 3 и 100 мкс соответствует увеличению средней мощности на 12 дБ. Уменьшение длительности импульса ниже 3 мкс приводит к возрастанию напряженности поля для сбоя: на 5 дБ – от 3 до 2 мкс, соответствующа увеличению средней мощности на 3 дБ. В результате исследования авторы сделали вывод, что для оптимизации требуемой энергии при разработке электромагнитного оружия необходимо найти компромисс между длительностью импульса и частотой его повторения.

Теоретическое и экспериментальное исследование восприимчивости к излучениям MOS и BJT операционных усилителей показало, что MOS операционные усилители значительно восприимчивей в широком диапазоне частот [76].

В [77] исследованы повреждения в схемах с переключаемыми конденсаторами, вызванные радиочастотными помехами. Оказалось, что главную роль в этом играют искажения в МОП ключах в рабочем состоянии. В [78] приводятся результаты экспериментального исследования устойчивости интегрального аналого-цифрового преобразователя (АЦП) к кондуктивным помехам по цепям питания и констатируется, что она определяется устойчивостью мультивибратора, управляющего преобразователем напряжения в частоту, входящего в состав АЦП.

Исследования защищенности передатчиков различных Bluetooth (рис. 4.25) показали, что сбои начинаются с напряженности поля 10 В/м (для одного случая – с 5 В/м), а с 50 В/м диапазон частот уязвимости значительно расширяется [79].

В [80] представлены результаты экспериментального исследования стойкости БИС и печатной платы по цепям питания (рис. 4.26).

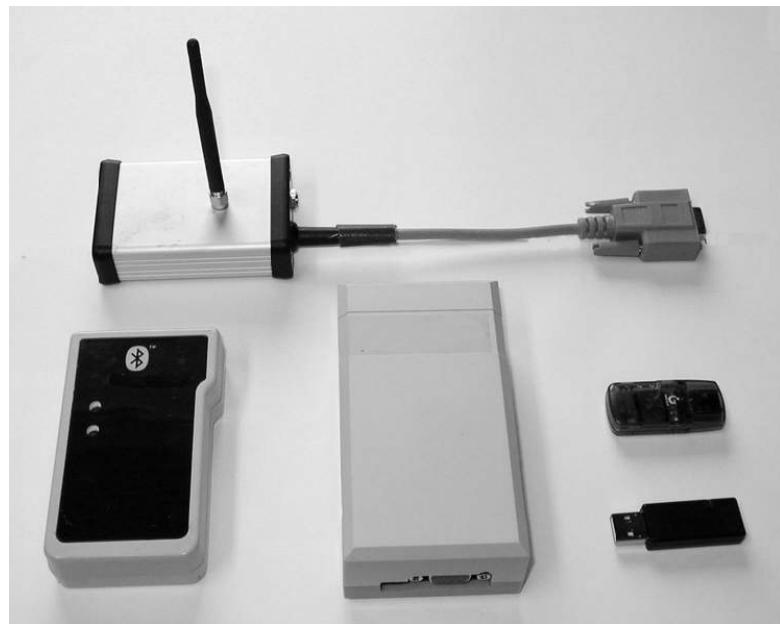


Рис. 4.25. Испытанные модули Bluetooth

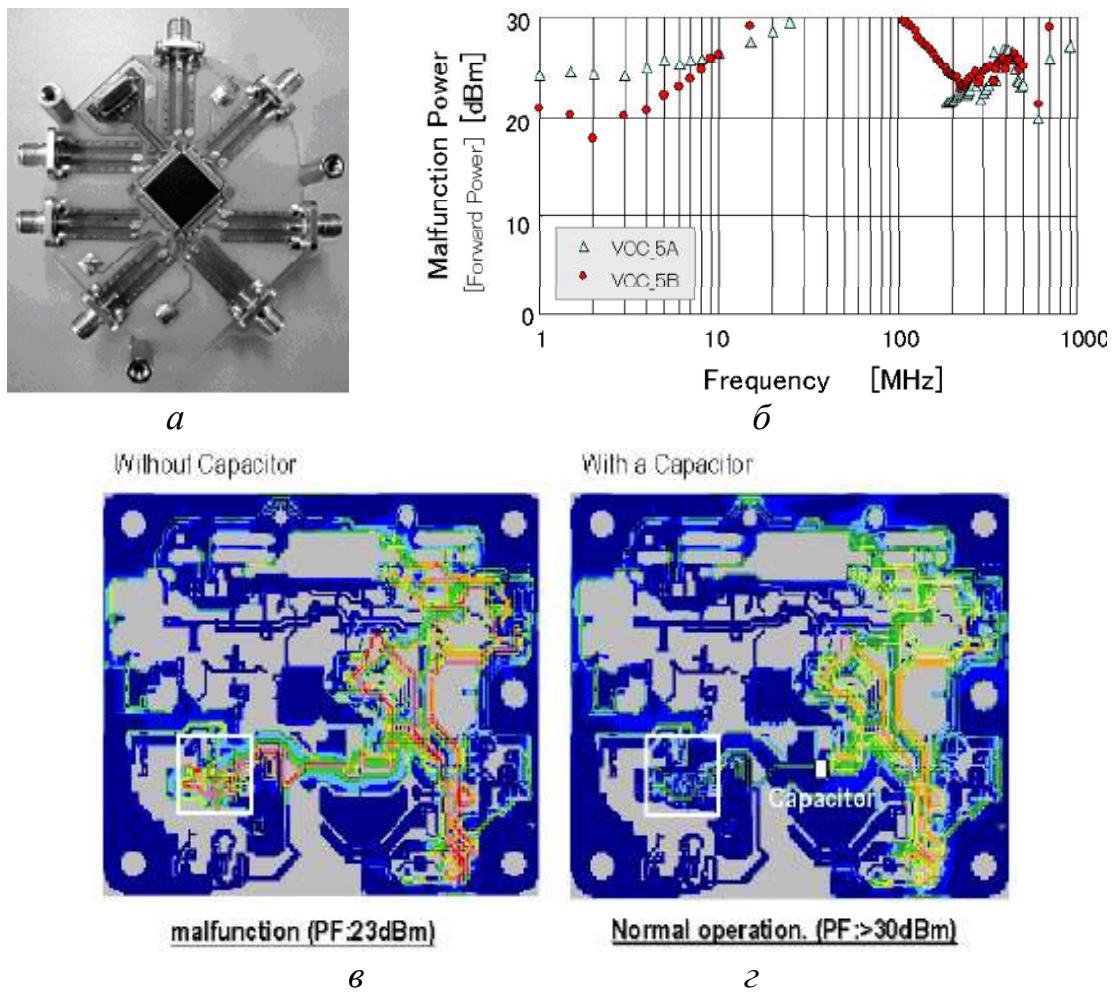


Рис. 4.26. Испытательный макет для БИС (а); мощность сигнала, приводящего к сбою по цепям питания 5 В для двух (А, В) контактов (б); анализ распределения тока в наиболее уязвимой цепи на печатной плате (в) и повышение стойкости установкой конденсатора (г)

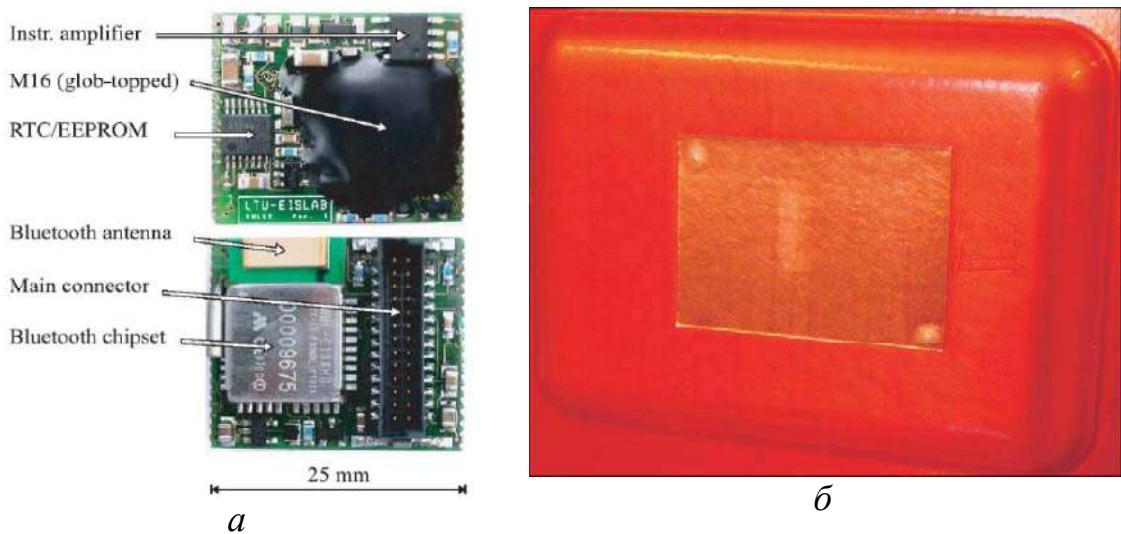
В исследовательской работе «Восприимчивость электроники к электромагнитному импульсу и сверхширокополосным воздействиям», выполненной по заказу Научного института защитных технологий Вооруженных сил Германии (ABC-Protection, Munster), изучена восприимчивость КМОП-схем [81]. Все деструктивные эффекты классифицируются на разрушения компонентов, внутричиповых проводов и подводящих проводов. Сначала на низких амплитудах поля происходит разрушение компонентов большей частью в результате эффектов пробоя. Если амплитуда возрастает, появляются разрушения внутричиповых проводов. Дальнейшее возрастание амплитуды ведет к дополнительным разрушениям подводящих проводов и многочисленным разрушениям компонентов и внутричиповых проводов. В этом же исследовании выполнена классификация по местам разрушения. Сначала на низких амплитудах поля происходит разрушение входных цепей защиты КМОП-приборов. Если амплитуда возрастает, появляются дополнительные разрушения выходных цепей. Дальнейший рост амплитуды ведет к разрушению непосредственно внутри электронной схемы (между входными и выходными цепями).

В [82] обсуждается и экспериментально исследуется уязвимость сенсорных сетей, которые могут стать частью критических систем в будущем (рис. 4.27).

В [83] рассмотрен тепловой перенос в полупроводниковых интегральных схемах при воздействии мощного внешнего электромагнитного импульса и показано, что только определенные составляющие теплопроводности влияют на значения тепловых градиентов, которые вызывают повреждения, и что учет температурной зависимости теплопроводности подложки интегральной схемы уменьшает значение температуры, до которой нагревается кристалл.

В [84] исследуется электрический пробой микрополосковых межсоединений и копланарных компонентов в результате воздействия мощных электромагнитных импульсов. Предложены и описаны эффективные методологии быстрой оценки максимальной плотности тока, протекающего по подводящему проводу; напряженности электрического поля, приводящего к пробою тон-

копленочных конденсаторов; средней и пиковой предельной мощности традиционных и тонкопленочных микрополосковых и копланарных линий.



SUMMARY OF IEMI INDUCED EFFECTS FOR THE SENSOR NETWORK

<i>Frequency [GHz]</i>	<i>E-field level [kV/m]</i>	<i>Comment</i>
2.25	0.13	Visible temperature rise
	0.29	Max level: ~ 7 °C temperature rise
2.45	0.20	First visible data loss
	0.22	Loss of contact at one Test occasion
	0.25	Max level: visible data loss
2.47	0.60	Microwave oven test: ~ 20 °C temperature rise

Рис. 4.27. Пример узла сенсорной сети (MULLE) (а); материалы ламинированной инкапсуляции со встроенными антеннами (б); сводка влияний ПЭМП на сенсорную сеть

Повреждение вызывается, как правило, тепловыми эффектами из-за рассеяния тепла; некоторые результаты воздействий мощных микроволн на автомобиль описываются в [53]. Сбой появляется, когда ложные наведённые сигналы нарушают правильную работу схемы; описание различных аспектов сбоев можно найти в [5, 69, 85]. Одной из основных причин отказа всей систе-

мы является выход из строя полупроводникового прибора [86]. Модель Вунша – Белла дает адекватную оценку энергии, достаточной для теплового повреждения полупроводникового прибора, в зависимости от длительности микроволнового импульса (более 100 нс). Однако при уменьшении длительности импульса от 100 до 5 нс происходит значительное снижение (примерно в 10 раз) энергии повреждения [87], показывающее, что именно электрическое поле, а не тепло является главной причиной повреждения. Результаты экспериментальных исследований воздействий микроволнового излучения на различные полупроводниковые диоды выявили следующее [25].

1. Влияние мощных микроволн на диоды может проявиться не только в сбое из-за последствий детектирования воздействующего сигнала и в неустранимом повреждении диода из-за рассеяния тепла, но и в ряде промежуточных эффектов, вызываемых значительными изменениями характеристик диодов именно из-за воздействия электрического поля, а не тепла. (Например, прямое и обратное напряжения могут значительно снизиться; ёмкость может увеличиться примерно в 3 раза.)

2. Интенсивность мощных микроволн определяет степень изменений параметров, а также время (до двух суток) возврата к прежнему состоянию до облучения (исключая неустранимое повреждение после облучения с критической интенсивностью).

3. Рост числа воздействующих импульсов мощных микроволн вызывает не монотонное уменьшение, а периодическое возрастание и убывание напряжения, выпрямленного диодом (рис. 4.28).

Последний факт находится в соответствии с периодическим поведением аналогичной зависимости, представленной в [88] (рис. 4.29), что может помочь объяснить немонотонную зависимость вероятности сбоя от числа воздействующих импульсов (см. табл. 4.5). Можно предположить, что это связано с начинаяющимися процессами лавинной генерации носителей заряда в локальных областях переходов полупроводниковых приборов, а также локального выжигания переходов на их неоднородностях шнуровыми токами.

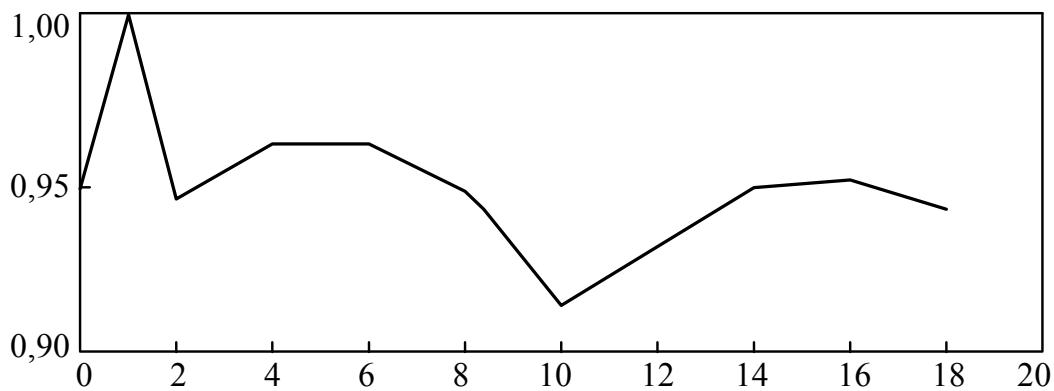


Рис. 4.28. Зависимость нормированной амплитуды напряжения с нагрузки детектора от числа воздействующих импульсов в пачке

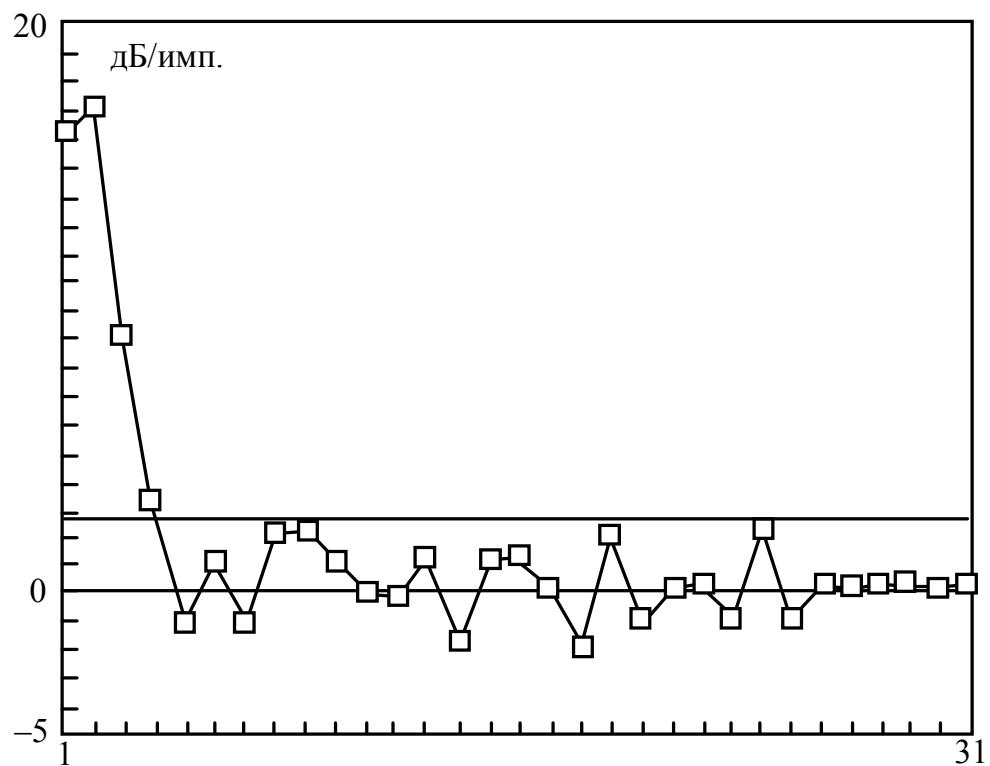


Рис. 4.29. Зависимость изменения потери преобразования смесителя от числа воздействующих импульсов

4.7. Разное

В [89] описываются испытания системы противоторпедной защиты (рис. 4.30) и приводятся его результаты (табл. 4.6).



Рис. 4.30. Система противоторпедной защиты военных кораблей в испытательной лаборатории

Рассматривается возможность срабатывания электровзрывателя из-за облучения полем на примере английской ракеты MILAN FIELD OVERSOCK MK 4, сравниваются стандарты ее испытаний, показана структура экранирующих тканей для ее защиты (рис. 4.31) [90].

В работе специалистов из Шведского агентства оборонных исследований [91] показывается возможность аппроксимации аддитивным белым гауссовым шумом при оценке результирующей вероятности битовых ошибок не только периодических импульсных помех с фиксированной амплитудой, но и более общих импульсных помех со случайными амплитудой и временем прихода при использовании статистик высшего порядка для оценки качества такой аппроксимации. Примечательно, что актуальность этого исследования вызвана все большим использованием гражданской электроники в военных целях из-за сокращения оборонного бюджета и перехода Вооруженных сил Швеции к обороне на основе сетевой центрированной борьбы (Network Centric Warfare).

Таблица 4.6

Результаты испытаний (N/A – не проводилось)

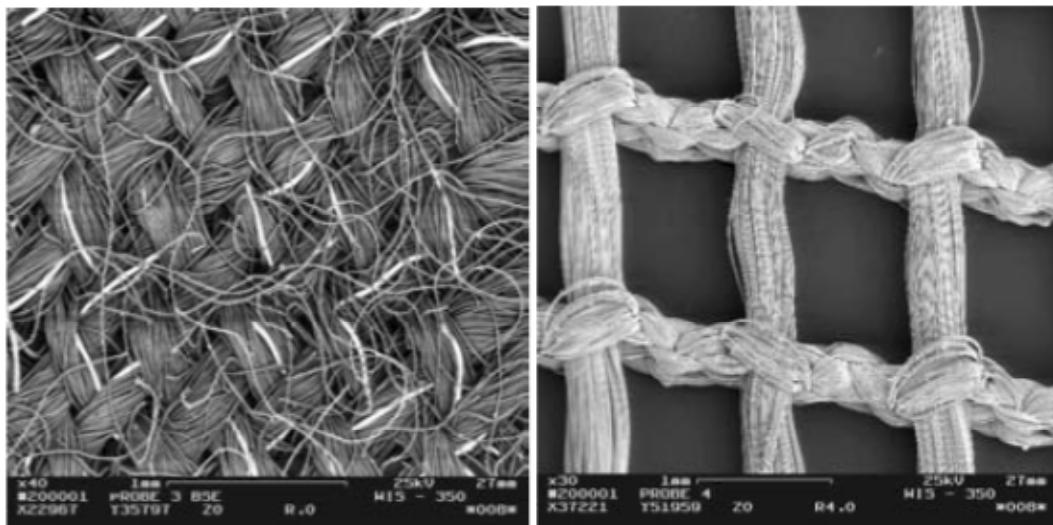
Kind of the test	Test result		
	Jammer	C&C Console	Launcher
AECTP 500, NCS 12; EN 61000-4-2	Passed	Passed	Passed
AECTP 500, NCS 08; EN 61000-4-4	N/A	Passed	Passed
EN 61000-4-5	N/A	Passed	N/A
EN 61000-4-8	Passed	Passed	Passed
EN 61000-4-9	Passed	Passed	Passed
MIL-STD-461E, RS-101; NO-06-A500, PRS-02	Passed	Passed	Passed
MIL-STD-461E, CS-114; NO-06-A500, PCS-06	N/A	Passed	Passed
EN 61000-4-11 NO-06-A104	N/A	Passed	N/A
MIL-STD-461E, RE-102; NO-06-A500, PRE-02	N/A	Passed see fig 6	N/A
MIL-STD-461E, CE-102; NO-06-A500, PCE-02	N/A	Passed see fig 7	N/A
N/A – non applicable			

*a*Рис. 4.31. Экранированные и неэкранированные ракеты MILAN (*a*) (начало, окончание см. на с. 66)

Table 3. Comparison between MIL STD 464 and STANAG

Frequency (Hz) Title	Environment (V/m – rms)		
	STANAG4234		MIL STD 464
	Comm.	Radar	Average
10 k – 525 k	300	-	200
525 k – 32 M	200	-	200
32 M – 150 M	61.4	-	200
150 M – 225 M	61.4	194.2	270
225 M – 400 M	61.4	137.3	240
400 M – 700 M	61.4	137.3	750
700 M – 790 M	61.4	137.3	240
790 M – 1000 M	61.4	614	610
1 G – 2 G	-	614	1000
2 G – 2.7 G	-	614	850
2.7 G 3.6 G	-	614	1230
3.6 G – 4 G	-	614	850
4 G – 5.4 G	-	614	610
5.4 G – 5.9 G	-	614	1230
5.9 G – 6 G	-	614	610
6 G – 7.9 G	-	614	670
7.9 G – 8 G	-	614	810
8 G – 14 G	-	614	1270
14 G – 18 G	-	614	614
18 G – 40 G	-	194.2	750

δ



ε

Рис. 4.31. Сравнение уровней восприимчивости двух стандартов (*δ*); экранирующие ткани с вплетенным проводом и с металлическим покрытием (*ε*) (окончание, начало см. на с. 65)

В [92] исследованы статистические характеристики беспроводных сетей при воздействии ПЭМП. В [93] на конкретном примере выполнена оценка защищенности электронного модуля от внешних электромагнитных помех, использующая передаточные функции. В [94] рассматривается проблема блокирования суперрегенеративных и супергетеродинных приемников (рис. 4.32) приборов ближнего действия (парковочных радаров, систем дистанционного управления) из-за сильных сигналов на соседних частотах. Обнаружено, что некоторые из имеющихся на рынке приборов могут быть непригодными для использования в текущем спектре, в частности большинство суперрегенеративных приемников может испытывать проблемы в присутствии сильных внеполосных сигналов. Даны детальные рекомендации по совершенствованию и тех и других приемников.

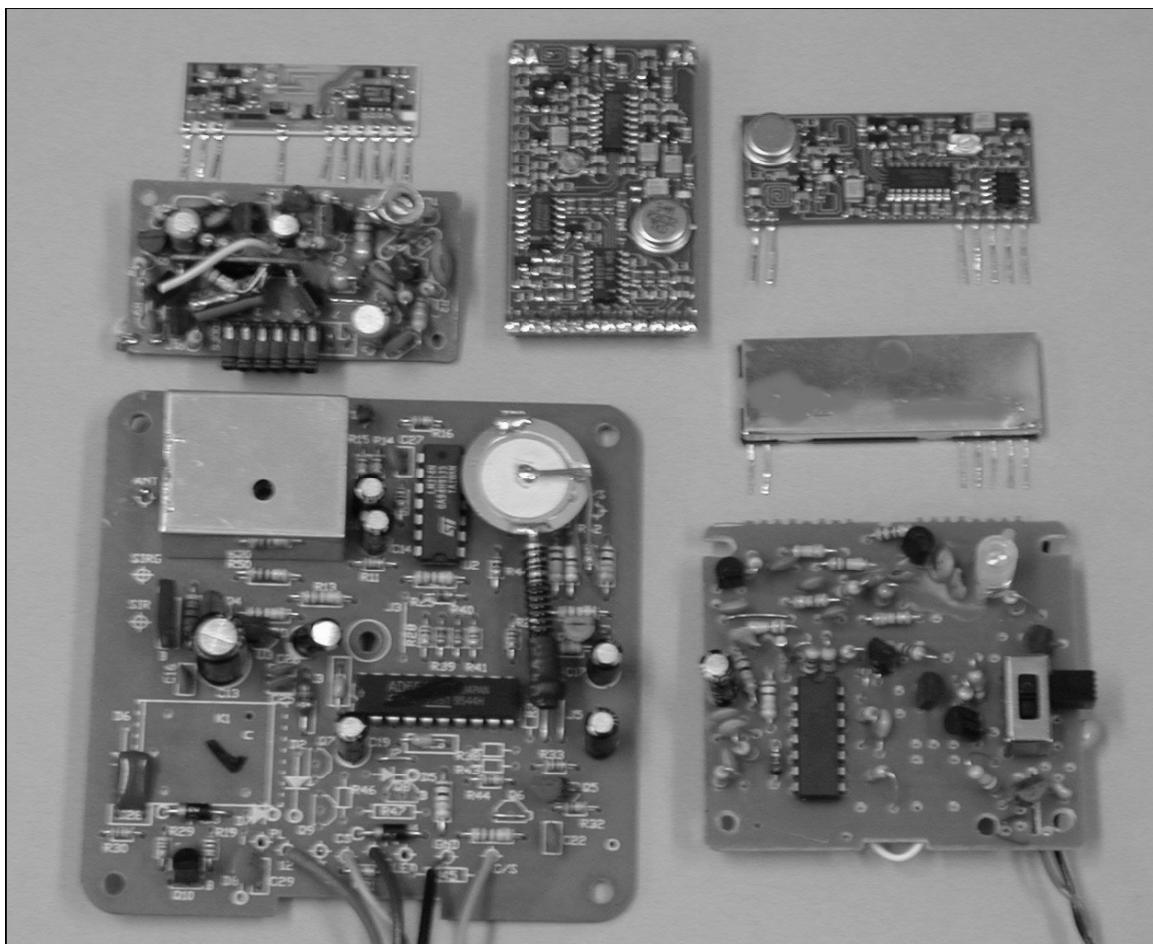


Рис. 4.32. Типичные приемники приборов ближнего действия

5. Ослабление или усиление электромагнитных воздействий

Имея представление о порядках ЭМ воздействий и уровнях уязвимости типового оборудования, естественно рассмотреть возможности ослабления этих воздействий. Известным способом ослабления ЭМ воздействий является экранирование. Однако даже в случае полностью замкнутых металлических поверхностей поле внутри может быть больше, чем снаружи, например в 3 раза, для электрического поля в центре полой сферы на резонансной частоте [95]. Между тем эффективность экранирования корпуса оборудования существенно снижается из-за щелей в корпусе. Чтобы оценить порядок величины возможного ослабления ПЭМП для наихудшего случая, рассмотрим некоторые образцы типовых корпусов. Например, измеренное отношение электрического поля внутри металлического корпуса с щелями к полю без корпуса в частотном диапазоне 1–6 ГГц изменяется от –60 дБ до более 0 дБ при среднем значении около –20 дБ (рис. 5.1) [24]. Средняя эффективность экранирования корпуса компьютера, измеренная в реверберационной камере, уменьшается в диапазоне частот 1–6 ГГц приблизительно от 20 до 10 дБ, сохраняясь почти постоянной около 10 дБ вплоть до 18 ГГц и даже уменьшаясь почти до 6 дБ на некоторых частотах (рис. 5.2) [96].

Обратимся к ослаблению ЭМ поля корпусом автомобиля. Результаты моделирования дают среднее значение около –60 дБ/В/м, а максимальное значение доходит до –25 дБ/В/м (рис. 5.3) [24].

Пример других результатов, полученных для аналогичного случая, дает среднее значение около –40 дБ/В/м и максимальное значение выше –20 дБ/В/м (рис. 5.4) [97]. Это означает, например, для внешнего поля 1 кВ/м среднее напряжение на нагрузке 50 Ом около 10 В и максимальное – выше 100 В.

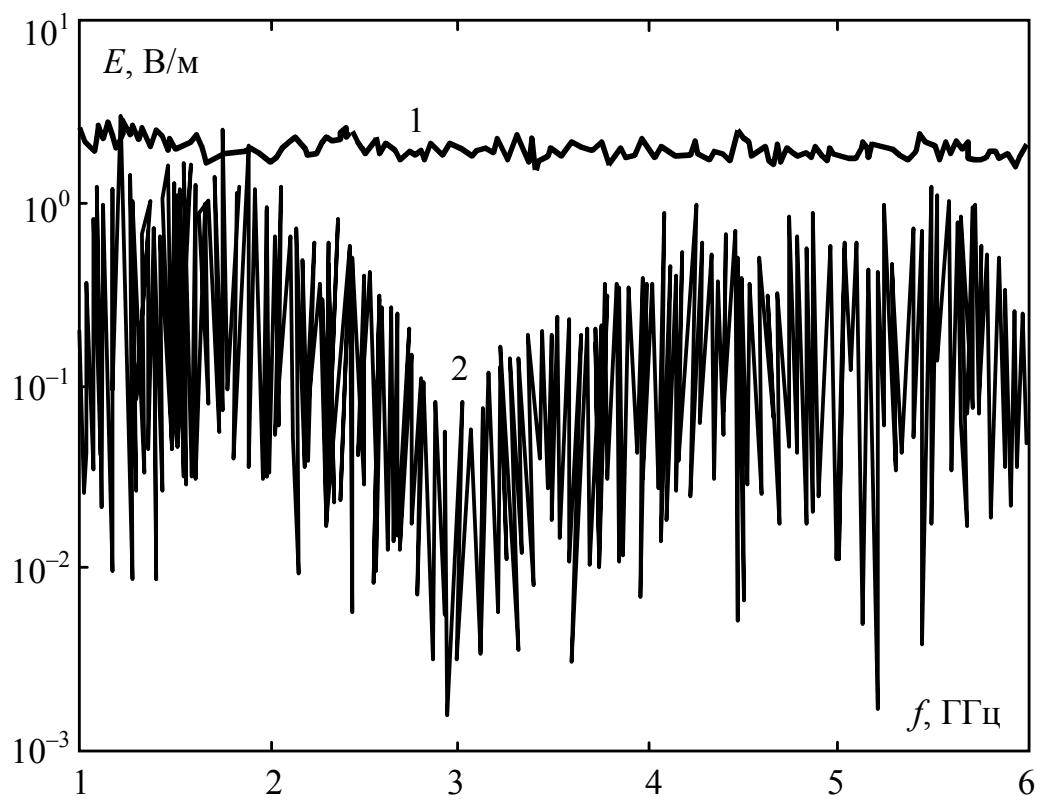


Рис. 5.1. Измеренное ЭМ поле снаружи (1) и внутри (2) металлического корпуса с щелями

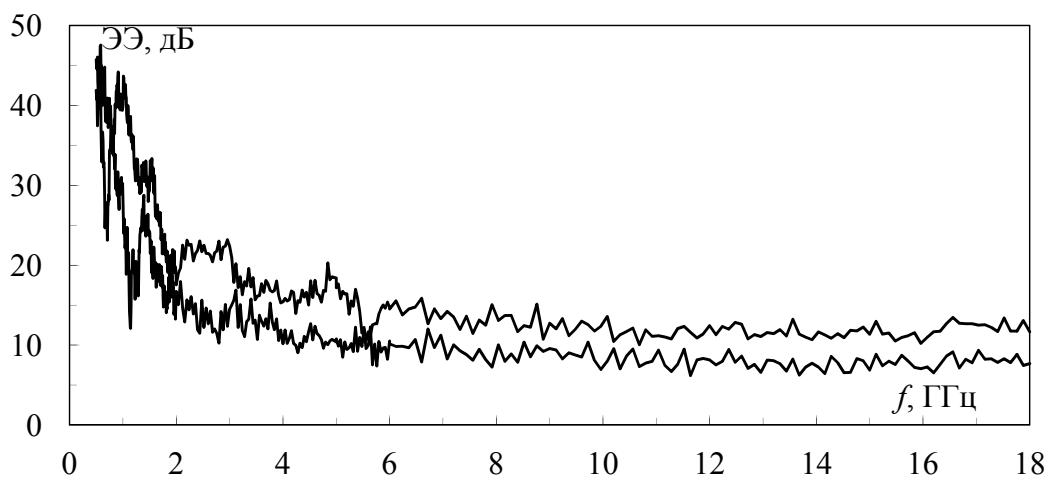


Рис. 5.2. Частотная зависимость средней эффективности экранирования компьютера

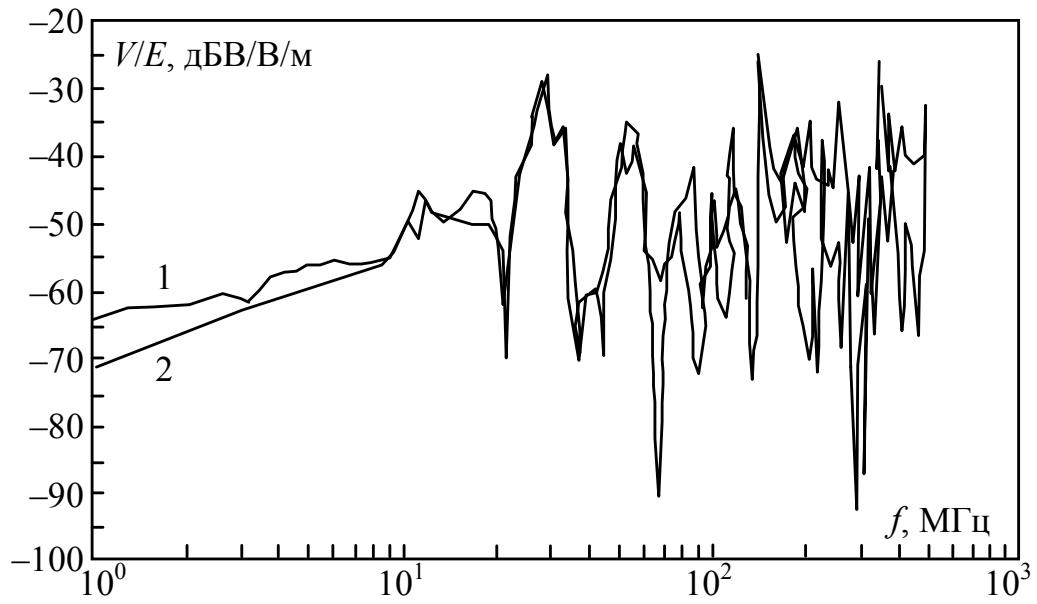


Рис. 5.3. Измеренное (1) и вычисленное (2) отношения напряжения на 50-омной нагрузке двухпроводной линии внутри автомобиля к напряжённости влияющего электрического поля

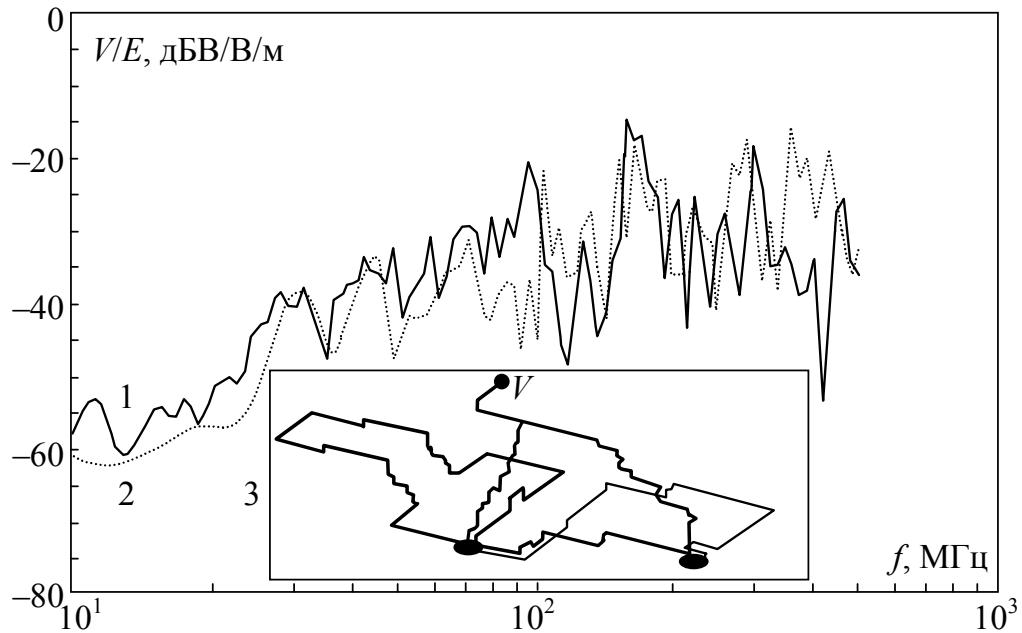


Рис. 5.4. Моделирование наводки внутри автомобиля от внешнего ЭМ поля: измерения (1); вычисления (2); структура разводки (3)

Обратимся к результатам измерения ослабления ЭМ поля фюзеляжем летательных аппаратов (табл. 5.1) [10]. Числовые значения невелики: 20–30 дБ вдоль фюзеляжа и 7–15 дБ у кабины самолёта. Самое низкое значение эффективности экранирования для испытываемых самолетов составило 0 дБ, а на некоторых из

вертолетов (с фюзеляжем из непроводящих материалов) наблюдался эффект повышения напряженности поля за счет отражений и резонанса. Измеренные ослабления сигнала достигали минус 6 дБ [10]. Следовательно, можно предположить, что если внешнее поле способно усилить поле внутри фюзеляжа, то внутренний источник может создать внутри фюзеляжа (как резонатора) намного более сильные поля.

Таблица 5.1
Минимальное ослабление в диапазоне 12,5–15 ГГц (дБ)

Часть самолета	DC-10	Boeing 747-236B
Носовая	7	15
Передняя	20	31
Средняя	26	31

Одним из критичных объектов является больница. В [98] приведены результаты измерений ослабления, обусловленного различными стенами и помещениями, в нескольких больницах для восьми дискретных частот в диапазоне от 42,6 до 5,2 ГГц.

В [99] предложена новая концепция экранированных корпусов на основе недорогих сдвоенных радиаторов из экструдированного алюминия.

Очевидно, что ПЭМП не посредством излучения, а по проводникам могут повлиять гораздо сильнее. Короткие импульсы легко распространяются по сети питания, например от трансформаторной подстанции на улице до блока питания компьютера, находящегося в комнате большого здания (рис. 5.5, 5.6) [100].

Часто полагают, что можно защититься традиционным устройством бесперебойного питания, однако оно само весьма подвержено деструктивному воздействию [6]. Грамотно построить защиту при укорочении импульсов, действующих по проводникам, непросто. Так, результаты экспериментального исследования напряжения срабатывания различных защитных приборов показывают его существенный рост относительно заявленного производителем [101] (рис. 5.7). Например, для традиционных газовых разрядников оно возрастает с 250 до 800 В, а с определен-

ногого порога разряд и вовсе не наступает, т.е. прибор не защищает.

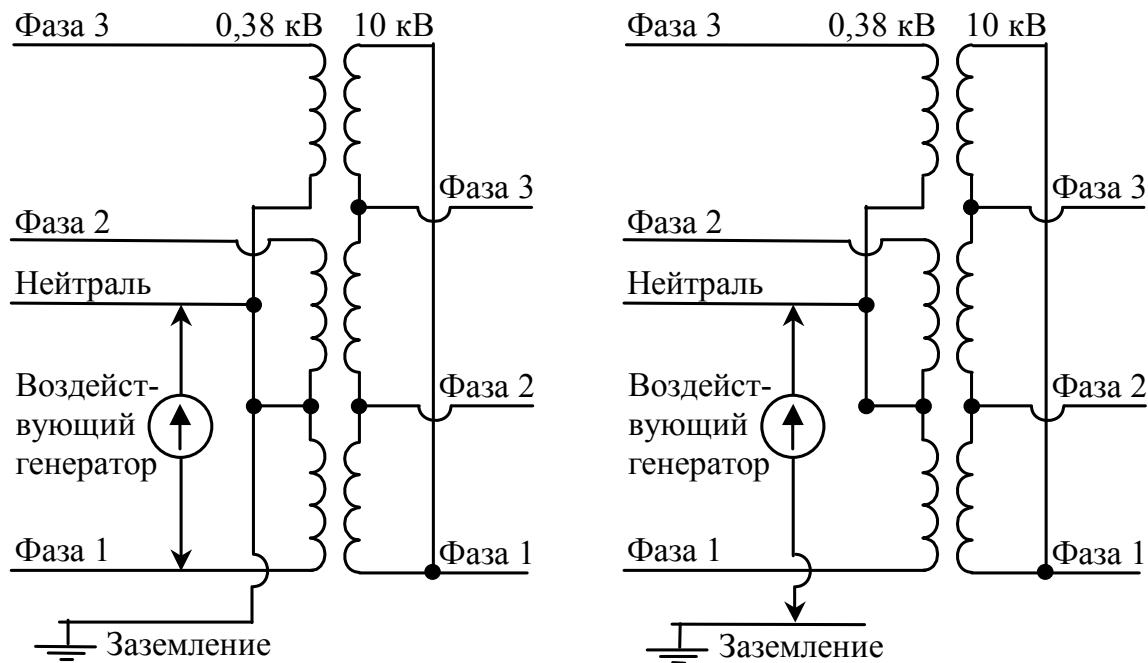


Рис. 5.5. Воздействие на цепи «фаза – нейтраль» (слева) и «нейтраль – земля» (справа)

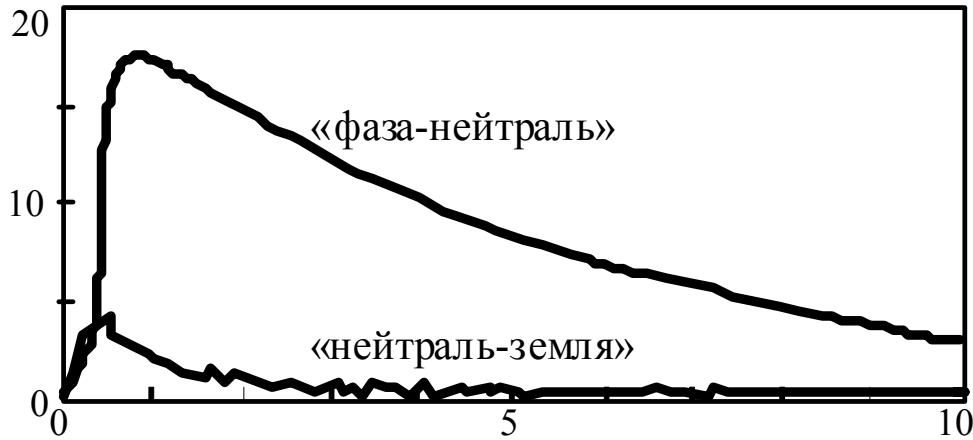
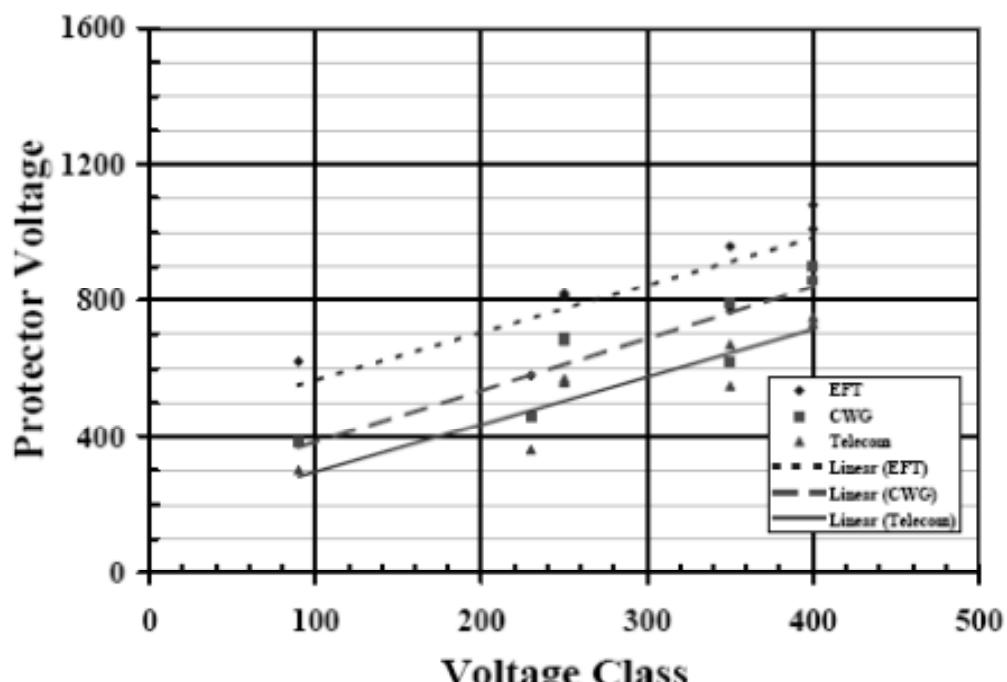
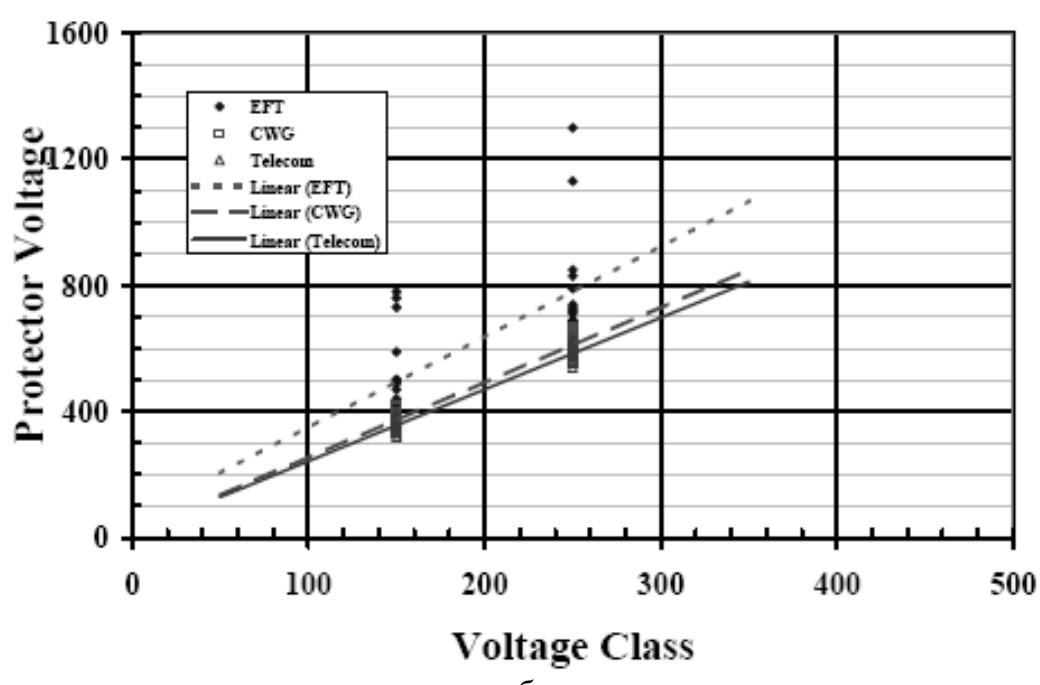


Рис. 5.6. Форма напряжения (кВ, мкс) на входном разъёме прибора при воздействиях (импульс амплитудой 20 кВ со временем нарастания 1 мкс и затухания 10 мкс) на цепи «фаза – нейтраль» и «нейтраль – земля»

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.



a



б

Рис. 5.7. Зависимости реального напряжения срабатывания относительно заявленного: *а* – для трехэлектродных газовых разрядников; *б* – для металлооксидных варисторов (начало, окончание см. на с. 74)

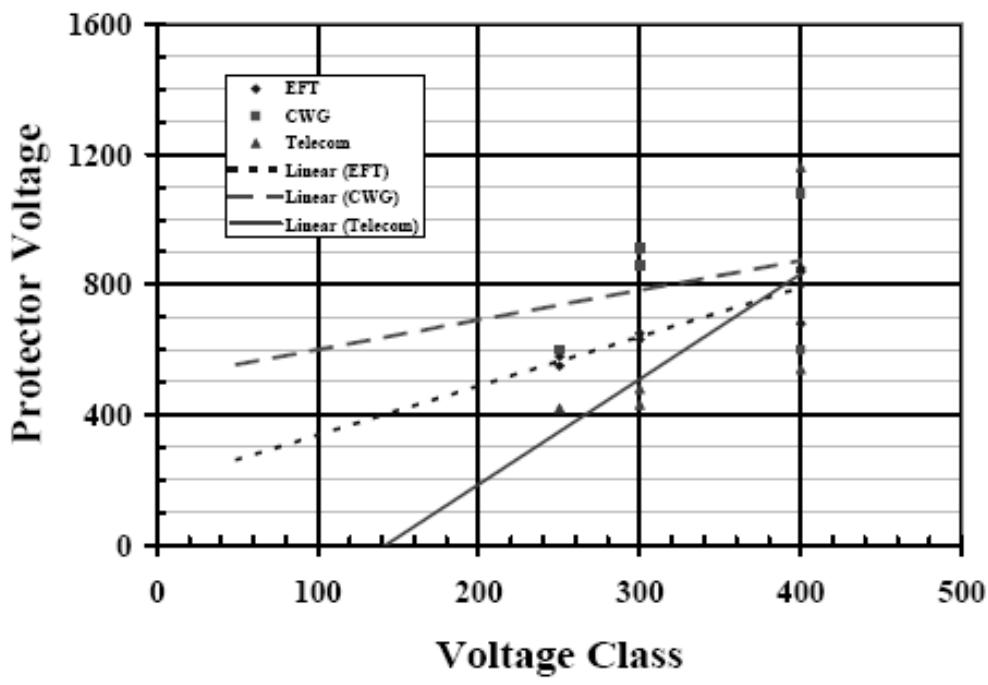


Рис. 5.7. Зависимости реального напряжения срабатывания относительно заявленного: ϑ – для TVS-диодов
(окончание, начало см. на с. 73)

Так, при испытании импульсами начальное напряжение у газоразрядных защитных приборов больше, чем у варисторов [102]. Например, при воздействии импульса с фронтом/спадом 5/100 нс амплитудой 2,5 кВ на разрядник с номинальным напряжением разряда для постоянного тока 90 В начальный пик напряжения превысил 1 кВ.

Ослабление кондуктивных ПЭМП без специальных мер (фильтры, разрядники, варисторы и т.п.) осуществляется только длиной кабеля от места воздействия до интересующего устройства. На рис. 5.8 приведены результаты ослабления стандартных EFT-импульсов типовым сетевым кабелем. Как видно, импульсы довольно хорошо распространяются по кабелю, поскольку изменение его длины от 3 до 30 м ослабляет их менее чем в 2 раза [5].

В [103] представлены результаты влияния места расположения (рис. 5.9) датчиков поля, созданного молнией: увеличение электрического поля на крыше здания в 1,7–1,9 раза и уменьшение в 5–20 раз на земле в 2 м от здания.

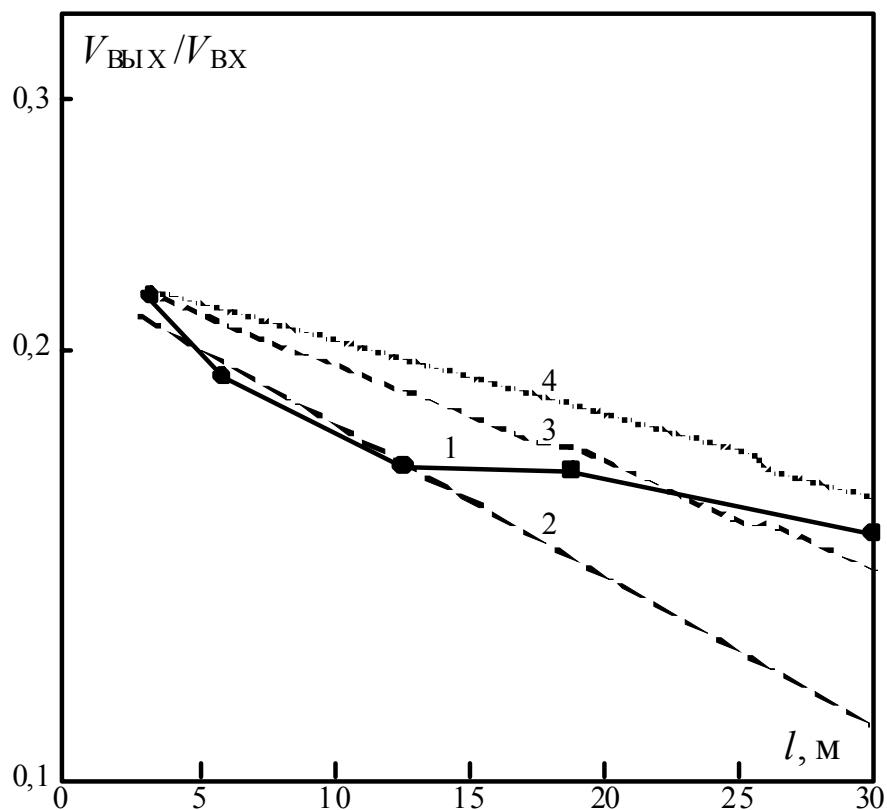


Рис. 5.8. Измеренные (1) и вычисленные при $Z/R=20$ (2), 30 (3) и 40 (4) ослабления EFT-импульсов кабелем 10Base-T (5-й категории) в зависимости от его длины

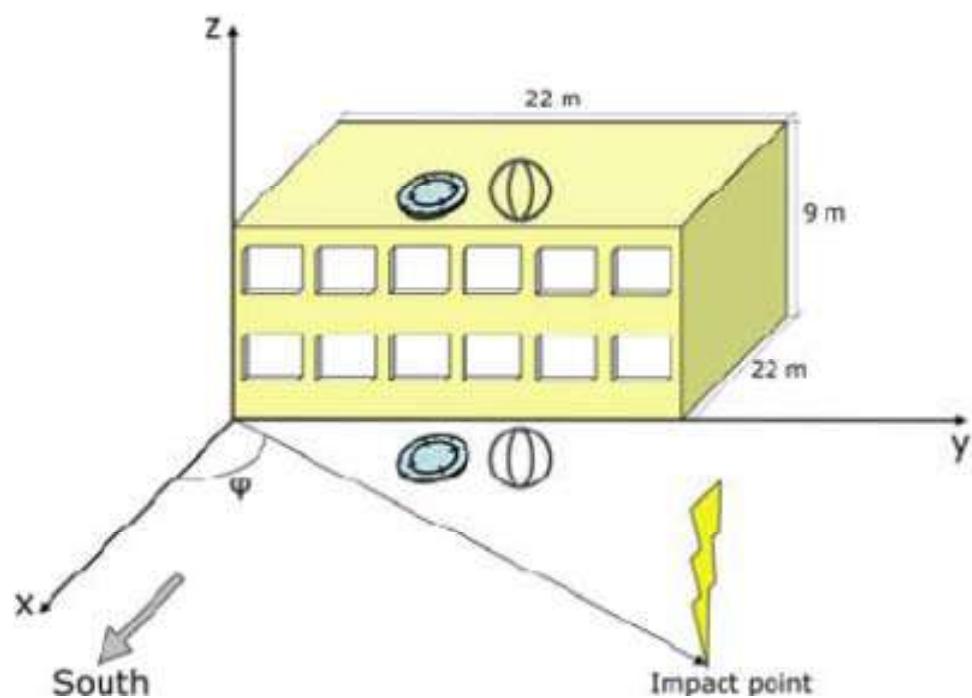


Рис. 5.9. Расположение датчиков поля на здании. Один набор расположен на земле в 2 м от южного фасада здания, а второй идентичный набор расположен на крыше здания (масштаб не сохранен)

Результаты исследования ослабления мощного микроволнового воздействия по пути распространения до цели с многочисленными данными коэффициентов распространения при различных параметрах среды представлены в [104].

Результаты исследования наводок на различных кабелях в системе, имитирующей наводки от протекания тока молнии (рис. 5.10) в фюзеляже самолета, представлены в [105] (рис. 5.11).

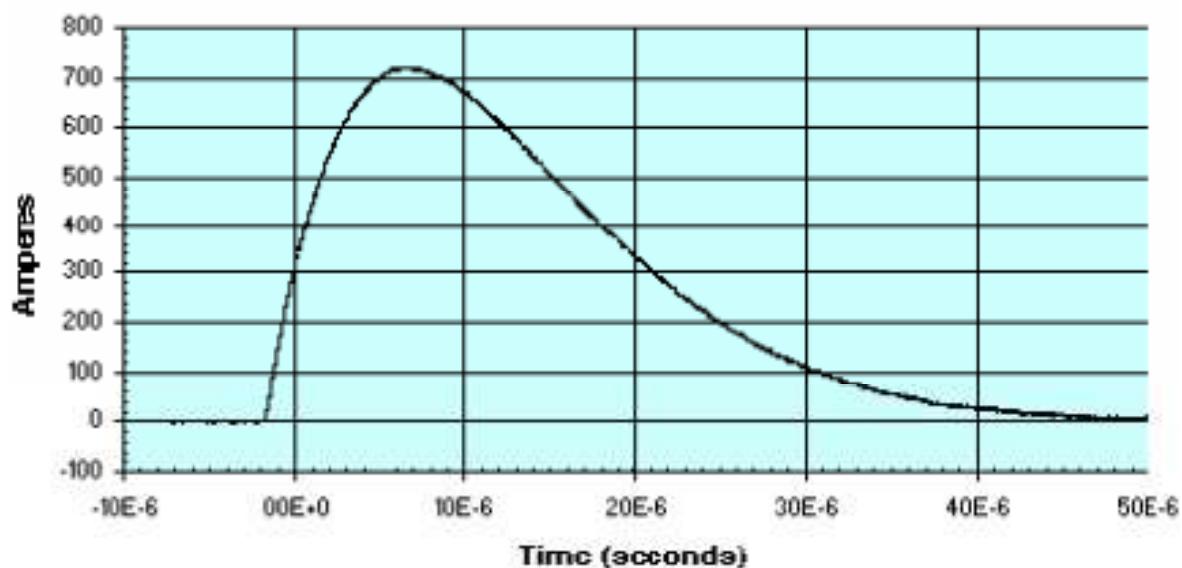


Рис. 5.10. Протекающий ток молнии в фюзеляже самолета

Test	Configuration I	Configuration II
Baseline OC Voltage/SC Current (Single Wire- without bundle)	-90 V / -34 A	-90 V / -34 A
Baseline OC Voltage/SC Current (Single Wire with bundle)	-65 V / -33 A	-76 V / -36.5 A
EEU – Single wire, Local Return - OC Voltage/SC Current - Internal Load Voltage	-90 V / -39 A -76 V	-40 V / -11.4 A -29 V
EEU – Two Wires, Return Grounded at Power Distribution Center - Internal Load Voltage	-32 V	+35 V
EEU – Twisted Pair, Return Grounded at Power Distribution Center - Internal Load Voltage	-31.5 V	+36.5 V
EEU – Shielded-Twisted Pair, Return Grounded at Power Distribution Center - Internal Load Voltage - Shield Current	-32.5 V -45 A	+28 V -50 A

Рис. 5.11. Сводные результаты наводок током молнии

6. Пути решения проблемы защиты от преднамеренных электромагнитных воздействий

6.1. Общие подходы

Рассмотрим общие принципы защиты [106]. Когда необходимо защитить здание и его внутреннее оборудование от угрозы ПЭМП, надо иметь в виду несколько аспектов. Первый – следует рассматривать эту задачу как часть проблемы обеспечения безопасности. Поскольку по большей части генераторы ПЭМП относительно малы по размерам, они должны находиться близко к цели. Таким образом, на снижение этой угрозы могут быть распространены обычные методы обеспечения безопасности. Конечно, для защиты могут применяться и электромагнитные методы. Очевидно, что надо исключить парковку транспортных средств в заданной зоне, а вся территория вокруг здания должна иметь определенный вид защиты для предотвращения установки генераторов помех. В частности, все области ввода питания и телекоммуникаций должны охраняться и время от времени проверяться. Важное оборудование внутри здания не следует размещать около внешних стен. Кроме того, необходимо резервирование внутренней разводки альтернативными трассами. Для важного оборудования должно быть предусмотрено резервное питание. Здание должно быть снабжено системами мониторинга как излучаемых, так и кондуктивных ЭМ-воздействий. Критичное оборудование следует электромагнитно экранировать, а для критичных кабельных вводов предусмотреть защитные приборы и фильтры. Рекомендуется использовать неметаллические волоконно-оптические кабели для электромагнитной защиты. Наконец, любая важная организация должна разработать программу испытаний для проверки уровня защиты здания, когда защита уже установлена, через фиксированные промежутки времени, чтобы убедиться, что защита не утратила свою силу.

Серьезный подход к защите от ПЭМП ведет к некоему виду холодной войны (по крайней мере, мысленной, если не реальной) между нападающим и защищающимся. Она похожа на состязание между преступником и детективом, между киллером и телохранителем или на лестничную модель (мера – контрмера – контрконтрмера –...) в разработке военного оружия [107].

Противостоящие стороны должны рассмотреть одну и ту же систему аналогично общему анализу, который провел Баум для передаточной функции от источника излучения до типовой системы (рис. 6.1) [108] и для формы воздействующего сигнала [109, 110]. Совпадение спектрального состава воздействия с частотным интервалом области резонансов системы – главное условие для эффективности воздействия (рис. 6.2) [69].

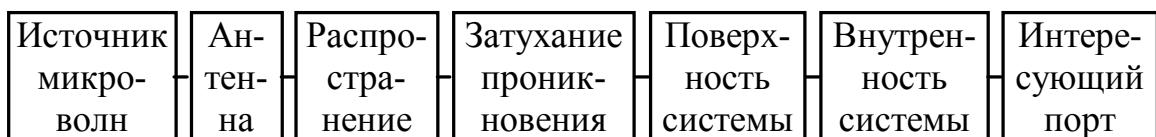


Рис. 6.1. Взаимодействие источника микроволн высокой мощности с типовой системой

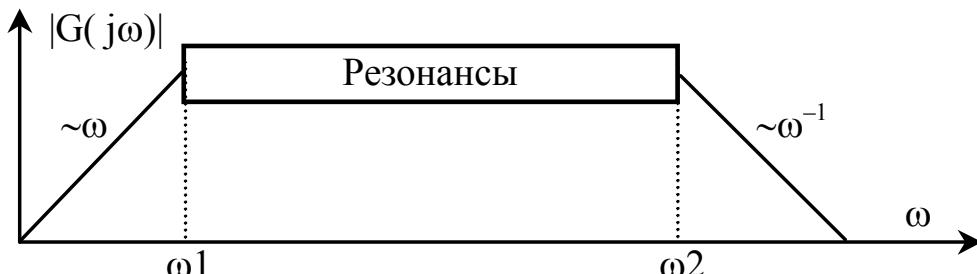


Рис. 6.2. Частотная зависимость отклика типовой системы

Подробный анализ внутри области резонансов позволяет идентифицировать точки «смерти» и «спасения» цели, которые могут быть очень близки друг к другу на частотной оси. Примеры эффективности экранирования металлического корпуса с щелями: разница 70 дБ для частот $\approx 4,19$ ГГц и $\approx 4,31$ ГГц на рис. 6.3 [111]; разница 50 дБ (по мощности) для частот $\approx 2,62$ ГГц и $\approx 2,63$ ГГц на рис. 6.4 [112].

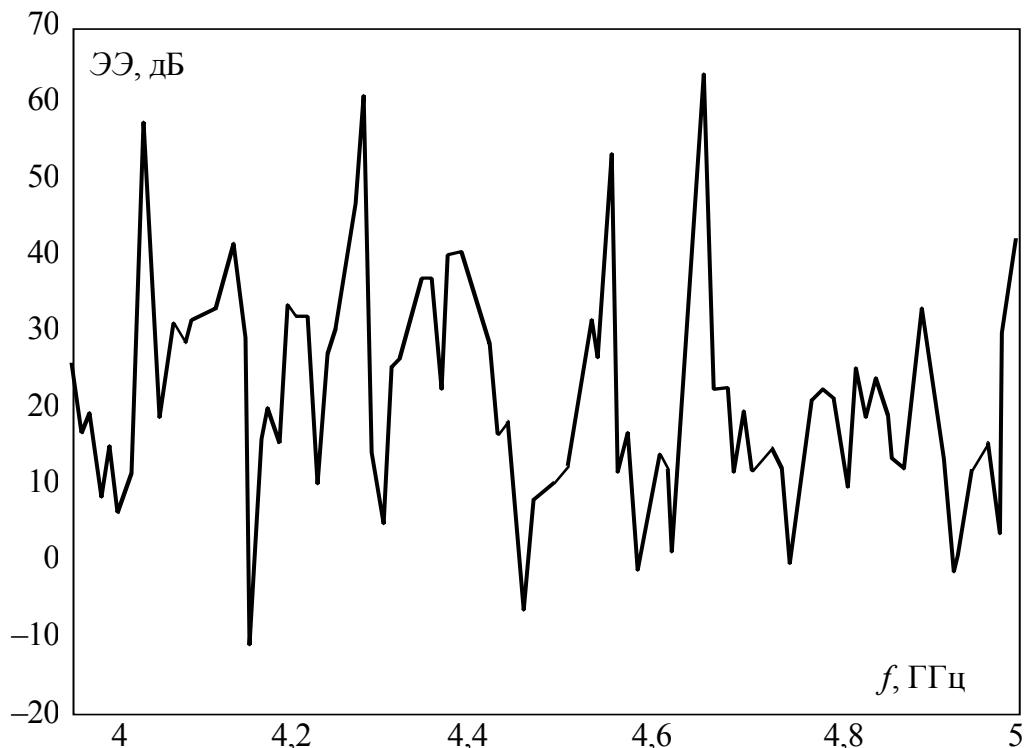


Рис. 6.3. Частотная зависимость эффективности экранирования корпусом с щелью Y-составляющей электрического поля

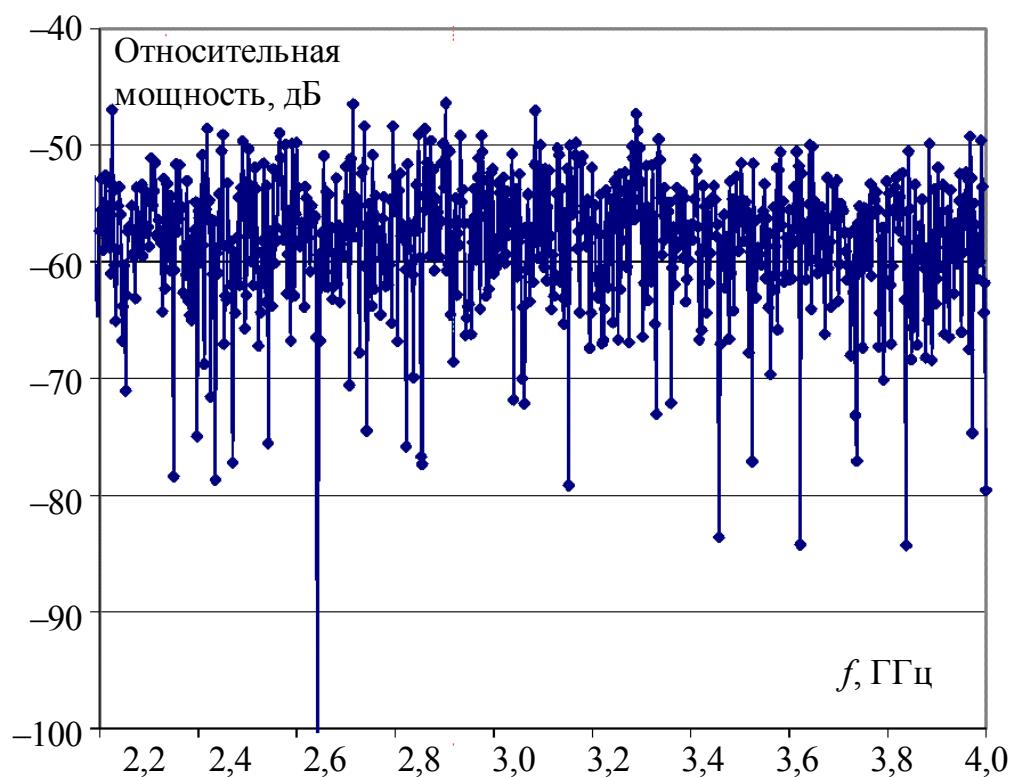


Рис. 6.4. Частотная зависимость наводки внутри корпуса с пятью отверстиями на каждой стороне

Необходимо отметить, что результаты этого анализа находятся в основе успеха как нападающего, так и защищающегося. Первый старается выявить жизненно важные резонансные частоты цели, чтобы улучшить своё воздействие (например, сосредоточив на выявленной частоте всю мощность непрерывного излучения ПЭМП). Второй должен выявить эти частоты (а затем, например, замаскировать их), чтобы защитить своё оборудование.

Задача выявления не очень сложна. Простейшим способом является хорошо известное измерение резонансной частоты конденсатора с замкнутыми выводами. Соответствующий электромагнитный мониторинг работающей системы или соответствующее облучение и анализ отклика неработающей системы анализатором спектра также не являются сложной проблемой для внутреннего и даже для удаленного вариантов. Эффективные и универсальные средства моделирования [113] могут быть весьма полезны для решения этой задачи, а специфичное, с многочисленными экстремумами поведение частотных зависимостей подсказывает использовать для выявления оптимальных частот генетические алгоритмы, способные обходить локальные экстремумы.

Кроме частоты, многие другие параметры могут использоваться нападающим для усиления, а защищающимся для ослабления воздействий ПЭМП.

Для источников ПЭМП предельная мощность сигнала на цели оценивается по напряженности поля для пробоя воздуха в апертуре антенны [2]. Между тем возможность суммирования мощностей импульсных генераторов с малым джиттером имеет следующие важные следствия для ПЭМП:

- ✓ суммирование мощности может выполняться на цели, так что ограничение, налагаемое пробоем воздуха, перемещается от апертуры антенны к самой цели и может быть достигнуто конечным числом излучателей на практических расстояниях до цели;
- ✓ синхронизированные излучатели могут располагаться вместе не только в одной решётке, но и в различных местах окружения цели;

✓ дополнительное преодоление ограничения пробоем воздуха состоит в том, что напряжённость электрического поля для пробоя воздуха коротким импульсом может быть много больше, чем непрерывным излучением.

Что касается уязвимости, то интересно отметить, что в передовой статье тематического выпуска по ПЭМП [8] в числе основных путей электромагнитной защиты цифровой аппаратуры от сбоев указывается введение избыточности для обнаружения и коррекции ошибок информации, хотя и отмечается необходимость учёта того, что ПЭМП может повторяться с частотой в мегагерцы. Между тем необычно длительно сохраняющиеся изменения характеристик полупроводникового прибора могут сильно нарушить корректную работу систем во времени. Поэтому традиционные программные методы (например, многочисленные попытки повтора неудавшихся действий), уместные для предотвращения кратковременных проблем, в этом случае не дадут успеха. Следовательно, потребуются другие методы. Например, старая проблема уменьшения чувствительности работы схемы к изменению параметров компонентов может получить новую актуальность: чем ниже чувствительность характеристик всей схемы к изменению характеристик её полупроводниковых приборов из-за длительных результатов ЭМ воздействия, тем меньше влияние ПЭМП на работу этой схемы.

Важно понимать, что в общем случае все находящееся между источником и целью, а также вокруг или вблизи них, может ослабить или усилить ПЭМП: результат зависит от параметров воздействия и конфигурации. Поэтому уместно говорить о явлениях ослабления и усиления вместе (формально различие в децибелах состоит лишь в знаке), по крайней мере, для того чтобы защищающийся всегда имел в виду, что ослабление может легко оказаться усилением. Яркими примерами являются многочисленные опубликованные зависимости эффективности экранирования от частоты: для металлического корпуса с щелями часто есть частоты, на которых уровень поля внутри корпуса больше, чем снаружи (например, несколько точек на рис. 5.1 и 6.3).

Отметим, что отражения и резонанс, упомянутые выше, являются известными причинами усиления поля. Один из трагиче-

ских примеров, когда отражения от металлических конструкций, установленных внутри сталеплавильного цеха вдоль стен, навели ЭМ помеху, достаточную для опрокидывания ковша с расплавленной сталью [114]. Простой и показательный пример усиления на 50 дБ взаимовлияния между двумя цепями печатной платы на резонансных частотах корпуса при установке этой платы в корпус представлен на рис. 6.5 [115].

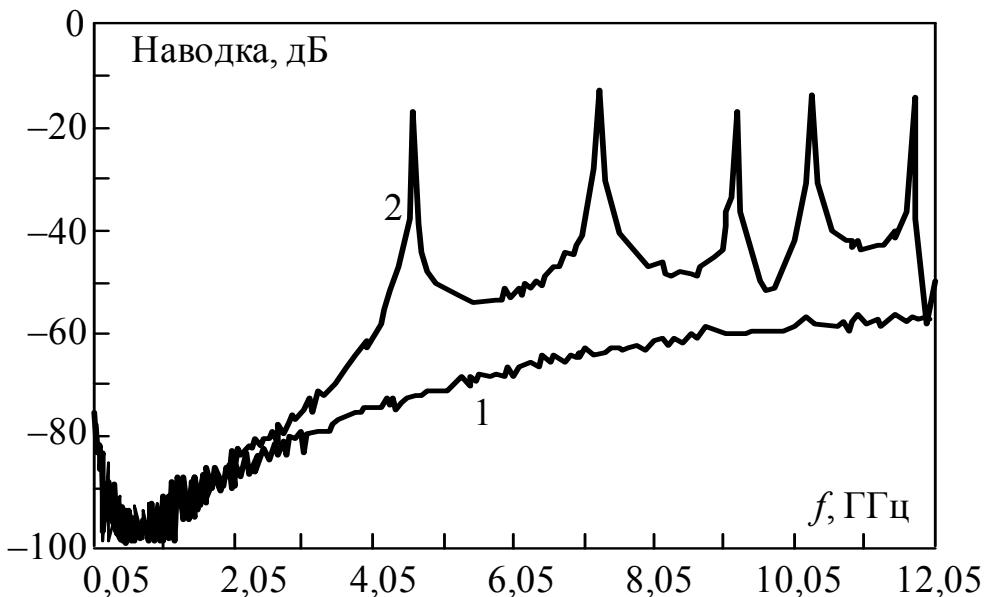


Рис. 6.5. Измеренные наводки между двумя тестовыми цепями на печатной плате без корпуса (1) и в корпусе (2)

Результаты экспериментов с передающей и приемной антеннами в реверберационной камере (рис. 6.6) еще более впечатляют: кратность частоты повторения импульсов нижней резонансной частоте камеры увеличивала сигнал этой частоты на 30 дБ, а при размещении между антеннами нелинейного рассеивателя – на 85 дБ по мощности (рис. 6.7) [116].

Таким образом, естественно допустить, что взаимовлияния между цепями источника и цели, размещенными внутри фюзеляжа самолета, могут значительно увеличиться из-за резонансов фюзеляжа и нелинейных рассеивателей в салоне самолета.

Неожиданные результаты могут иметь место и в открытом пространстве. Так, описан пример усиления примерно в 100 раз сигнала посадочного маяка вдоль взлетно-посадочной полосы самолётом, находящимся на стоянке [113] (рис. 6.8).

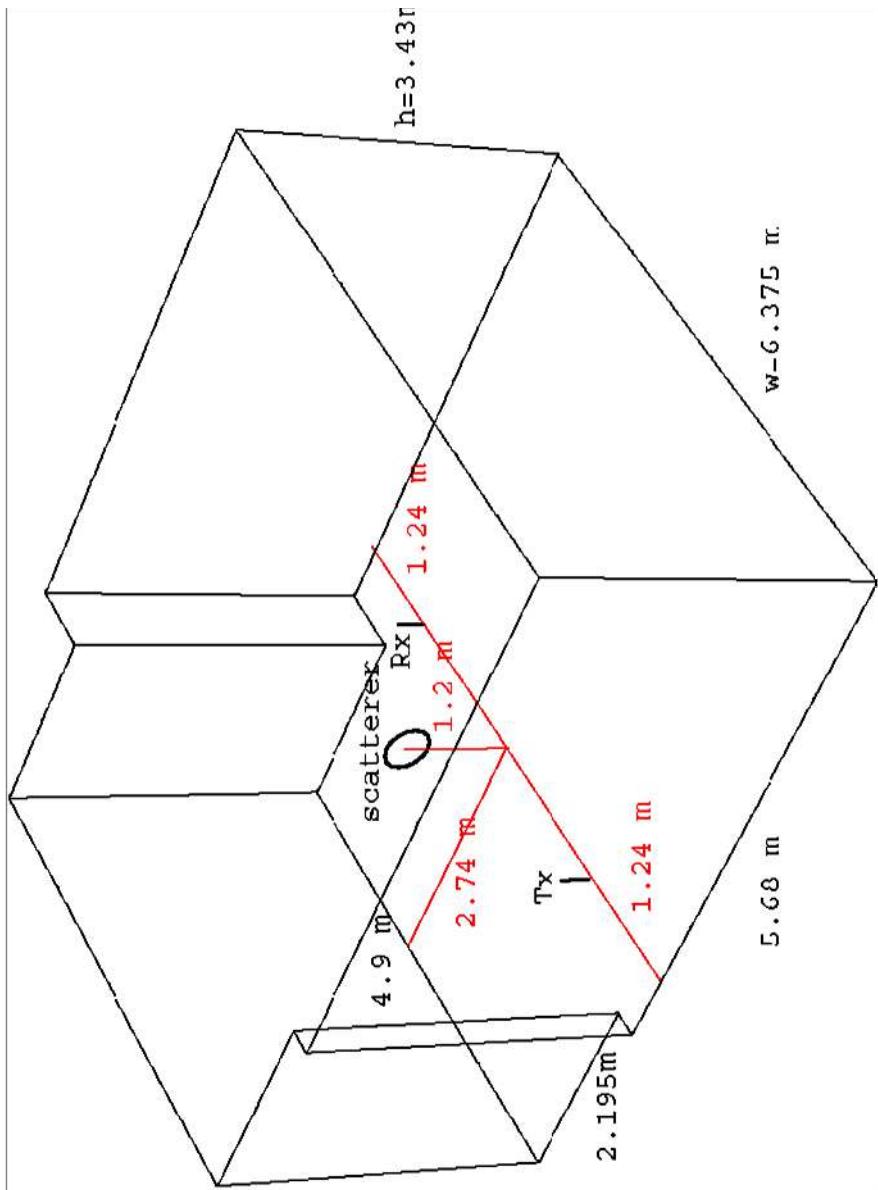


Рис. 6.6. Экспериментальная установка: Tx – излучающая антенна (33 см);
 Rx – приемная штыревая антенна (97 см). Диаметр
нелинейно нагруженного контура (рассеивателя) 47 см

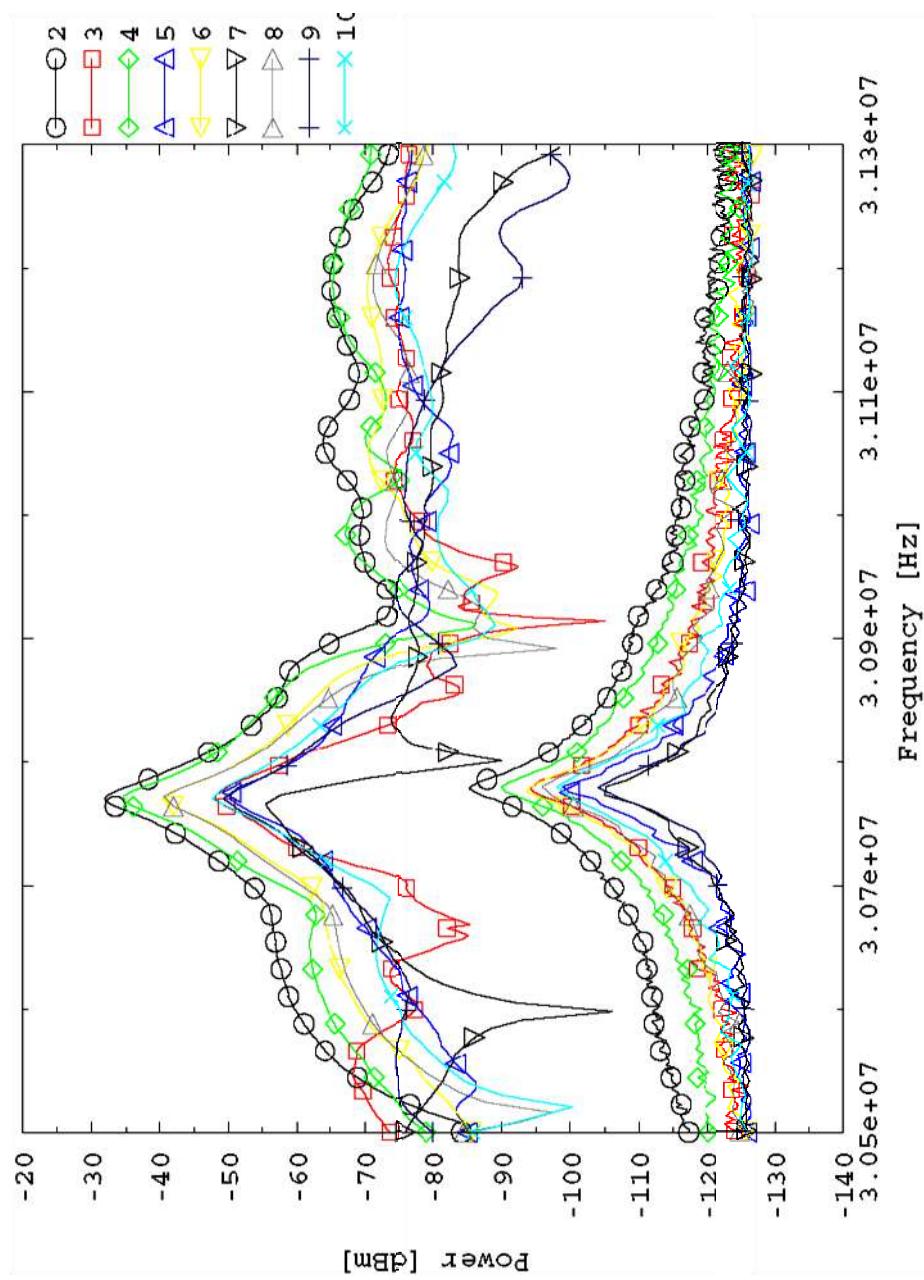


Рис. 6.7. Максимумы низкочастотной составляющей для разных частот повторения импульса с нелинейным рассеивателем (верхние кривые) и без него (нижние кривые).
Маркеры отображены для каждой десятой точки данных

Возможно использование отражений и резонанса для ослабления ЭМ воздействий. Примером является применение экранов различной формы, в том числе проводных рассеивателей, эффективно работающих на интересующей частоте. Так, простые решётки рассеивателей позволяют «дальнее экранирование» в 20 дБ [117]. Много полезных подходов для ослабления ПЭМП можно получить из идеи использования ЭМ излучения от цели для дезориентации нападающего [107]. Например, простыми мерами можно организовать излучение или рассеяние на ложных (не опасных для цели) резонансных частотах для маскировки жизненно важных резонансных частот.

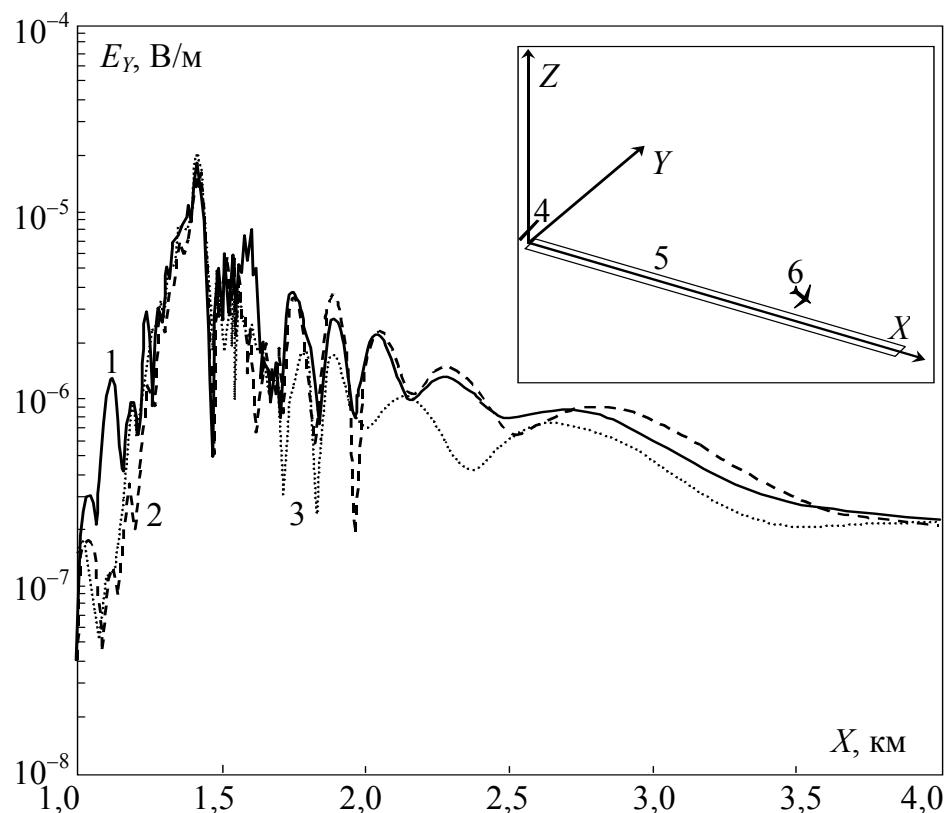


Рис. 6.8. Моделирование методом моментов (1), методом физической оптики (2) и методом физической оптики с учетом токов Фуко (3) искажения поля диполя (4) вдоль взлетно-посадочной полосы (5) стоящим в стороне самолетом (6)

Таким образом, важно осознавать, что посредством окружающей обстановки можно достичь значительного изменения ЭМ взаимодействия источника(ов) и цели(ей) за счет изменения распределения поля в пространстве (в том числе изменения на-

правления распространения ЭМ волны или максимизации/минимизации поля в заданной точке).

Следует отметить важность применения ПЭМП в качестве электромагнитного оружия, в частности для обороны военного самолета от ракет на малых расстояниях, когда все традиционные средства радиоэлектронной борьбы уже не эффективны. Это направление оказалось столь серьезным и перспективным, что разработка и производство соответствующих средств относится к области ключевых технологий, определяющих уровень оборонной техники современного государства [87].

6.2. Некоторые технические решения

В [118] выполнена оценка способности проводящих тканей ослаблять электромагнитные поля и защищать электронное оборудование. Измерена эффективность экранирования тканевых сумок (с замком-молнией с металлическими зубцами и проводящими нитями) в диапазоне от 0,1 до 5 ГГц. Результаты показали рост защищенности печатных плат в 6–8 раз, когда они помещались внутрь такой сумки (рис. 6.9).

В качестве гибкой меры экранирования оперативных командных пунктов США рассматривается использование модульных тентов из проводящих тканей (рис. 6.10) [119].

В презентации семинара [120] обсуждались различные аспекты защиты от мощных электромагнитных воздействий.

В качестве эффективной меры фильтрации частот выше 1 ГГц предложена UG-технология от фирм ELOP и SigNext [121], основанная на сильном затухании на микроволновых частотах, вносимом аморфными материалами. Представлены готовые варианты и частотные характеристики изделий различного исполнения (рис. 6.11) [122].

В качестве средства защиты от кондуктивных высоковольтных импульсов рассматриваются полосковые фильтры (рис. 6.12) [123]. Приводятся многочисленные результаты компьютерного и экспериментального моделирования их частотных характеристик, а также результаты вычисления (в Spice) времен-

ного отклика на высоковольтный входной импульс (рис. 6.13). В [124] приведены детали указанного моделирования.

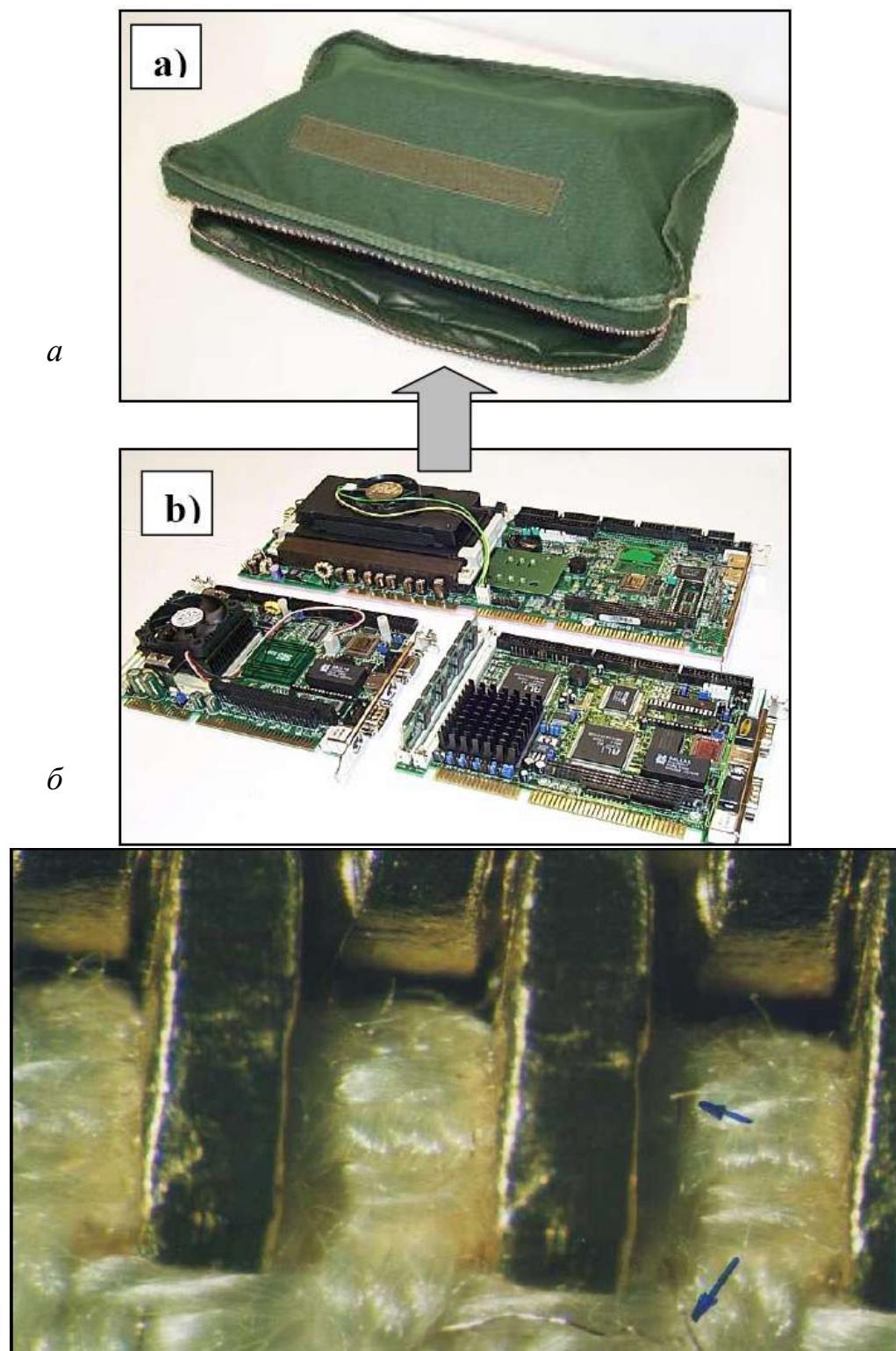


Рис. 6.9. Защитная сумка (а), микропроцессорные платы (б), замок-молния с металлическими зубцами и проводящими нитями (в)



Рис. 6.10. Испытание электромагнитными помехами
модульных тентов из проводящей ткани

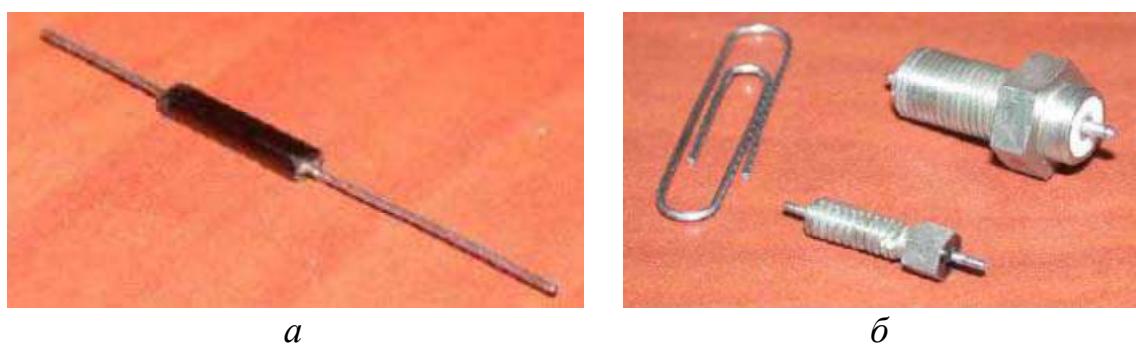


Рис. 6.11. UG-фильтр в выводном (а), проходном (б) исполнении



Рис. 6.12. Топология полосопропускающего (1 ГГц)
фильтра на подложке RT/Durouid 5880 с параметрами:
 $\epsilon_r=2,2$; $h=0,5$ мм; $t=35$ мкм; $\tan\delta=0,0009$

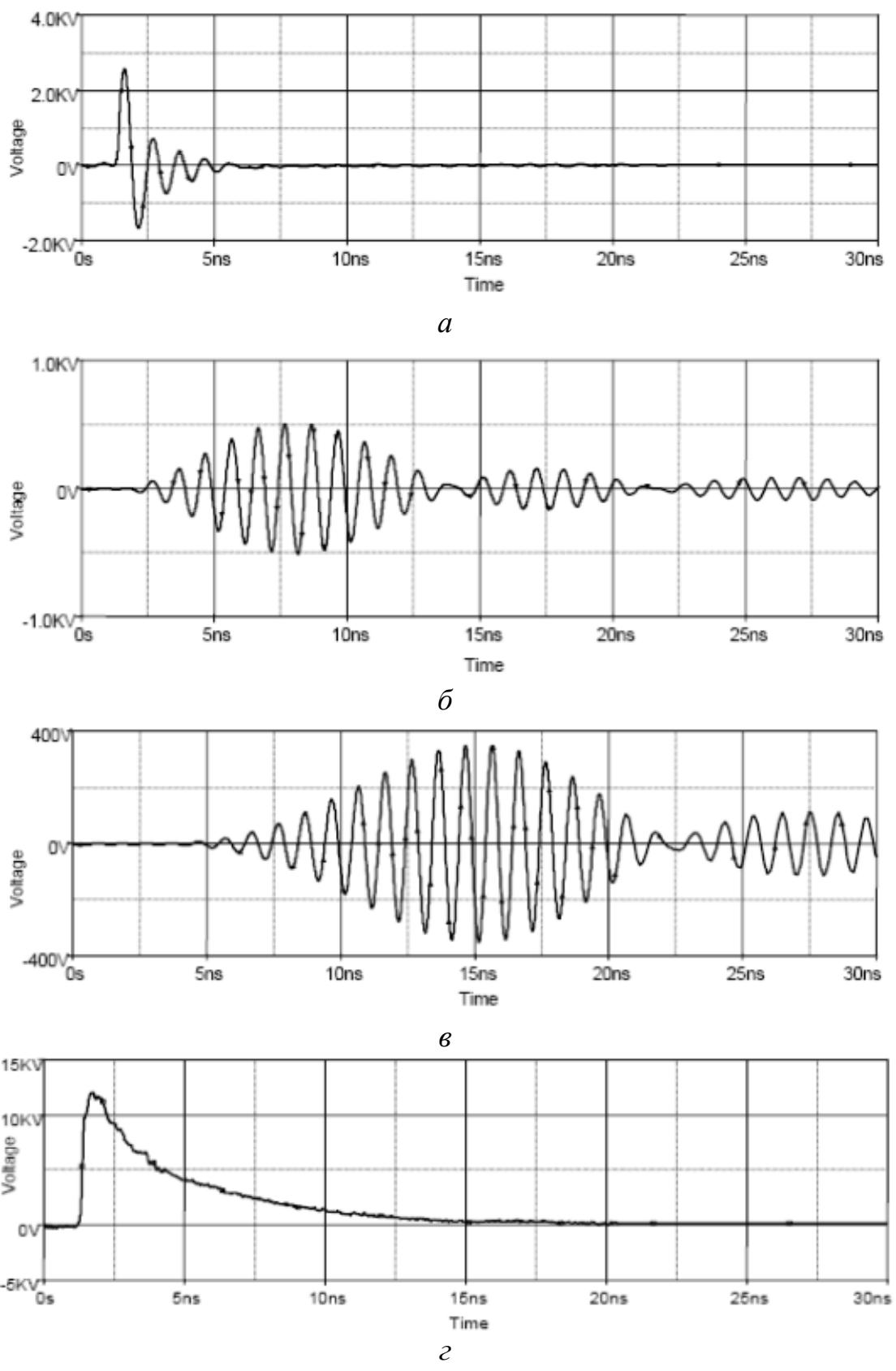


Рис. 6.13. Отклики фильтров 1-го (*а*), 3-го (*б*), 5-го (*в*) порядка на тестовое входное воздействие (*г*)

Особенно важной проблемой становится своевременное обнаружение факта электромагнитного воздействия. Оригинальным предложением является мониторинг излучений от критичного оборудования: во время мощного воздействия на оборудование спектр излучений от него изменяется особенным образом во время перехода из линейного в нелинейный режим [125].

При исследовании КМОП и ТТЛ компонентов различных производителей обнаружен эффект памяти, состоящий в повышении стойкости компонентов после многократно проведенных испытаний меньшими уровнями воздействий [126]. В [127] детально исследовано повышение стойкости тестовой конфигурации из нескольких компьютеров в результате повторяемого облучения (эффект «тренировки») источником электромагнитных помех. Предлагается математическое доказательство существования такого явления.

Исследование возможности использования пробоя в щели в качестве меры защиты выполнено в [128]. Щели облучались микроволновыми (S-диапазон) импульсами с временем нарастания 80 нс и длительностью 1 мкс от магнетрона 700 кВт. Наблюдались типичные уровни пробоя 13 кВ/м и ослабление энергии до 25 дБ.

В [129] в качестве меры по обеспечению ЭМС электроники, всё более проникающей в автомобили, рассматривается интеграция вычислительного моделирования ЭМС в цикл разработки промышленных транспортных средств.

В [130] выполнено компьютерное моделирование восприимчивости быстродействующих интегральных схем и межсоединений в экранирующем корпусе с подсоединенными внешними сигнальным кабелем (рис. 6.14).

В [131] с помощью метода моментов проведено моделирование падения радиочастотного напряжения между любыми двумя точками межсоединения печатной платы.

В [132] рассматривается резонансное поведение поля, перенесенного печатной платой, в качестве способа диагностики проблем излучений печатных плат. Предложен новый подход к экспериментальной оценке резонансных свойств печатных плат, основанный на измерениях эффективной поверхности рассеяния

в GTEM-камере, которая используется одновременно для измерения эмиссий и восприимчивости.

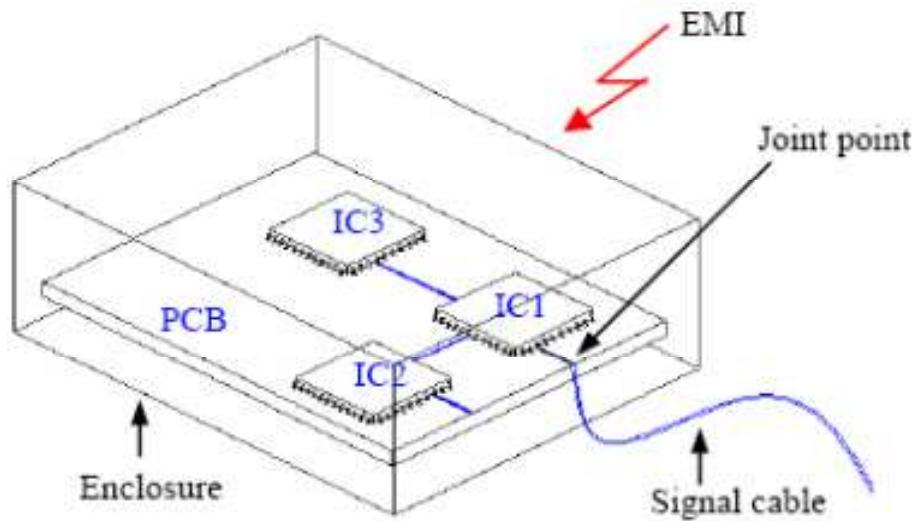


Рис. 6.14. Схема анализируемой конфигурации

В [133] системно рассматривается старая проблема ПЭМИН. В [134] описан простой инженерный метод определения защищенности системы от влияния беспроводных GSM-устройств, а также выявления наиболее уязвимых частей системы.

Заключение

Сформулируем основные тенденции и прогноз развития проблемы защиты от ПЭМП.

1. Источники ПЭМП: увеличение мощности и частоты (для узкополосных источников); уменьшение времени фронта/спада (для сверхширокополосных источников); увеличение частоты повторения импульсов; уменьшение джиттера; возможность синхронизации; уменьшение веса; переход к полупроводниковым приборам; уменьшение расстояния до цели. Прогноз: рост воздействия до пробоя среды у цели.

2. Восприимчивость: естественное снижение стойкости из-за уменьшения разности уровней цифровой логики; расширяющийся переход к оптике на разных структурных уровнях – кабели, платы, компоненты. Прогноз: переход к микромеханике; использование микровакуумных приборов; использование нанотехнологий.

3. Защита: совершенствование защитных приборов и устройств на их основе (использование защитных вариантов новых генераторных полупроводниковых приборов); использование пассивных компонентов (полосковых фильтров); использование свойств плазмы; использование нанотехнологий (например, для новых экранирующих и поглощающих покрытий); более тщательное, адекватное и точное компьютерное моделирование (не только в части анализа, но и в части синтеза и оптимизации) системы целиком; для анализа слабых мест использование диверсионного подхода с применением теории решения изобретательских задач; пересмотр и обновление нормативной базы, разработка новых стандартов; всемерное внедрение, особенно на стадии разработки, принципов электромагнитной совместимости и стойкости аппаратуры; просвещение и образование в области защиты от ПЭМП; международное сотрудничество. Прогноз: рост защищенности от ПЭМП.

4. Большое количество публикаций по исследованию влияния ПЭМП на электронику ракеты. Можно полагать, что это связано с одним из основных военных применений ПЭМП: защитой

от летящей крылатой ракеты на малых расстояниях, когда никакой другой защиты уже нет.

5. Довольно малое количество публикаций по мерам защиты от ПЭМП.

6. Террористический акт в США 11 сентября 2001 г. показал всему миру реальность того, что представлялось невозможным. Естественно полагать, что аналогичное возможно и с проблемой электромагнитного терроризма. Осознание этой возможности уже стимулировало финансирование исследований для решения данной проблемы.

7. Причиной масштабного отключения электроэнергии в США, по мнению некоторых специалистов, могли быть созданные ПЭМП. Косвенным подтверждением этого является финансирование работ, связанных с ПЭМП в электроэнергетике, в частности проводимых фирмой Метатеч (в том числе совместно с российскими учеными), владельцем которой является У. Радаски.

8. Мнения специалистов о возможности решения проблемы ПЭМП различны. Есть мнение, что ее решение не представляет технической сложности, а является вопросом только экономическим. Существует также мнение, что от современных источников ПЭМП, которые непрерывно совершенствуются, защититься традиционными методами невозможно: нужна защита, основанная на новых физических принципах. Полагают, что существенно продвинуться в её решении поможет всеобщая осведомленность о ней, основанная на просвещении и образовании.

9. Решению проблемы ПЭМП, используемых террористами, преступниками и хакерами, весьма способствует анализ исследований и применения ПЭМП в военной технике, а также в спецтехнике, где результаты на десятилетия опережают исследования в гражданском секторе.

10. Ряд гипотез, выдвинутых в докторской диссертации Т.Р. Газизова, независимо от работ других исследователей нашел свое подтверждение. Так, возможность синхронного суммирования ПЭМП широко используется, причем не только в решетках антенн, но и во множестве сброшенных парашютных излучателей и электромагнитных бомб, синхронное срабатывание которых возможно по команде GPS. Идея поиска частотных точек «смер-

ти» и «спасения» за счет оптимизации используется в спецтехнике, подтверждая действенность моделирования в решении проблемы ПЭМП. Принцип преднамеренной перекрестной помехи реализуется при кондуктивных воздействиях по различным проводящим структурам.

Контрольные вопросы

Раздел 1

1. Кем, где и когда началось открытое обсуждение проблемы ПЭМП?
2. Где и когда опубликован первый обзор проблемы ПЭМП?
3. Где и когда состоялся первый семинар по проблеме ПЭМП?
4. Где и когда состоялась первая рецензируемая секция симпозиума по проблеме ПЭМП?
5. Как называется первая книга по проблеме ПЭМП?

Раздел 2

1. До каких значений уровней и частот простираются требования в стандартах по испытаниям на восприимчивость авионики к радиочастотам?
2. Какой должна быть поляризация при испытаниях по зарубежным стандартам для частот выше 30 МГц?
3. Какая проблема, связанная с испытаниями на электромагнитную совместимость, возникает из-за нормативного срока эксплуатации самолетов до 30 лет?
4. В чем заключается новая процедура определения спектра широкополосного сигнала?
5. Какой новой величиной характеризуется широкополосность сигнала?
6. Какие установлены категории полосы сигнала?

Раздел 3

1. Каковы порядки значений мощности и частоты генераторов электромагнитного излучения для ПЭМП?
2. За счет какой энергии получают гигантский одиночный импульс?
3. Какую уникальную возможность дает малый джиттер импульсов, генерируемых полупроводниковыми приборами?
4. Уровень напряженности чего может быть одного порядка с уровнем уязвимости оборудования пролетающего самолета?
5. Как выполняется поиск «уязвимых» частот на расстоянии?

6. Каков действенный способ преодоления ослабления воздействующего поля расстоянием?

7. Чем коммутируется фотопроводящий полупроводниковым ключом?

8. Как называется американская программа построения станций исследования ионосферы, применимых для ПЭМП?

Раздел 4

1. Назовите русские и английские термины, связанные с защищенностью аппаратуры.

2. Насколько низким может быть уровень уязвимости персонального компьютера, не защищенного электромагнитным экраном?

3. Во сколько раз уровни повреждения компьютеров из-за ПЭМП для импульсных сигналов больше уровней сбоя?

4. Во сколько раз изменяется напряженность поля от первых сбоев до разрушения PIC-микроконтроллера?

5. Почему вероятность помех авионике становится выше на малой высоте?

6. Какие из переносных электронных устройств имеют максимальный уровень излучения?

7. В чем могут проявиться результаты влияния мощных микроволн на диоды?

8. Сколько может длиться возврат к прежнему состоянию характеристик диода после воздействия мощных микроволн?

9. Назовите два вида экранирующих тканей.

Раздел 5

1. Может ли в случае полностью замкнутых металлических поверхностей электромагнитное поле внутри быть больше, чем снаружи?

2. Из-за чего может существенно снижаться эффективность экранирования корпуса оборудования?

3. До какого значения может снижаться средняя эффективность экранирования корпуса реального компьютера, измеренная в реверберационной камере в диапазоне частот 1–18 ГГц?

4. Каковы порядки эффективности экранирования фюзеляжем самолета?

5. Замена каких материалов на какие на вертолетах приводит к уменьшению эффективности экранирования?

6. Какую угрозу создает открытый доступ к шине заземления?

7. Как может измениться реальное напряжение срабатывания различных защитных приборов относительно заявленного производителем при укорочении воздействующих импульсов ПЭМП?

8. Каков недостаток быстродействующих защитных диодов по сравнению с газовыми разрядниками и варисторами?

Раздел 6

1. Могут ли быть распространены обычные методы безопасности на снижение угрозы ПЭМП?

2. Как для эффективности воздействия должны соотноситься спектральный состав воздействия с частотным интервалом области резонансов системы?

3. Кто провел общий анализ для передаточной функции от источника излучения до типовой системы?

4. Почему резонансные частоты цели важны для нападающего и защищающего?

5. Куда от апертуры антенны перемещается ограничение, налагаемое пробоем воздуха, за счет суммирования мощностей импульсных генераторов с малым джиттером?

6. Можно ли рассматривать в общем случае все, находящееся между источником и целью, а также вокруг или вблизи них, как то, что может ослабить или усилить ПЭМП?

7. На сколько может увеличиться взаимовлияние между двумя цепями на печатной плате на резонансных частотах корпуса при установке этой платы в корпус?

8. Как могут изменить связь между передающей и приемной антеннами кратность частоты повторения радиоимпульсов нижней резонансной частоте корпуса и размещение между антеннами нелинейного рассеивателя?

9. Почему эффективно применение ПЭМП в качестве электромагнитного оружия, в частности для обороны военного самолета от ракет на малых расстояниях?

10. Что обеспечивает помещение электронного оборудования в экранирующие тканевые сумки с замком-молнией с металлическими зубцами и проводящими нитями?

Список сокращений

АЦП	аналого-цифровой преобразователь
БИС	большая интегральная схема
ВВС США	Военно-воздушные силы Соединенных Штатов Америки
КМОП	комплементарная структура металл – оксид – полупроводник
МЭК	международная электротехническая комиссия
НСВ	намеренное силовое воздействие
ПДЭМВ	преднамеренное силовое электромагнитное воздействие
ПК	персональный компьютер
ПЭМП	преднамеренные электромагнитные помехи
РЭА	радиоэлектронная аппаратура
СДВ	силовое деструктивное воздействие
ТТЛ	транзисторно-транзисторная логика
ФП	функциональное поражение
ЭМ	электромагнитный
ЭМС	электромагнитная совместимость
ЭЭ	эффективность экранирования
CEG	Centre des Etudes de Gramat
EMC	Electromagnetic Compatibility
FOL	Fiber Optic Lead
HAARP	High Frequency Active Auroral Research Program
HPEM	High Power Electromagnetics
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IEMI	Intentional Electromagnetic Interference
URSI	Union Radio-Scientifique Internationale

Литература

1. Loborev V.M. The modern research problems // AMEREM Conference. Albuquerque, NM, 1996. May.
2. Gardner R.L. Electromagnetic terrorism. A real danger // Proc. of the 14th Int. Wroclaw Symposium on EMC, Wroclaw, Poland, June 23–25, 1998. P. 10–14.
3. 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, February 16–18, 1999. P. 181–200.
4. URSI resolution on «Criminal activities using electromagnetic tools» // The Radio Science Bulletin. 1999, September. N 290. P. 62–63.
5. Radasky W.A., Messier M.A., Wik M.W. Intentional electromagnetic interference (EMI): Test data and implications // Proc. of the 14th Int. Zurich Symp. on EMC. Zurich, Switzerland, February 20–22, 2001. P. 29–36.
6. Барсуков В.С. Безопасность: технологии, средства, услуги. – М. КУДИЦ–ОБРАЗ, 2001. 496 с.
7. Электромагнитный терроризм на рубеже тысячелетий / под ред. Т.Р. Газизова. – Томск: Том. гос. ун-т, 2002. – 206 с.
8. Radasky W.A., Baum C.E., Wik M.W. Introduction to the special issue on high-power electromagnetics (HPEM) and intentional electromagnetic interference (IEMI) // IEEE Trans. on Electromag. Compat. 2004, August. Vol. 46. P. 314–321.
9. Radasky W.A. The Threat of Intentional Electromagnetic Interference (IEMI) to Wired and Wireless Systems // Proc. of the 17-th Int. Zurich Symp. on EMC. Singapore, February 27–March 3, 2006. P. 161–164.
10. 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, June 27–30, 2000. P. 763–769.
11. Borgstrom E.J. EMC requirements for avionics: RTCA/DO–160D, Change 1 and Change 2. The Int. // Journal for EMC. ITEM 2002. P. 18–30.

12. Borgstrom E.J. EMC requirements for avionics: RTCA/DO–160D, Change No.3. // The Int. Journal for EMC. Interference technology. 2003. P. 34–40.
13. Brewer R., Trout D. Modern Spacecraft – Antique Specifications // Proc. of Int. IEEE Symp. on EMC. 2006.
14. Rothenhausler M. HPM Threat to airbone systems // Book of abstracts EUROEM 2004, 12–16 July, Magdeburg, Germany. P. 20.
15. Kreitmair-Steck W., Tauber W. Aircraft hazards by using portable electronic devices (PED) // Proc. of the 16th Int. Symp. on EMC. Wroclaw, Poland, June 25–28, 2002. P. 383–388.
16. Канащенков А.И., Меркулов В.И., Самарин О.Ф. Облик перспективных бортовых радиолокационных систем. Возможности и ограничения. М.: ИПРЖР, 2002. 176 с.
17. 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, June 27–30, 2000. Late Papers. P. 11–20.
18. Яноз М. Стандартизация в области ЭМС // Сб. науч. докл. IV Междунар. симп. по электромагнитной совместимости и электромагнитной экологии, г. Санкт-Петербург, 19–22 июня 2001 г. С. 9–14.
19. Wik M.W., Radasky W.A. IEC Standardisation of immunity to high power electromagnetic transient phenomena // Proc. of IEEE Int. Symp. on EMC, 2003, Istanbul, Turkey.
20. IEC 61000-2-13 Ed. 1.0. Electromagnetic compatibility (EMC). Part 2–13: Environment – High power electromagnetic (HPEM) environments. 2005.
21. Jaekel B.W. EMC and functional safety – challenges and standards // Proc. of 7th Int. Symp. on electromagntic compatibility and electromagnetic ecology, 2007, Saint-Petersburg, Russia. P. 208–211.
22. Clouds C. EMI and Functional Safety Why Traditional Immunity Testing is Inadequate and What Should be Done Instead // Proc. of Int. IEEE Symp. on EMC. 2006.
23. Heather F. Lightning Strikes and Aircraft Operational Performance // Proc. of Int. IEEE Symp. on EMC. 2005.

24. 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, Feb. 16–18, 1999. P. 191–194.
25. Экспериментальные исследования воздействия импульсного СВЧ излучения на материалы / Н.С. Вернигоров [и др.] // Информост. 2002. № 6. С. 53–58.
26. Анцев Г.В., Сарычев В.А. Сверхширокополосные системы и поляриметрия // Труды 2-й Всероссийской научно-технической конференции по проблемам создания перспективной авионики, Томск, 15–17 апреля 2003 г. С. 105–112.
27. Генератор гигаваттных импульсов сверхширокополосного излучения / Ю.А. Андреев [и др.] // Приборы и техника эксперимента. 2000. № 2. С. 82–88.
28. Сверхширокополосные комбинированные антенны и решетки / Ю.А. Андреев [и др.] // Труды Всероссийской научно-технической конференции «Сверхширокополосные сигналы в радиолокации, связи и акустике», Муром, Россия, 1–3 июля 2003 г. С. 48–53.
29. The New Cold War: Defending Against Criminal EMI // Compliance Engineering. 2001, May/June. Vol. XVIII, N 4. P. 12–19.
30. A computer code for estimating pulsed electromagnetic disturbances penetrating into building power and earthing circuits / V.E. Fortov [et al.] // Proc. of the 14th Int. Zurich Symp. on EMC, Zurich, Switzerland, Feb. 20–22, 2001. P. 37–40.
31. Eastwood J.W., Hook M.P. Novel Crossed-Field Tubes for Compact Book of abstracts EUROEM 2004, 12–16 July, Magdeburg, Germany. P. 93.
32. Giri D.V. JOLT: A highly directive, very intensive, impulse-like radiator // Book of abstracts EUROEM 2004, 12–16 July, Magdeburg, Germany. P. 19.
33. Bohl J. Application of HPM-Technology for Protective Measures // Book of abstracts EUROEM 2004, 12–16 July, Magdeburg, Germany. P. 19.
34. Staines D.G., Urban D.J. DIEHL High-Power RF Source Development // Book of abstracts EUROEM 2004, 12–16 July, Magdeburg, Germany. P. 90.

35. High-Power Microwave System for Stopping Vehicles / J. Tatoian, D. Giri, G. Franceschetti, G. Gibbs // Book of abstracts EUROEM 2004, 12–16 July, Magdeburg, Germany. P. 148.
36. Schenk U. Directivity of Parachute Antennas for Microwave Weapons // Book of abstracts EUROEM 2004, 12–16 July, Magdeburg, Germany. P. 156.
37. Herlemann H., Koch M., Sabath F. UWB Antenna for Artillery Applications // Book of abstracts EUROEM 2004, 12–16 July, Magdeburg, Germany. P. 148.
38. A Lens TEM Horn with an Artificial Dielectric / W.S. Bigelow, E.G. Farr, L.H. Bowen, D.E. Ellibee, D.I. Lawry // Book of abstracts EUROEM 2004, 12–16 July, Magdeburg, Germany. P. 155.
39. Podgorski A.S. 100 GHz Broadband High Power Antennas // Book of abstracts EUROEM 2004, 12–16 July, Magdeburg, Germany. P. 170.
40. Davanloo F., Collins C.B., Agee F.J. Development of Ultra-Wideband Pulsers at the University of Texas at Dallas // Book of abstracts EUROEM 2004, 12–16 July, Magdeburg, Germany. P. 172.
41. Compact Photoconductive Switches for Ultra-Wideband High Power Microwave Generation / N.E. Islam, W. Nunnally, G. Tzeremes, J.A. Gaudet // Book of abstracts EUROEM 2004, 12–16 July, Magdeburg, Germany. P. 172.
42. Giri D.V., Tesche F.M. High-Power Electromagnetic (HPEM) Source Considerations // Proc. of IEEE Int. Symp. on EMC, Istanbul, Turkey. 2003.
43. Farr E.G. The Evolution of Impulse Radiating Antennas // Book of abstracts EUROEM 2004, 12–16 July, Magdeburg, Germany. P. 130.
44. Schamiloglu E. High Power Microwave (HPM) Sources: A Tutorial // Proc. of IEEE Int. Symp. on EMC, Istanbul, Turkey. 2003.
45. Sugrue E., Gleaves M. A new and reliable method for testing microwave susceptibility // Proc. of 7th Int. Symp. on electromagntic compatibility and electromagnetic ecology, 2007, Saint-Petersburg, Russia.
46. Chavka G., Sadowski M. HAARP – the research ionosphere station or the ultimate weapon of the conspiracy // 18th Int. Wroclaw

symposium and exhibition on electromagnetic compatibility, Wroclaw, 28–30 June, 2006.

47. Radiated emissions from unstructured networks: potential impact on maritime and aeronautical radio / I.D. Flintoft, A.D. Papatsoris, D.W. Welsh, M.H. Capstick, A.C. Marvin // Proc. of the 15th Int. Zurich Symp. on EMC, Zurich, Switzerland, 2003. P. 93–98.

48. LoVetri J., Wilbers A.T.M., Zwamborn A.P.M. Microwave Interaction With a Personal Computer: Experiment and Modeling // Proc. of the 13th Int. Zurich Symp. on EMC, Zurich, Switzerland, February 16–18, 1999. P. 203–206.

49. Trends in EM Susceptibility of IT Equipment / R. Hoad, N.J. Carter, D. Herke, S.P. Watkins // IEEE Trans. on Electromagn. Compat. 2004, August. Vol. 46. N 3.

50. Hoad R., Lambourne A., Wraight A. HPEM and HEMP susceptibility assessments of computer equipment // Proc. of the 17th Int. Zurich Symp. on EMC. Singapore, 2006. P. 168–171.

51. Gray R.F., Bollen W.M. HPM Effects on Central Processor Units // Book of abstracts EUROEM 2004, 12–16 July, Magdeburg, Germany. P. 126.

52. Study on the Failure Mechanism of the Electronic Device in the Transient Electromagnetic Field / Liu Di-chen [et al.] // Proc. of IEEE Int. Symp. on EMC, Istanbul, Turkey. 2003.

53. Backstrom M. HPM testing of a car: A representative example of the susceptibility of civil systems // Supplement to Proc. of the 13th Int. Zurich Symp. on EMC, Zurich, Switzerland, Feb. 16–18, 1999. P. 189–190.

54. High Power EMI on Digital Circuits Within Automotive Structures / Y. Bayram, P.C. Chang, J.L. Volakis, K. Kim, A. Iliadis // Proc. of Int. IEEE Symp. on EMC. 2006.

55. Höijer M., Bäckström M. How We Confused the Comparison between High Level Radiated Susceptibility Measurements in the Reverberation Chamber and at the Open Area Test Site // Proc. of IEEE Int. Symp. on EMC, Istanbul, Turkey. 2003.

56. Höijer M., Bäckström M., Loré J. Angular patterns in low level coupling measurements and in high level radiated susceptibility

testing // Proc. of 15th Int. Zurich Symp. on EMC, February 2003. P. 347–352.

57. Chevalier B., Hoffmann P., Sonnemann F. Study of HPM Effect on Electronics: Parasitic Reset // Book of abstracts EUROEM 2004, 12–16 July, Magdeburg, Germany. P. 94.

58. Ritter J., Joly J.-C. French/German Simulations of EM Coupling into the GENEC Testobject // Book of abstracts EUROEM 2004, 12–16 July, Magdeburg, Germany. P. 118.

59. Sonnemann F. Susceptibility Investigations of High-Power EM-Fields on Electronic Systems // Proc. of 15th Int. Zurich Symp. on EMC, February 2003. P. 115–120.

60. Zehong W., Binxian L., Chengrong L. The Susceptibility of the Microprocessor-Based Relay of High Voltage Substations to EMP // Proc. of IEEE Int. Symp. on EMC, Istanbul, Turkey. 2003.

61. Kappenman J.G., Radasky W.A., Gilbert J.L. Electric Power Grid Vulnerability to Natural and Intentional Geomagnetic Disturbances // Proc. of the 16th Int. Zurich Symp. on EMC, 2005, Zurich, Switzerland. P. 447–450.

62. Distribution Class Insulators to Steep-Front/Short Duration (SFSD) / / J. Kappenman, W. Radasky, S. Grzybowski, Y. Song // Impulses to Simulate the Early-Time HEMP. P. 381–384.

63. Grzybowski S., Kappenman J., Radasky W.A. Electrical Strength of Distribution Insulators under Steep Front, Short Duration Pulse // 17th International Zurich Symposium on Electromagnetic Compatibility. 2006. P. 610–613.

64. Fast Pulse Testing of Power System Control Equipment to Determine their Susceptibility to HEMP Conducted Transients / E. Savage, K. Smith, M. Madrid, J. Gilbert, W. Radasky // Proc. of the 16th Int. Zurich Symp. on EMC. Zurich, Switzerland, 2005. P. 377–380.

65. Immunity Research of Wireless Communication in Switch Cabinet Monitoring and Control / Z. Li, Y. Huang, X. Wang, R. Zeng // Proc. of Int. IEEE Symp. on EMC. 2006.

66. Kazuo Y., Kimio Y., Naruto Y. PED interference reporting system in Japan // Proc. of 7th Int. Symp. on electromagnitic compatibility and electromagnetic ecology, 2007, Saint-Petersburg, Russia. P. 220–223.

67. Kreitmair-Steck W., Tauber W. Can Portable Electronic Devices (PEDs) Interfere with Aircraft Systems? // Proc. of IEEE Int. Symp. on EMC, Istanbul, Turkey. 2003.
68. Passenger Transmitters as A Possible Cause of Aircraft Fuel Ignition / T.X. Nguyen, J.J. Ely, K.L. Dudley, M.O. Hatfield, R.E. Richardson // In Support of an Aircraft Accident Investigation. Proc. of Int. IEEE Symp. on EMC. 2006.
69. UWB and EMP susceptiblity of microprocessors and networks / C. Mojert [et al.] // Proc. of the 14th Int. Zurich Symp. on EMC, Zurich, Switzerland, February 20–22, 2001. P. 47–52.
70. Comparison of the High Power Microwave and Ultra Wide Band Susceptibility of Modern Microprocessor Boards / D. Nitsch, F. Sabath, H.-U. Schmidt, C. Braun // International Zurich Symposium on EMC, February 2003. P. 121–126.
71. Camp M., Garbe H. Influence of Operation- and Program- States on the Breakdown Effects of Electronics by Impact of EMP and UWB // Proc. of IEEE Int. Symp. on EMC, Istanbul, Turkey. 2003.
72. Camp M., Garbe H., Sabath F. Coupling of Transient Ultra Wide Band Electromagnetic Fields to Complex Electronic Systems // Proc. Int. IEEE Symp. on EMC. 2005.
73. Korte S., Camp M., Garbe H. Hardware and software simulation of transient pulse impact on integrated circuits // Proc. Int. IEEE Symp. on EMC. 2005.
74. Musolino F., Fiori F. Investigation on the susceptibility of microcontrollers to EFT interference. WE-AM-2-5.
75. Chevalier B., Martin M., Brette R. HPM Susceptibility of Electronic Circuit Boards // Book of abstracts EUROEM 2004, 12–16 July, Magdeburg, Germany. P. 94.
76. Fiori F., Crovetti P.S. Comparison of the susceptibility to EMI of MOS and BJT operational amplifiers // Proc. of the 16th Int. Zurich Symp. on EMC. Zurich, Switzerland. 2005. P. 369–372.
77. Crovetti Paolo S., Fiori Franco. RFI-Induced Failures in Switched Capacitor Circuits. TU-PM-3-4.
78. Mutoh A., Nitta S., Jikumaru T. Noise Immunity Characteristics of Integral Analog-to-Digital Converter including Voltage-to-Frequency Converter for Noise on Power-Supply-Lines // Proc. of IEEE Int. Symp. on EMC, Istanbul, Turkey. 2003.

79. Schoof A., ter Haseborg J.L. Immunity of Bluetooth-transmitters against interfering electromagnetic fields with high field-strengths // Proc. of the 16th Int. Zurich Symp. on EMC. 2005. Zurich, Switzerland. P. 27–30.
80. Simulation of Integrated Circuit Immunity with LECCS Model / K. Ichikawa, M. Inagaki, Y. Sakurai, I. Iwase, M. Nagata, O. Wada // Proc. of the 17th Int. Zurich Symp. on EMC, Singapore. 2006. P. 308–311.
81. Camp M., Korte S., Garbe H. Classification of the Destruction Effects in CMOS-Devices after Impact of Fast Transient Electromagnetic Pulses // Book of abstracts EUROEM 2004, 12–16 July, Magdeburg, Germany. P. 96.
82. Susceptibility of Sensor Networks to Intentional Electromagnetic Interference / J. Delsing, J. Ekman, J. Johansson, S. Sundberg, M. Bäckström, T. Nilsson // Proc. of the 17th Int. Zurich Symp. on EMC, Singapore. 2006. P. 172–175.
83. Zhuravliov V., Alexeev V. Thermal Conductivity Influence on Failures of Semiconductor ICs under Powerful EMP Action // Proc. of IEEE Int. Symp. on EMC, Istanbul, Turkey. 2003.
84. Breakdown Predictions of Microstrip Interconnects and Coplanar Waveguide-Built Devices in the Presence of HP-EMPs / W.-Y. Yin, X.T. Dong, J. Mao, L.-W. Li // Proc. of the 17th Int. Zurich Symp. on EMC, Singapore. 2006. P. 445–448.
85. Kohlberg I., Carter R.J. Some theoretical considerations regarding the susceptibility of information systems to unwanted electromagnetic signals // Proc. of the 14th Int. Zurich Symp. on EMC, Zurich, Switzerland, February 20–22, 2001. P. 41–46.
86. Влияние мощных импульсных микроволновых помех на полупроводниковые приборы и интегральные микросхемы / В.В. Антипов [и др.] // Зарубежная радиоэлектроника. 1995. № 1. С. 37–53.
87. Современное состояние и перспективы развития авиационных средств радиоэлектронной борьбы / О.В. Викулов [и др.] // Зарубежная радиоэлектроника. Успехи современной радиоэлектроники. 1998. № 12. С. 3–16.
88. Glenn C.M., Garver R.V. Trends in mixer damage, IEEE MTT-S // Int. Microwave Symp. Digest, 1989. Vol. 1. P. 475–477.

89. Dymarkowski K., Namiotko R., Katulski J.R. Electromagnetic compatibility tests of warship antitorpedo jamming system // Proc. 18th Int. Wroclaw symposium and exhibition on electromagnetic compatibility, Wroclaw, 28 – 30 June, 2006.
90. Koch M., Zappe W., Camp M. The Safety of Ordnance in High Frequency Electromagnetic Fields // Proc. of IEEE Int. Symp. on EMC, Istanbul, Turkey. 2003.
91. Linder S., Rantakokko J., Stenumgaard P. A New Approach for Estimating the Impact of Pulsed Interference on Digital Communication Systems // Proc. of IEEE Int. Symp. on EMC, Istanbul, Turkey. 2003.
92. Potrykus H.G., Kohlberg I. Resistance to extended IEMI by physical/correlated wireless random and non-random networks // Proc. of the 17th Int. Zurich Symp. on EMC, Singapore, 2006. P. 176–179.
93. Chen C. Examination of Electronic Module Immunity Using Transfer Functions // Proc. Int. IEEE Symp. on EMC. 2005.
94. Capstick M., Pearce D. EMC Susceptibility of Low Power Radio Receivers // Proc. of IEEE Int. Symp. on EMC, Istanbul, Turkey 2003.
95. Jakobus U. Application of numerical techniques based on the method of moments to the solution of a variety of real-world EMC problems // Journal for EMC. ITEM 2001. P. 98–105.
96. Microwave Testing of a Computer: a Representative Example of the Susceptibility of Commercial System / T.S. Seow [et al.] // Digest of EUROEM2000. Edinburgh, Scotland, 30 May – 2 June 2000. P. 14.
97. Susceptibility analysis of wiring in a complex system combining a 3-D solver and a transmission-line network simulation / L. Paletta [et al.] // IEEE Trans. Electromagn. Compat. 2002. Vol. 44, N 2. P. 309–317.
98. Schäfer M.T., Maurer J., Wiesbeck W. Attenuation measurements of different walls and rooms in hospitals // Proc. of the 15th Int. Zurich Symp. on EMC, Zurich, Switzerland. 2003. P. 635–638.
99. Siebert W.P. New Solutions for High Frequency Electronic Packaging // Proc. of IEEE Int. Symp. on EMC, Istanbul, Turkey. 2003.

100. A computer code for estimating pulsed electromagnetic disturbances penetrating into building power and earthing circuits / V.E. Fortov [et al.] // Proc. of the 14th Int. Zurich Symp. on EMC, Zurich, Switzerland, Feb. 20–22, 2001. P. 37–40.
101. Response of telecom protection to three IEC waveforms / M.A. Messier [et al.] // Proc. of the 15th Int. Zurich Symp. on EMC, Zurich, Switzerland, Feb. 18–20, 2003. P. 127–132.
102. Thottappillil R., Montano R., Mansson D. Response of Surge Protective Devices to Very Fast Transient Conducted Pulses // Book of abstracts EUROEM 2004. 12–16 July, Magdeburg, Germany. P. 86.
103. Distortion of electric and magnetic fields from lightning due to close-by metallic structures / A. Mosaddeghi, D. Pavanello, F. Rachidi, M. Rubinstein, P. Zweicker // Proc of IEEE Symp. on EMC. 2005.
104. Larsson A., Johansson B., Nyholm E.S. Radiated Electric Field Strength from High-Power Microwave Systems // Proc. of the 17th Int. Zurich Symp. on EMC, Singapore. 2006. P. 441–444.
105. He T., Kuhlman B. Investigation of Lightning Induced Transients on Power Interfaces for Aircraft Avionics Systems // Proc. of Int. IEEE Symp. on EMC. 2005.
106. Radasky W.A., Wik M.W. Intentional electromagnetic interference (IEMI) – understanding the threat and developing protection concepts // International Zurich Symposium on EMC, February 2003. P. 111–114.
107. 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. of the 15th Int. Wroclaw Symp. on EMC, June 27–30, 2000. Late Papers. P. 11–20.
108. Baum C.E. Maximization of electromagnetic response at a distance // Sensor and Simulation Note 312, October 1988, and IEEE Trans. on EMC, 1992. P. 148–153.
109. Baum C.E. Comparative system response to resonant and unipolar waveforms // Interaction Note 509, November 1994.

110. Baum C.E. A time-domain view of choice of transient excitation waveforms for enhanced response of electronic systems // Interaction Note 560, 14 Sept. 2000.
111. Bunting C.F., Yu S.-P. Statistical shielding effectiveness – an examination of the field penetration in a rectangular box using modal MOM // Proc. of IEEE Int. Symp. on EMC, August 19–23, 2002, Minneapolis, Minnesota. P. 210–215.
112. Ladbury J.M., Lehman T.H., Koepke G.H. Coupling to devices in electrically large cavities, or why classical EMC evaluation techniques are becoming obsolete // Proc. of IEEE Int. Symp. on EMC. August 19–23, 2002, Minneapolis, Minnesota. P. 648–655.
113. Jakobus U. Application of numerical techniques based on the method of moments to the solution of a variety of real-world EMC problems // Journal for EMC. ITEM 2001. P. 98–105.
114. White D., Atkinson K., Osburn D. Taming EMI in microprocessor systems // IEEE Spectrum. 1985. Vol. 22, N 12. P. 30–37.
115. Clupper T. A new PCB-level shielding technology // Interference technology. 2003. P. 187–195.
116. Krauthauser H.G., Tkachenko S., Nitsch J. The action of non-linear effects in a resonator // Proceedings of General Assembly of URSI. 2002.
117. Яцкевич В.А., Викулов Ю.Н. Экраны для защиты от электромагнитных волн СВЧ-диапазона // Сб. науч. докл. IV Междунар. симп. по электромагнитной совместимости и электромагнитной экологии, г. Санкт-Петербург, 19–22 июня 2001 г. С. 451–454.
118. Protection Properties of Advanced Textile Shields Determined in Frequency and Time Domain / M. Koch, M. Camp, R. Kebel, H. Garbe, F. Sabath, D. Nitsch // International Zurich Symposium on EMC, February 2003. P. 137–142.
119. E3 Characterization Testing of Modular Conductive Tents / W. Crevier, N. Wild, T. Gray, S. Colvin // Book of abstracts EUROEM, 2004, 12–16 July, Magdeburg, Germany. P. 33.
120. Thomas L. Weaver. Designing for High Level Excitation // Proc. of Int. IEEE Symp. on EMC. 2006.

121. Recht E., Naxon T., Cohen A. UG Filtering – An Effective Technology Against IEMI and HPM // Book of abstracts EUROEM 2004, 12–16 July, Magdeburg, Germany. P. 86.
122. Recht E., Naxon T., Cohen A. UG Filtering – An Effective Technology Against IEMI and HPM // Proc of IEEE Symp. on EMC. 2005.
123. Krzikalla R., Weber T., ter Haseborg J.L. Interdigital microstrip filters as protection devices against ultrawideband pulses // Proc. of IEEE Int. Symp. on EMC, Istanbul, Turkey. 2003.
124. Krzikalla R., ter Haseborg J.L. SPICE Simulations of UWB pulse stressed protection elements against transient interferences // Proc. of Int. IEEE Symp. on EMC. 2005.
125. The Effects and Diagnostic Uses of the Interaction of Radio Frequency Electromagnetic Radiation with Digital Electronic Systems / A.C. Marvin, I.D. Flintoft, M.P. Robinson, K. Fischer // Book of abstracts EUROEM 2004, 12–16 July, Magdeburg, Germany. P. 94.
126. Esser N., Smailus B. Measuring the Upset of CMOS and TTL due to HPM-Signals // Book of abstracts EUROEM 2004, 12–16 July, Magdeburg, Germany. P. 94.
127. Ropiak C.A., Stoudt D.C. Conditioned hardening of test objects due to repeated EMI testing // Proc. of the 16th Int. Zurich Symp. on EMC, Zurich, Switzerland. 2005. P. 539–544.
128. Microwave Breakdown in Slots / U. Jordan, D. Anderson, A. Kim, M. Lisak, M. Backstrom, O. Lunden // Book of abstracts EUROEM 2004, 12–16 July, Magdeburg, Germany. P. 113.
129. Bocquet F., Kedzia J.-C. Simulating the Electromagnetic Susceptibility of Automotive Vehicles in their Early Design Stage // Proc. of the 16th Int. Zurich Symp. on EMC, Zurich, Switzerland. 2005. P. 99–102.
130. Phyu H.N., Li Er-Ping, Yuan W. Analysis of Electromagnetic Susceptibility on High Speed Circuits Located in a Shielded Enclosure // Proc. of the 17th Int. Zurich Symp. on EMC, Singapore. 2006. P. 312–315.
131. Chua E.K., See K.Y., Liu Z. Modeling RF Voltage Drop of Printed Circuit Interconnects Using a Full-Wave Approach // Proc. of the 17th Int. Zurich Symp. on EMC, Singapore. 2006. P. 332–335.

132. Pouhe D., Monich G., Kemi W.F. Assessment of Resonance Properties of Electrically Small PCBs via Radar Cross-Section Measurements in a GTEM Cell // Proc. of the 16th Int. Zurich Symp. on EMC, Zurich, Switzerland. 2005. P. 357–362.
133. Pennesi S., Sebastiani S. Information Security and Emissions Control // Proc. of Int. IEEE Symp. on EMC. 2005.
134. Thomason G., Ivanov V. Method for Evaluating System Immunity to Wireless GSM Devices // Proc. of Int. IEEE Symp. on EMC. 2005.

Оглавление

Введение	3
1. ХРОНОЛОГИЯ ИССЛЕДОВАНИЙ.....	5
2. АКТУАЛЬНОСТЬ ИССЛЕДОВАНИЙ	7
3. ИСТОЧНИКИ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ	15
4. ЭЛЕКТРОМАГНИТНАЯ УЯЗВИМОСТЬ СИСТЕМ И КОМПОНЕНТОВ	28
4.1. Компьютеры.....	28
4.2. Автомобиль	35
4.3. Макет корпуса ракеты GENEC	37
4.4. Электроэнергетика	42
4.5. Авионика	45
4.6. Компоненты	49
4.7. Разное.....	64
5. ОСЛАБЛЕНИЕ ИЛИ УСИЛЕНИЕ ЭЛЕКТРОМАГНИТНЫХ ВОЗДЕЙСТВИЙ	68
6. ПУТИ РЕШЕНИЯ ПРОБЛЕМЫ ЗАЩИТЫ ОТ ПРЕДНАМЕРЕННЫХ ЭЛЕКТРОМАГНИТНЫХ ВОЗДЕЙСТВИЙ	77
6.1. Общие подходы	77
6.2. Некоторые технические решения	86
Заключение	92
Контрольные вопросы	95
Список сокращений	99
Литература.....	100

Учебное издание

Газизов Тальгат Рашитович

Заболоцкий Александр Михайлович

Куксенко Сергей Петрович

**ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ: ПРЕДНАМЕРЕННЫЕ
СИЛОВЫЕ ЭЛЕКТРОМАГНИТНЫЕ ВОЗДЕЙСТВИЯ**

Учебное пособие

Подписано в печать 30.05.18. Формат 60x84/16.

Усл.-печ. л. 6,74. Тираж 100 экз. Заказ 211.

Томский государственный университет
систем управления и радиоэлектроники.
634050, г. Томск, пр. Ленина, 40.
Тел. (3822) 533018.